

Ordinanza sul sistema per il trattamento dei dati relativi alla protezione dello Stato (Ordinanza ISIS)

del 30 novembre 2001

Il Consiglio federale svizzero,

visti gli articoli 15 capoversi 3 e 5, e 30 della legge federale del 21 marzo 1997¹ sulle misure per la salvaguardia della sicurezza interna (LMSI);
visto l'articolo 39 capoverso 3 della legge federale del 20 giugno 1997² sulle armi, gli accessori di armi e le munizioni (LArm);

ordina:

Sezione 1: Disposizioni generali

Art. 1 Oggetto

La presente ordinanza disciplina la gestione, il corpus dei dati e l'utilizzazione del sistema per il trattamento dei dati relativi alla protezione dello Stato (ISIS).

Art. 2 Scopo

¹ L'ISIS serve agli scopi seguenti:

- a. misure preventive in materia di protezione federale dello Stato;
- b. compiti di polizia di sicurezza e amministrativa;
- c. esecuzione della legislazione sulle armi.

² È utilizzato per:

- a. analizzare i dati rilevati e la documentazione;
- b. elaborare rapporti di situazione;
- c. svolgere compiti amministrativi;
- d. depositare e gestire documenti.

RS 120.3

¹ **RS 120**

² **RS 514.54**

Art. 3 Definizioni

Nella presente ordinanza s'intende per:

- a. dati: le informazioni memorizzate nell'ISIS;
- b. dati di base: le informazioni generali che si riconducono a uno o più dati sugli antecedenti;
- c. principali informazioni biografiche: indicazione dei seguenti dati di base: cognome, nome, rispettivamente organizzazione o ditta; pseudonimo, anno di nascita; falso anno di nascita; data di nascita; falsa data di nascita; grafia fonetica di tutti i cognomi e nomi; cittadinanza; per gli Svizzeri il luogo d'origine;
- d. dati sugli antecedenti: le informazioni in merito a singoli eventi;
- e. dati marginali sugli antecedenti: tutti i dati sugli antecedenti senza il testo sugli antecedenti;
- f. consultazione breve: consultazione combinata di persone e terzi, nella quale sono visualizzati soltanto i dati di base e i dati marginali sugli antecedenti;
- g. immagini: documenti registrati nell'ISIS sotto forma di immagini;
- h. dati statistici: rilevamenti numerici delle informazioni memorizzate nell'ISIS;
- i. terzi: persone o organizzazioni che hanno un legame con una persona o organizzazione sulla quale sono rilevati dati di base, ma che non adempiono le condizioni per essere registrate.

Art. 4 Banche dati

L'ISIS si compone delle banche dati seguenti:

- a. «Protezione dello Stato» (ST): informazioni su persone e eventi, provenienti dall'attività di natura preventiva esplicita nel settore della protezione dello Stato;
- b. «Polizia amministrativa» (VP): informazioni su persone e eventi, provenienti dal settore degli uffici centrali di polizia amministrativa del Servizio di analisi e prevenzione (SAP);
- c. «Amministrazione» (VE): informazioni necessarie al controllo delle pratiche;
- d. «Documentazione» (DO): informazioni documentarie provenienti da tutto il settore d'attività del SAP e corrispondenti all'articolo 11 dell'ordinanza del 27 giugno 2001³ sulle misure per la salvaguardia della sicurezza interna (OMSI);
- e. «Sistema numerico» (NU): informazioni su eventi, provenienti da programmi di ricerca selezionati;

³ RS 120.2

- f. «Acquisto di armi da parte di stranieri» (DEWA): informazioni su persone, concernenti l'acquisto di armi da parte di cittadini stranieri senza permesso di domicilio in Svizzera;
- g. «Revoca di autorizzazioni e sequestro di armi» (DEBBWA): informazioni su persone, concernenti la revoca di autorizzazioni e il sequestro di armi in Svizzera;
- h. «Gestione elettronica dei documenti» (EAV): immagini dei documenti sui quali si fondano i dati di base e i dati sugli antecedenti;
- i. «Analisi strategica e descrizione della situazione» (STRALAG): informazioni che servono ad elaborare le analisi strategiche e i rapporti di situazione del SAP;
- j. «INFOPRESS»; informazioni provenienti da fonti accessibili al pubblico.

Art. 5 Dati trattati

¹ I dati sugli antecedenti, memorizzati nelle banche dati ISIS, sono raggruppati in categorie secondo le materie, nella misura in cui sia sensato per il dispositivo d'accesso.

² I singoli campi di dati sono elencati nell'allegato 1⁴.

Art. 6 Intranet

¹ L'Intranet ISIS è un sistema di comunicazione a circuito chiuso e gestito in maniera codificata. Si compone di un Intranet e di una posta elettronica.

² Il SAP lo mette esclusivamente a disposizione degli utenti dell'ISIS.

Sezione 2: Utenti, collegamento e accesso ai dati

Art. 7 Utenti

¹ Utenti dell'ISIS sono gli agenti del SAP e degli organi cantonali incaricati di salvaguardare la sicurezza interna. Sono collegati al sistema per mezzo di una procedura di richiamo.

² Per consultazioni brevi o per consultazioni relative alle principali informazioni biografiche, gli agenti del Servizio federale di sicurezza (SFS), della Polizia giudiziaria federale (PGF) e del servizio competente per i controlli di sicurezza delle persone presso la Confederazione possono essere collegati al sistema mediante procedura di richiamo.

³ Gli utenti hanno accesso ai dati di cui necessitano per l'adempimento dei loro compiti legali.

⁴ Il testo degli allegati 1 e 2 dell'ordinanza del 30 novembre 2001 sul sistema per il trattamento dei dati relativi alla protezione dello Stato non è pubblicato né nella RU né nella RS. Gli estratti sono ottenibili presso l'EDMZ, 3003 Berna.

⁴ I diritti d'accesso sono disciplinati dal Dipartimento federale di giustizia e polizia (Dipartimento) nell'allegato 2⁵ della presente ordinanza. Il capo del SAP decide in merito alle richieste individuali.

Art. 8 Collegamento dei Cantoni

Gli organi cantonali sono collegati all'ISIS non appena il Cantone garantisce mediante provvedimenti organizzativi l'utilizzazione corretta dei dati e la loro sicurezza e il Dipartimento ha approvato la domanda cantonale di collegamento.

Art. 9 Accesso alla banca dati ST

¹ Nel caso richiedano informazioni alla banca dati relativa alla protezione dello Stato (ST), agli agenti del SAP sono forniti tutti i dati di base, i dati sugli antecedenti e le immagini necessari all'adempimento dei loro compiti legali.

² Nel caso richiedano informazioni alla banca dati relativa alla protezione dello Stato (ST), agli agenti degli organi cantonali incaricati di salvaguardare la sicurezza interna sono forniti, ad eccezione dei dati classificati provenienti dai contatti diretti con le autorità di sicurezza estere, tutti i dati di base, i dati sugli antecedenti e le immagini necessari all'adempimento dei loro compiti legali.

³ Agli agenti della PGF e del SFS può essere rilasciata, per l'adempimento dei loro compiti legali, l'autorizzazione di effettuare consultazioni brevi della banca dati ST.

⁴ Le altre autorità federali di polizia o preposte al perseguimento penale sono collegate alla banca dati ST mediante procedura di richiamo per quanto necessitano dei dati per l'adempimento dei loro compiti legali.

⁵ Agli agenti del servizio competente per i controlli di sicurezza delle persone presso la Confederazione può essere rilasciata, per l'adempimento dei loro compiti legali, l'autorizzazione per consultare le principali informazioni biografiche della banca dati ST.

Sezione 3: Trattamento dei dati

Art. 10 Introduzione dei dati e controllo della qualità

¹ Nell'ISIS possono essere trattate soltanto informazioni corrispondenti agli scopi definiti nell'articolo 2.

² L'Analisi preventiva del SAP introduce i dati nell'ISIS e determina la categoria di antecedenti e la durata di conservazione.

³ Le informazioni destinate alle banche dati ST e VP sono, in un primo tempo, introdotte provvisoriamente (codice «p») e valutate secondo provenienza, modo di

⁵ Il testo degli allegati 1 e 2 dell'ordinanza del 30 novembre 2001 sul sistema per il trattamento dei dati relativi alla protezione dello Stato non è pubblicato né nella RU né nella RS. Gli estratti sono ottenibili presso l'EDMZ, 3003 Berna.

trasmissione, contenuto e conoscenze già disponibili (codice «g» per i dati attendibili sugli antecedenti e codice «u» per quelli poco attendibili).

⁴ Il servizio di controllo della qualità ISIS del SAP (Controllo della qualità) esamina il tenore della registrazione provvisoria, segnatamente l'indicazione delle fonti, la valutazione dell'informazione, la data della prossima valutazione globale e la durata di conservazione e conferma la registrazione definitiva dei dati (codice «k» per i dati controllati).

⁵ Il capo del SAP o il suo sostituto può incaricare il servizio di controllo della qualità di esaminare le altre banche dati.

Art. 11 Gestione elettronica dei documenti

¹ Si può rinunciare al deposito cartaceo dei documenti per quanto i documenti su cui si fondano i dati di base e i dati sugli antecedenti siano memorizzati come immagini nella gestione elettronica dei documenti.

² La gestione elettronica dei documenti deve garantire la regolare tenuta dei documenti e l'archiviazione.

Art. 12 Consultazione dei dati

¹ I dati possono essere consultati secondo le principali informazioni biografiche, i dati di base e i dati sugli antecedenti oppure i dati di base e i dati sugli antecedenti. Le immagini non possono essere richiamate separatamente.

² Per i dati sugli antecedenti può essere consultata soltanto una banca dati alla volta.

³ Agenti del SAP specialmente formati possono procedere a valutazioni nel loro campo d'attività.

Art. 13 Comunicazione di dati personali

¹ Ad eccezione di quelli delle banche dati DEWA e DEBBWA nonché dei dati rilevati nell'ambito dei controlli di sicurezza delle persone, in singoli casi il SAP può comunicare i dati personali trattati nell'ISIS:

- a. alle autorità cantonali preposte al perseguimento penale, allo scopo di prevenire e perseguire atti punibili;
- b. al Dipartimento federale degli affari esteri, per valutare le istanze di accreditamento o il diritto di presenza in Svizzera di cittadini di Stati esteri o di membri di organizzazioni internazionali se necessario alla tutela degli obblighi di protezione risultanti dal diritto internazionale pubblico nonché nel quadro dei suoi diritti di cooperare nel settore della legislazione sugli scambi commerciali con l'estero;
- c. ad altre unità amministrative dell'Ufficio federale di polizia:
 1. a sostegno di procedure d'indagine di polizia giudiziaria nonché alle ricerche preliminari atte al rilevamento dei fatti nel settore della lotta contro il crimine organizzato e il traffico illecito di stupefacenti,

2. nel quadro dell'assistenza amministrativa internazionale in materia penale (INTERPOL),
 3. per iscrizioni nel sistema di ricerca informatizzata di polizia RIPOL,
 4. per la valutazione dei rischi per la sicurezza relativi alla protezione di persone ed edifici;
- d. all'Ufficio federale di giustizia, per completare o eseguire una richiesta d'assistenza giudiziaria in materia penale;
- e. all'Ufficio federale degli stranieri, per i provvedimenti nei confronti degli stranieri, segnatamente per il loro allontanamento come anche per il trattamento delle domande di naturalizzazione;
- f. all'Ufficio federale dei rifugiati, per valutare le domande d'asilo;
- g. al Dipartimento federale della difesa, della protezione della popolazione e dello sport, per l'esercizio dei suoi diritti di cooperare nel settore della legislazione sull'economia esterna;
- h. al Servizio della sicurezza militare, allo scopo di:
1. valutare la situazione dal profilo della sicurezza militare,
 2. proteggere informazioni e opere militari,
 3. adempiere compiti di polizia di sicurezza e di polizia criminale nell'ambito dell'esercito;
- al Servizio della sicurezza militare quando i militari sono chiamati in servizio attivo, allo scopo di:
4. garantire la sicurezza preventiva dell'esercito da spionaggio, sabotaggio e altri atti illeciti,
 5. acquisire informazioni,
 6. garantire la protezione delle persone con importanti cariche pubbliche;
- i. al servizio informazioni del Dipartimento federale della difesa, della protezione della popolazione e dello sport, in relazione a informazioni rilevanti in materia di politica di sicurezza;
- j. alla giustizia militare, per l'adempimento dei compiti di polizia giudiziaria e di sicurezza;
- k. agli organi delle guardie di confine e delle dogane, per accertare la dimora delle persone, operare controlli doganali ed effettuare procedimenti amministrativi penali;
- l. al Segretariato di Stato dell'economia, per l'esecuzione della legge federale del 13 dicembre 1996⁶ sul materiale bellico e delle misure nel settore della legislazione sull'economia esterna;
- m. all'Ufficio federale della formazione professionale e della tecnologia, per la concessione dei permessi d'uso di sostanze esplosive;

⁶ RS 514.51

- n. all'Ufficio federale dell'aviazione civile e alla Posta Svizzera, per l'esecuzione di misure di polizia di sicurezza;
- o. all'Ufficio federale dell'energia, per l'esecuzione della legge del 23 dicembre 1959⁷ sull'energia nucleare e per l'esercizio dei suoi diritti di cooperare nel settore della legislazione sull'economia esterna;
- p. ai servizi competenti della Confederazione e dei Cantoni, per procedere ai controlli di sicurezza relativi alle persone;
- q. all'ufficio interessato, se necessario per garantirne la sicurezza;
- r. agli uffici e ai privati, se la comunicazione dei dati è necessaria per permettere loro di motivare una domanda d'informazione;
- s. a privati, se ciò permette di prevenire un pericolo considerevole.

² Per la comunicazione dei dati all'estero si applica l'articolo 17 capoversi 3-5 e 7 LMSI.

³ La comunicazione di dati non è ammessa se vi si oppongono interessi preponderanti pubblici o privati.

⁴ In occasione di ogni comunicazione di dati, il destinatario va informato sull'attendibilità e l'attualità dei dati (art. 10). Egli può utilizzare i dati soltanto per lo scopo per cui gli sono stati trasmessi. È reso attento sulle limitazioni d'utilizzazione e sul fatto che l'autorità che comunica i dati si riserva il diritto di esigere informazioni sull'utilizzazione che ne è stata fatta.

⁵ La comunicazione dei dati nonché i destinatari, l'oggetto e il motivo della stessa vanno registrati.

⁶ La comunicazione di dati contenuti nelle banche dati DEWA e DEBBWA è retta dall'articolo 43 dell'ordinanza del 21 settembre 1998⁸ sulle armi.

Art. 14 Copia di dati in altre collezioni di dati

¹ I dati dell'ISIS non possono essere copiati in altre collezioni di dati né per il tramite di installazioni di comunicazione né di supporti di dati. Questa disposizione non è applicabile all'archiviazione elettronica dei dati dell'ISIS nell'Archivio federale.

² Per procedere a valutazioni speciali è possibile trasferire per breve tempo i dati dell'ISIS in banche dati di lavoro. Tali dati devono essere cancellati dopo la conclusione delle valutazioni.

⁷ RS 732.0

⁸ RS 514.541

Art. 15 Diritto d'essere informati delle persone interessate

¹ Il diritto d'essere informati è retto dall'articolo 18 LMSI.

² Il diritto d'essere informati concernente dati delle banche dati DEWA e DEBBWA è retto dagli articoli 8 e 9 della legge federale del 19 giugno 1992⁹ sulla protezione dei dati.

Art. 16 Valutazione globale periodica dei dati nella banca dati ST

¹ Il Controllo della qualità procede a una nuova valutazione globale di ciascun insieme di dati (dati di base e dati sugli antecedenti) al più tardi cinque anni dopo la registrazione del primo dato o tre anni dopo l'ultima valutazione globale.

² Esso valuta, tenendo conto dei pericoli e rischi attuali, se, per quanto concerne il rischio per la sicurezza interna, o per la valutazione amministrativa, gli antecedenti registrati in un insieme di dati presentino un elevato grado di plausibilità e possano essere ulteriormente utilizzati per altre attività nel settore della protezione preventiva dello Stato.

³ I dati sugli antecedenti di una persona memorizzati come poco attendibili da più di tre anni possono continuare a essere trattati come tali (codice «u») fino alla prossima valutazione globale soltanto se necessari per l'adempimento dei compiti legali e se il capo del SAP o il suo sostituto ne abbia autorizzato il trattamento.

⁴ I dati concernenti terzi, registrati da più di tre anni senza dati di base propri, sono anonimizzati in occasione della valutazione globale.

⁵ Il Controllo della qualità cancella i dati che non sono più necessari. In caso di utilizzazione ulteriore di dati ancora necessari va annotata la valutazione globale.

Art. 17 Durata di conservazione dei dati

¹ I dati di polizia preventiva possono essere memorizzati nell'ISIS per 15 anni al massimo.

² Per i dati indicati qui di seguito si applica la seguente durata massima di conservazione:

- a. per i dati dei programmi di ricerca di polizia preventiva in corso: 20 anni;
- b. per i dati concernenti divieti d'entrata: fino a 10 anni dopo la loro scadenza;
- c. per dati provenienti da procedure di controllo di sicurezza relative alle persone: 5 anni;
- d. per dati provenienti dalla corrispondenza con organi amministrativi e privati: 30 rispettivamente 10 anni.

³ I dati delle banche dati sulla documentazione (DO), STRALAG e INFOPRESS possono essere conservati per una durata illimitata.

⁹ RS 235.1

⁴ La conservazione dei dati contenuti nelle banche dati DEWA e DEBBWA è retta dall'articolo 45 dell'ordinanza del 21 settembre 1998¹⁰ sulle armi.

Art. 18 Cancellazione dei dati

¹ I dati sugli antecedenti sono cancellati entro 3 mesi dalla scadenza della durata di conservazione, a meno che, valutati i rischi e pericoli attuali, gli stessi risultino indispensabili per l'adempimento dei compiti legali secondo la decisione del capo del SAP o del suo sostituto.

² Nei casi di cui al capoverso 1 la durata di conservazione ulteriore è di 3 anni. È possibile una sola proroga.

³ Con la cancellazione dell'ultimo antecedente deve essere cancellato l'intero insieme di dati (dati di base e dati sugli antecedenti).

Art. 19 Comunicazione della cancellazione ai Cantoni

Se sono cancellati dati dell'ISIS provenienti da organi cantonali con compiti di sicurezza, il Controllo della qualità informa detti organi affinché distruggano i dati e documenti tenuti parallelamente.

Art. 20 Obbligo di offrire i documenti all'Archivio federale

¹ I dati e i documenti non più utilizzati o quelli destinati alla cancellazione sono offerti all'Archivio federale per l'archiviazione.

² Non sono offerti per l'archiviazione i dati classificati provenienti dal da rapporti diretti con autorità di sicurezza estere.

³ I documenti designati dall'Archivio federale come non degni di essere archiviati sono distrutti. Sono salve le altre disposizioni legali in materia di distruzione dei documenti.

⁴ Prima della consegna dei documenti dei fascicoli personali all'Archivio federale, il SAP introduce nella banca dati relativa all'amministrazione la data di consegna, il numero di registrazione e le informazioni biografiche della persona interessata; tali informazioni vi sono conservate per dieci anni e quindi cancellate.

Sezione 4: Disposizioni organizzative

Art. 21 Sicurezza dei dati e verbalizzazione automatica

¹ La sicurezza dei dati è disciplinata dall'articolo 20 dell'ordinanza del 14 giugno 1993¹¹ relativa alla legge federale sulla protezione dei dati e dal capitolo 3 dell'ordinanza del 23 febbraio 2000¹² concernente l'informatica e la telecomunicazione nell'Amministrazione federale.

¹⁰ RS 514.541

¹¹ RS 235.11

¹² RS 172.010.58

² Il SAP disciplina nel regolamento per il trattamento dei dati le misure organizzative e tecniche intese a evitare il trattamento non autorizzato dei dati e ad assicurare la verbalizzazione automatica dei dati introdotti.

³ Durante l'intera operazione di trasmissione, i dati dell'ISIS sono trasmessi soltanto in forma codificata.

Art. 22 Responsabilità e competenze

¹ Il SAP è responsabile dell'ISIS . Esso emana il regolamento per il trattamento dei dati.

² Il Controllo della qualità vigila affinché gli utenti si attengano alla presente ordinanza, ai relativi allegati e al regolamento per il trattamento dei dati.

³ Il Centro Servizi Informatici (ICS) del Dipartimento è responsabile della gestione e della sicurezza dell'ISIS.

⁴ Nel singolo caso il consulente per la protezione dei dati dell'Ufficio federale di polizia può verificare la conformità del trattamento dei dati nell'ISIS alle prescrizioni sulla protezione dei dati.

Art. 23 Finanziamento

¹ La Confederazione finanzia la trasmissione dei dati fino alla centrale di collegamento dei Cantoni.

² I Cantoni assumono le spese:

- a. per l'acquisto e la manutenzione dei loro apparecchi;
- b. per l'installazione e la gestione della loro rete di distribuzione capillare.

Art. 24 Esigenze tecniche

¹ Il Dipartimento fissa le esigenze tecniche che devono essere soddisfatte dai terminali dei Cantoni.

² I particolari sono fissati nel regolamento per il trattamento dei dati.

Sezione 5: Disposizioni finali

Art. 25 Diritto previgente: abrogazione

L'ordinanza del 1° dicembre 1999¹³ sul sistema per il trattamento dei dati relativi alla protezione dello Stato è abrogata.

¹³ RU 1999 3461, 2000 1227 e 2027

Art. 26 Disposizione transitoria

¹ I dati provenienti da procedure d'indagine di polizia giudiziaria della Confederazione che sono registrati nell'ISIS sono trasferiti nella banca dati JANUS della PCF.

² Il SAP verifica in precedenza di quali dati provenienti da procedure d'indagine di polizia giudiziaria della Confederazione necessita per scopi di polizia preventiva e quali dati sono nuovamente trattati nell'ISIS. I rimanenti dati sono cancellati dopo il trasferimento secondo il capoverso 1.

Art. 27 Entrata in vigore

La presente ordinanza entra in vigore il 1° gennaio 2002.

30 novembre 2001 In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Moritz Leuenberger
La cancelliera della Confederazione, Annemarie Huber-Hotz