

Verordnung über das Staatsschutz-Informationen-System (ISIS-Verordnung)

Änderung vom 30. Juni 2004

*Der Schweizerische Bundesrat
verordnet:*

I

Die ISIS-Verordnung vom 30. November 2001¹ wird wie folgt geändert:

Art. 2 Abs. 2 Bst. a, e und f

² Es wird verwendet zur:

- a. Recherche und Analyse der erfassten Daten;
- e. Dokumentation;
- f. Geschäftsabwicklung.

Art. 3 **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;

¹ SR 120.3

- j. Factsheets: Standardisierte, periodisch nachgeführte Beurteilungen der strategischen Analyse zu einem bestimmten Objekt.

Art. 4 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. «ISIS01 Staatsschutz» mit den Datenbanken «Staatsschutz», «Verwaltungspolizei», «Dokumentation» und «Nummernsystem»;
- c. «ISIS02 Verwaltung» mit der Datenbank «Verwaltung»;
- d. «ISIS03 Waffen» mit den Datenbanken «Waffenerwerb durch Ausländer» und «Entzug von Bewilligungen und die Beschlagnahme von Waffen»;
- 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. «Verwaltungspolizei» (VP): personen- und ereignisbezogene Informationen aus dem Bereich der verwaltungspolizeilichen Zentralstellen des Dienstes für Analyse und Prävention (DAP);
- c. «Dokumentation» (DO): dokumentarische Informationen aus dem gesamten Arbeitsbereich des DAP sowie gemäss Artikel 11 der Verordnung vom 27. Juni 2001² 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;
- 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;

² SR 120.2

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

Art. 5 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 Justiz- und Polizeidepartement (Departement) geregelt.

Art. 6 Abs. 1

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

Art. 7 Benutzerinnen und Benutzer

¹ Benutzerinnen und Benutzer von ISIS sind:

- a. die Bediensteten des DAP und der kantonalen Organe zur Wahrung der inneren Sicherheit; sie sind über ein Abrufverfahren an das System angeschlossen;
- b. Mitarbeiterinnen und Mitarbeiter des Bundessicherheitsdienstes (BSD), der Bundeskriminalpolizei (BKP) und der für die Personensicherheitsprüfung beim Bund zuständigen Stelle (Fachstelle PSP, IOS); sie können mittels Abrufverfahren Kurzabfragen vornehmen.

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 Departement geregelt. Die Chefin oder der Chef DAP oder deren oder dessen Stellvertreterin oder Stellvertreter entscheidet über die individuellen Anträge.

⁵ Die Qualitätssicherung DAP ist für den Vollzug der Zugriffsberechtigungen zuständig.

Art. 8 Anschluss der Kantone

Das Departement 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. 9

Aufgehoben

Art. 10 Abs. 2, 2bis, 3 und 4

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

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

- a. Mitarbeiterinnen und Mitarbeiter des Ausländerdienstes des DAP: Daten aus der Fotopasskontrolle;
- b. Mitarbeiterinnen und Mitarbeiter der Zentralstelle Waffen des DAP: Daten der Datenbanken DEWA und DEBBWA;
- c. Mitarbeiterinnen und Mitarbeiter der Zentralstelle Sprengstoff/Pyrotechnik des DAP: Daten der Datenbank BARBARA und VP;
- d. Mitarbeiterinnen und Mitarbeiter der Analyse des DAP: Factsheets;
- e. Mitarbeiterinnen und Mitarbeiter des Bereichs Personensicherheitsprüfungen: Daten der Datenbank PSP
- f. Mitarbeiterinnen und Mitarbeiter der kantonalen Organe zur Wahrung der inneren Sicherheit: Daten der Datenbank NU.

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).

⁴ Die Qualitätssicherung des DAP 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).

Art. 11 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 Abs. 1, 2 und 4

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

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

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

Art. 13 Abs. 1 Bst. c Einleitungssatz, e, p und t

¹ Der DAP kann, mit Ausnahme von Daten der Datenbanken DEWA und DEBBWA sowie der im Rahmen von Personensicherheitsprüfungen erhobenen Daten, die in ISIS bearbeiteten Personendaten im Einzelfall weitergeben an:

- c. andere Verwaltungseinheiten des Bundesamtes für Polizei (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,
 4. zur Beurteilung von Sicherheitsrisiken beim Schutz von Personen und Gebäuden;
- e. das Bundesamt für Zuwanderung, Integration und Auswanderung (IMES) für Massnahmen gegenüber Ausländern, insbesondere zu deren Fernhaltung sowie für die Behandlung von Einbürgerungsgesuchen;
- p. 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;
- t. 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.

Art. 16 Abs. 1–4

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.

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 Staatsschutzfähigkeit 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 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.

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

Art. 17 Abs. 3

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

Art. 18 Abs. 1, 3 und 4

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.

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

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

Art. 19 Daten und Akten der kantonalen Staatsschutzdienste

¹ Die kantonalen Organe zur Wahrung der inneren Sicherheit dürfen die im Rahmen ihrer Staatsschutzfähigkeit 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 Abs. 1–3

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

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.

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.

Art. 21 Abs. 1

¹ Für die Gewährleistung der Datensicherheit gelten Artikel 20 der Verordnung vom 14. Juni 1993³ zum Bundesgesetz über den Datenschutz, die Verordnung vom 26. September 2003⁴ über die Informatik und Telekommunikation in der Bundesverwaltung sowie die vom Departement nach Artikel 8 festzulegenden Voraussetzungen für den Anschluss der kantonalen Organe zur Wahrung der inneren Sicherheit.

Art. 22 Abs. 2

² Die Qualitätssicherung DAP ist zuständig für die Ausbildung und Betreuung der Benutzerinnen- und Benutzer und sorgt für die Durchsetzung des Bearbeitungsreglementes.

Art. 26

Aufgehoben

II

Diese Änderung tritt am 1. September 2004 in Kraft.

30. Juni 2004

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Josef Deiss

Die Bundeskanzlerin: Annemarie Huber-Hotz

³ SR 235.11

⁴ SR 172.010.58

Zur Übereinstimmung der Seitenzahlen in allen
Amtssprachen der AS bleibt diese Seite leer.