Ordinanza sui sistemi d'informazione del Servizio delle attività informative della Confederazione (OSI-SIC)

del 4 dicembre 2009 (Stato 1° aprile 2011)

Il Consiglio federale svizzero,

visto l'articolo 5 capoversi 1 e 4 della legge federale del 3 ottobre 2008[1] sul servizio informazioni civile (LSIC);
visti gli articoli 15 capoversi 3 e 5 nonché 30 della legge federale del 21 marzo 1997[2] sulle misure per la salvaguardia della sicurezza interna (LMSI);
visto l'articolo 17*a* della legge federale del 19 giugno 1992[3] sulla protezione dei dati,

ordina:

Sezione 1: Oggetto e definizioni

Art. 1 Oggetto

La presente ordinanza disciplina la gestione, il corpus dei dati e l'utilizzazione dei seguenti sistemi d'informazione del Servizio delle attività informative della Confederazione (SIC):

a. Sistema d'informazione Sicurezza esterna (ISAS);

b. Sistema d'informazione Sicurezza interna (ISIS).

Art. 2 Definizioni

Nella presente ordinanza s'intende per:

a. dati: informazioni memorizzate nei sistemi d'informazione del SIC;

b. oggetti: compilazioni di dati relative a una o più persone, organizzazioni, cose o eventi;

c. comunicazioni: singole informazioni immesse, relative a uno o più oggetti;

d. relazioni: connessioni tra singoli oggetti e singole comunicazioni;

e. insieme di dati: insieme di comunicazioni e relazioni concernenti un oggetto;

f. dati OCR: dati relativi a documenti registrati in maniera da consentire una ricerca a testo libero;

RU **2009** 7041

1 RS **121**
2 RS **120**
3 RS **235.1**

g. immagini: documenti registrati sotto forma di immagini;

h. consultazioni brevi: consultazioni online limitate volte a verificare se una persona è registrata in un sistema d'informazione del SIC;

i. terzi: persone o organizzazioni che sono rilevanti ai fini della protezione dello Stato unicamente in virtù di un legame con un oggetto;

j. schede informative: valutazioni periodiche standardizzate dell'analisi strategica concernente un oggetto.

Sezione 2: Disposizioni generali sui sistemi d'informazione del SIC

Art. 3 Scopo dei sistemi d'informazione del SIC

1 I sistemi d'informazione del SIC servono a quest'ultimo per l'adempimento dei propri compiti ai sensi dell'articolo 1 LSIC.

2 Essi sono utilizzati per:

a. ricerche nel corpus dei dati rilevati e relative analisi;

b. l'elaborazione di rapporti di situazione;

c. lo svolgimento di compiti amministrativi;

d. il deposito e la gestione di documenti;

e. l'esecuzione di lavori di documentazione;

f. lo svolgimento delle pratiche.

Art. 4 Autorizzazioni di consultazione

1 Chi per principio è autorizzato a consultare i sistemi d'informazione del SIC ha accesso ai dati di cui abbisogna per l'adempimento dei compiti stabiliti dalla legge.

2 Il Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) disciplina le autorizzazioni di consultazione.

3 Il direttore del SIC o il suo sostituto decide in merito alle singole richieste.

4 Il settore Gestione delle informazioni del SIC è competente per l'esecuzione delle autorizzazioni di consultazione.

Art. 5 Consultazione e visualizzazione di dati

1 Gli utenti dei sistemi d'informazione del SIC possono consultare i dati secondo gli oggetti, le relazioni, le comunicazioni, le attività, nonché mediante ricerca a testo libero.

2 Gli oggetti e le loro relazioni possono essere visualizzati e le visualizzazioni possono essere memorizzate.

Art. 6 Strumento informatizzato di analisi e valutazione

Mediante uno strumento informatizzato di analisi e valutazione, gli utenti dei sistemi d'informazione del SIC possono, nel quadro delle rispettive autorizzazioni d'accesso, accedere contemporaneamente a tutti i sistemi d'informazione del SIC.

Art. 7 SILAN

1 Il sistema SILAN è un sistema di comunicazione criptato interno al SIC per il trattamento di dati classificati SEGRETO.

2 Il SIC mette a disposizione il sistema SILAN unicamente agli utenti del SIC.

Art. 8 Intranet SIC

1 L'Intranet SIC è un sistema di comunicazione criptato per il trattamento di dati classificati CONFIDENZIALE.

2 Il SIC mette a disposizione l'Intranet SIC unicamente agli utenti del sistema ISIS.

Art. 9 Documentazione generale

1 Nei suoi sistemi d'informazione il SIC gestisce una documentazione proveniente da fonti pubblicamente accessibili, con:

a. informazioni su persone, organizzazioni e fattispecie nell'ambito dei compiti previsti dalla LSIC;

b. informazioni su persone e organizzazioni la cui sicurezza potrebbe essere minacciata in Svizzera;

c. informazioni su Paesi nonché contesti sociali e politici che potrebbero essere rilevanti per la valutazione della situazione;

d. informazioni scientifiche e tecniche nel campo d'attività delle autorità di sicurezza.

2 Il SIC gestisce un portale personalizzato per l'utilizzo di fonti pubblicamente accessibili (Portale interattivo per fonti pubbliche, IPOS).

3 Esso gestisce un servizio di documentazione su materiale che propugna razzismo o atti di violenza. Questo servizio coadiuva procedimenti penali o procedure amministrative relativi a siffatto materiale di propaganda.

Art. 10 Comunicazione di dati personali

1 Il SIC può comunicare i dati personali trattati nei suoi sistemi d'informazione alle autorità e agli uffici di cui all'allegato 3 dell'ordinanza del 4 dicembre 2009[4] sul Servizio delle attività informative della Confederazione (O-SIC), per gli scopi menzionati e alle condizioni stabilite in detto allegato.

4 RS **121.1**

2 Per quanto concerne la comunicazione dei dati all'estero sono applicabili:

a. per informazioni concernenti l'estero: gli articoli 5 capoverso 3 LSIC e 14 O-SIC;

b. per informazioni concernenti la Svizzera: l'articolo 17 capoversi 3–5 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 SIC informa il destinatario sull'attendibilità e l'attualità dei dati.

5 Il SIC rende attento il destinatario:

a. sullo scopo esclusivo per il quale il destinatario è autorizzato a utilizzare i dati comunicati;

b. sul fatto che il SIC si riserva il diritto di esigere informazioni sull'utilizzazione fatta dei dati comunicati.

6 Il SIC registra la comunicazione di dati del sistema ISIS, nonché il destinatario, l'oggetto e il motivo della comunicazione.

Art. 11 Copia di dati in altre collezioni di dati

1 I dati dei sistemi d'informazione del SIC non possono essere copiati in altre collezioni di dati né per il tramite di installazioni di comunicazione né per il tramite di supporti di dati.

2 Per procedere a valutazioni speciali è possibile trasferire per breve tempo i dati dei sistemi d'informazione del SIC in banche dati di lavoro. Tali dati devono essere distrutti dopo la conclusione delle valutazioni.

Art. 12 Distruzione dei dati

1 I dati sono distrutti entro tre mesi dalla scadenza della corrispondente durata di conservazione conformemente agli articoli 24 e 33.

2 Il direttore del SIC o il suo sostituto può decidere una proroga unica di tre anni del termine di conservazione di dati che, valutati i rischi e i pericoli attuali, risultano indispensabili per l'adempimento dei compiti legali del SIC.

3 Con la distruzione dell'ultima comunicazione (incluse le relazioni, le immagini e i mandati corrispondenti) sono cancellati l'intero insieme di dati nonché eventuali schede informative.

4 I dati destinati alla distruzione sono trasferiti nel modulo di archiviazione; è fatto salvo l'articolo 13 capoverso 2.

Art. 13 Archiviazione

1 Il SIC propone all'Archivio federale per l'archiviazione i dati e i documenti non più necessari o destinati alla distruzione.

2 Il SIC non propone per l'archiviazione dati e documenti classificati derivanti da relazioni dirette con servizi di sicurezza esteri o provenienti dalla ricerca di informazioni operativa. Esso conserva internamente tali dati e documenti d'intesa con l'Archivio federale e li distrugge dopo 45 anni.

3 Il SIC distrugge, unitamente ai corrispondenti documenti, i dati del modulo di archiviazione designati dall'Archivio federale come non degni di essere archiviati. Sono fatte salve le altre disposizioni legali in materia di distruzione dei dati.

Art. 14 Sicurezza dei dati e verbalizzazione automatica

1 Per la garanzia della sicurezza dei dati sono applicabili:

a. l'articolo 20 dell'ordinanza del 14 giugno 1993[5] relativa alla legge federale sulla protezione dei dati;

b. l'ordinanza del 26 settembre 2003[6] concernente l'informatica e la telecomunicazione nell'Amministrazione federale;

c. le condizioni stabilite dal DDPS conformemente all'articolo 28 per il collegamento degli organi cantonali incaricati di salvaguardare la sicurezza interna.

2 Il SIC disciplina in regolamenti per il trattamento dei dati:

a. le misure organizzative e tecniche intese a evitare il trattamento non autorizzato dei dati;

b. la verbalizzazione automatica dei dati immessi.

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

Art. 15 Responsabilità e competenze

1 Il SIC è responsabile dei propri sistemi d'informazione.

2 Esso emana i regolamenti per il trattamento dei dati.

3 Il settore Gestione delle informazioni del SIC è competente per la formazione e l'assistenza degli utenti e provvede all'applicazione dei regolamenti per il trattamento dei dati.

4 La responsabilità tecnica generale per i sistemi d'informazione del SIC compete al DDPS.

5 Il fornitore di prestazioni informatiche è responsabile della gestione, della manutenzione e della sicurezza.

6 Nel singolo caso il consulente per la protezione dei dati del SIC può verificare la conformità del trattamento dei dati nei sistemi d'informazione del SIC alle prescrizioni sulla protezione dei dati.

5 RS **235.11**
6 RS **172.010.58**

Art. 16 Requisiti tecnici

1 Il DDPS stabilisce i requisiti tecnici che devono essere soddisfatti dai terminali degli utenti.

2 I dettagli per ogni singolo sistema d'informazione sono stabiliti nei regolamenti per il trattamento dei dati.

Sezione 3:[7] Sistema d'informazione Sicurezza esterna (ISAS)

Art. 17 Esercizio pilota del sistema ISAS

1 Il sistema ISAS è gestito nel quadro di un esercizio pilota di durata limitata ai sensi dell'articolo 17*a* della legge federale del 19 giugno 1992[8] sulla protezione dei dati.

2 Il SIC presenta un rapporto di valutazione al Consiglio federale al più tardi due anni dopo l'attivazione del sistema ISAS.

3 Il Consiglio federale decide in merito al passaggio dall'esercizio pilota del sistema ISAS all'esercizio regolare.

4 Le disposizioni delle sezioni 1 e 2 (art. 1–16) sono applicabili all'esercizio pilota del sistema ISAS.

Art. 18 Banche dati

1 Il sistema ISAS si compone delle banche dati seguenti:

a. «Dati grezzi» (RD);
b. «Estremismo» (EX);
c. «Terrorismo» (TE);
d. «Non proliferazione» (NP);
e. «Attività informative» (ND);
f. «Questioni militari» (MI);
g. «Economia e risorse» (WR);
h. «Politica internazionale e questioni strategiche» (IPS);
i. «Documentazione» (DO).

2 Le banche dati contengono le seguenti informazioni concernenti l'estero rilevanti per l'adempimento dei compiti del SIC ai sensi dell'articolo 1 LSIC:

a. RD: dati OCR, in forma non strutturata o semistrutturata, che possono essere trattati in EX, TE, NP, ND, MI, WR, IPS e DO;
b. EX: informazioni in forma strutturata, su persone ed eventi, relative al settore dell'estremismo violento;

7 In vigore sino al 31 dic. 2014.
8 RS **235.1**

c. TE: informazioni in forma strutturata, su persone ed eventi, relative al settore del terrorismo;

d. NP: informazioni in forma strutturata, su persone ed eventi, relative al settore della non proliferazione; possono comprendere anche informazioni concernenti la Svizzera;

e. ND: informazioni in forma strutturata, su persone ed eventi, relative al settore dello spionaggio;

f. MI: informazioni in forma strutturata, su persone, eventi e cose, relative al settore delle questioni militari;

g. WR: informazioni in forma strutturata, su persone ed eventi, relative al settore dell'economia e delle risorse;

h. IPS: informazioni in forma strutturata, su persone ed eventi, relative al settore della politica internazionale e delle questioni strategiche;

i. DO: informazioni documentarie, su persone ed eventi, provenienti dalle attività preventive di protezione dello Stato nonché informazioni provenienti da fonti pubblicamente accessibili ai sensi dell'articolo 9.

Art. 19 Dati trattati

1 Le banche dati ISAS EX, TE, NP, ND, MI, WR, IPS e DO sono strutturate secondo le comunicazioni, gli oggetti e le relazioni.

2 Il DDPS disciplina i singoli campi di dati.

Art. 20 Autorizzazioni di consultazione

I collaboratori del SIC competenti per l'esercizio pilota possono consultare il sistema ISAS per quanto necessario per l'adempimento dei loro compiti legali.

Art. 21 Immissione dei dati e controllo della qualità

1 Nel sistema ISAS possono essere trattate soltanto informazioni corrispondenti agli scopi di cui all'articolo 3.

2 Il settore Analisi preventiva del SIC immette i dati nel sistema ISAS.

3 Nelle banche dati indicate di seguito sono inoltre autorizzate a immettere dati, e a determinare la categoria delle comunicazioni, le persone seguenti:

a. i collaboratori del settore ComCenter del SIC: dati per la banca dati RD;

b. i collaboratori del settore Valutazione del SIC: dati per le banche dati EX, TE, NP, ND, MI, WR, IPS e DO.

4 Il direttore del SIC o il suo sostituto può incaricare il settore Controllo della qualità ISIS di verificare le banche dati del sistema ISAS.

Art. 22 Deposito dei documenti

1 Nell'ambito del deposito di documenti devono essere garantite una gestione e un'archiviazione corrette dei documenti.

2 I documenti alla base degli oggetti e delle comunicazioni possono essere registrati in forma di dati OCR.

3 Se i documenti alla base degli oggetti e delle comunicazioni sono registrati in forma di dati OCR, si può rinunciare al deposito dei documenti in forma cartacea.

Art. 23 Diritto d'essere informati delle persone interessate

Il diritto d'essere informati è retto dalle disposizioni della legge federale del 19 giugno 1992[9] sulla protezione dei dati.

Art. 24 Durata di conservazione dei dati

1 I dati del sistema ISAS e i corrispondenti documenti possono essere conservati per 30 anni al massimo a decorrere dalla data del loro ultimo trattamento.

2 Il termine di conservazione massimo è di 45 anni.

Sezione 4: Sistema d'informazione Sicurezza interna (ISIS)

Art. 25 Sistemi e banche dati

1 Il sistema ISIS si compone dei sottosistemi e delle banche dati seguenti:

a. «ISIS00 Generale» con il deposito dei documenti, la gestione dei mandati, l'analisi dei rischi, la statistica e il modulo di archiviazione;

b. «ISIS01 Protezione dello Stato» con le banche dati:
   1. «Protezione dello Stato»,
   2. «Polizia amministrativa»,
   3. «Documentazione»,
   4. «Sistema numerico»;

c. «ISIS02 Amministrazione» con la banca dati «Amministrazione»;

d. «ISIS05 News» con le banche dati:
   1. «NEWS»,
   2. «ELIS»,
   3. «IPIS»,
   4. «Infopress»,
   5. «ISIS-Info»;

9 RS **235.1**

e. «ISIS06 Controlli di sicurezza relativi alle persone» con la banca dati «Controlli di sicurezza relativi alle persone»;

f. «ISIS07 Politica di sicurezza» con la banca dati «Politica di sicurezza».

2 Le banche dati contengono le seguenti informazioni concernenti la Svizzera rilevanti per l'adempimento dei compiti del SIC ai sensi dell'articolo 1 LSIC:

a. «Protezione dello Stato» (ST): informazioni su persone ed eventi, provenienti dalle attività preventive di protezione dello Stato;

b. «Polizia amministrativa» (VP): informazioni su persone ed eventi, provenienti dal settore degli uffici centrali di polizia amministrativa dell'Ufficio federale di polizia (fedpol);

c. «Documentazione» (DO): informazioni documentarie provenienti dalle attività preventive di protezione dello Stato nonché informazioni provenienti da fonti pubblicamente accessibili ai sensi dell'articolo 9;

d. «Sistema numerico» (NU): informazioni su eventi provenienti da programmi di ricerca selezionati;

e. «Amministrazione» (VE): informazioni necessarie per il controllo delle pratiche;

f. «NEWS»: comunicati stampa provenienti da Internet rilevanti ai fini della protezione dello Stato;

g. «ELIS»: descrizione in forma elettronica della situazione della sicurezza interna;

h. «IPIS»: comunicati di agenzie di stampa rilevanti ai fini della protezione dello Stato;

i. «Infopress»: analisi della stampa stilate quotidianamente dal SIC;

j. «ISIS-Info»: piattaforma d'informazione per gli utenti dell'ISIS;

k. «Controlli di sicurezza relativi alle persone» (PSP): informazioni necessarie per il controllo delle pratiche nell'ambito dei controlli di sicurezza relativi alle persone;

l. «ISIS07 Politica di sicurezza» (SIPOL): informazioni rilevanti in materia di politica di sicurezza concernenti l'esercito, l'economia, le risorse, la politica internazionale e questioni strategiche.

Art. 26 Dati trattati

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

2 Le banche dati del sistema ISIS sono strutturate in base alle comunicazioni, agli oggetti e alle relazioni.

3 Il DDPS disciplina i singoli campi di dati.

Art. 27 Autorizzazioni di consultazione

1 Per quanto necessario per l'adempimento dei rispettivi compiti legali, il sistema ISIS può essere consultato dalle autorità e dai servizi seguenti:

a. collaboratori del SIC e degli organi cantonali incaricati di salvaguardare la sicurezza interna; essi sono collegati al sistema per mezzo di una procedura di richiamo;
b. collaboratori del Servizio federale di sicurezza (SFS), della Polizia giudiziaria federale (PGF), della Cooperazione operativa di polizia, della Centrale operativa e del servizio di fedpol competente per l'emanazione di decisioni in merito a misure di respingimento ai sensi degli articoli 67 capoverso 2 e 68 della legge federale del 16 dicembre 2005[10] sugli stranieri; essi possono effettuare consultazioni brevi mediante una procedura di richiamo;
c.[11] collaboratori dei servizi competenti per i controlli di sicurezza relativi alle persone presso la Confederazione; essi possono effettuare consultazioni brevi mediante una procedura di richiamo.

2 Gli organi cantonali incaricati di salvaguardare la sicurezza interna non hanno accesso ai dati classificati provenienti da relazioni dirette con autorità di sicurezza estere.

Art. 28 Requisiti tecnici per il collegamento dei Cantoni

1 Il DDPS stabilisce i requisiti tecnici per il collegamento degli organi cantonali incaricati di salvaguardare la sicurezza interna.

2 Gli organi cantonali sono collegati al sistema ISIS non appena soddisfano detti requisiti.

Art. 29 Immissione dei dati e controllo della qualità

1 Nel sistema ISIS possono essere trattate soltanto informazioni corrispondenti agli scopi di cui all'articolo 3.

2 Il settore Analisi preventiva del SIC immette i dati nel sistema ISIS e determina la categoria delle comunicazioni.

3 Sono inoltre autorizzate a immettere i dati indicati di seguito, e a determinare la categoria delle comunicazioni, le persone seguenti:

a. i collaboratori del Servizio degli stranieri del SIC: dati provenienti dal controllo delle fotografie dei passaporti;
b. i collaboratori del settore Valutazione del SIC: schede informative;
c. i collaboratori del settore Controlli di sicurezza relativi alle persone: dati della banca dati PSP.

10 RS **142.20**
11 Nuovo testo giusta il n. 2 dell'all. 3 dell'O del 4 mar. 2011 sui controlli di sicurezza relativi alle persone, in vigore dal 1° apr. 2011 (RU **2011** 1031).

4 Le informazioni della banca dati ST sono in un primo tempo immesse provvisoriamente (codice «p») e, secondo la provenienza, il modo di trasmissione, il contenuto e le conoscenze già disponibili, valutate come segue:

a. con il codice «g» per le comunicazioni attendibili;

b. con il codice «u» per le comunicazioni poco attendibili.

5 Il settore Controllo della qualità ISIS verifica il contenuto delle registrazioni provvisorie, segnatamente l'indicazione delle fonti, la valutazione dell'informazione, la data della successiva valutazione globale e conferma la registrazione definitiva dei dati (codice «k»).

6 Il direttore del SIC o il suo sostituto può incaricare il settore Controllo della qualità ISIS di verificare le altre banche dati.

Art. 30 Deposito dei documenti

1 Nell'ambito del deposito di documenti devono essere garantite una gestione e un'archiviazione corrette dei documenti.

2 I documenti alla base degli oggetti e delle comunicazioni possono essere registrati in forma di dati OCR. Sono eccettuate le banche dati ST e PSP, nelle quali la registrazione dei documenti avviene unicamente in forma di immagini.

3 Se i documenti alla base degli oggetti e delle comunicazioni sono registrati in forma di dati OCR o di immagini, si può rinunciare al deposito dei documenti in forma cartacea.

Art. 31 Diritto d'essere informati delle persone interessate

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

Art. 32 Valutazione globale periodica dei dati nella banca dati ST

1 Il settore Controllo della qualità ISIS procede a una nuova valutazione globale di ciascun insieme di dati al più tardi cinque anni dopo la registrazione della prima comunicazione 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, le comunicazioni e gli oggetti registrati in un insieme di dati presentano un elevato grado di plausibilità e se i dati sono necessari per le ulteriori attività di protezione dello Stato.

3 Le comunicazioni e le relazioni memorizzate come poco attendibili da più di tre anni (codice «u») possono continuare a essere trattate come tali fino alla successiva valutazione globale soltanto se:

a. sono necessarie per l'adempimento dei compiti legali; e

b. il direttore del SIC o il suo sostituto ne ha autorizzato il trattamento.

4 In caso di utilizzazione ulteriore di dati ancora necessari ne va annotata la valutazione globale.

5 Gli oggetti che da più di tre anni sono contrassegnati come dati concernenti terzi sono cancellati in occasione della valutazione globale.

6 Il settore Controllo della qualità ISIS cancella i dati che non sono più necessari.

Art. 33 Durata di conservazione dei dati

1 Per quanto concerne i dati del sistema ISIS si applicano le seguenti durate massime di conservazione:

a. per i dati preventivi: 15 anni;

b. per i dati dei programmi di ricerca preventiva in corso: 20 anni;

c. per i dati concernenti divieti d'entrata: fino a 10 anni dopo la loro scadenza;

d. per dati provenienti da procedure di controllo di sicurezza relative alle persone: 5 anni;

e. per dati provenienti dalla corrispondenza con organi amministrativi: 30 anni;

f. per dati provenienti dalla corrispondenza con privati: 10 anni;

g. per i dati delle banche dati DO, NEWS, IPIS, Infopress e ISIS-Info: 45 anni.

2 Scaduta la durata di conservazione, i dati e i documenti sono distrutti.

Art. 34 Dati e documenti degli organi cantonali incaricati di salvaguardare la sicurezza interna

1 Gli organi cantonali incaricati di salvaguardare la sicurezza interna possono conservare dati e documenti, raccolti per conto della Confederazione nell'ambito della loro attività di protezione dello Stato, al massimo durante cinque anni.

2 Scaduta la durata di conservazione, i dati e i documenti sono distrutti.

Art. 35 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 propri apparecchi;

b. per l'installazione e la gestione della propria rete di distribuzione capillare.

Sezione 5: Disposizioni finali

Art. 36 Diritto previgente: abrogazione

L'ordinanza del 30 novembre 2001[12] sul sistema per il trattamento dei dati relativi alla protezione dello Stato è abrogata.

Art. 37 Entrata in vigore e validità

[1] La presente ordinanza entra in vigore il 1° gennaio 2010.

[2] Le disposizioni della sezione 3 (art. 17–24) si applicano sino al 31 dicembre 2014.

12 [RU **2001** 3173, **2004** 3495 4813 all. n. 2, **2006** 921, **2008** 4943 I 2 5525 all. 4 n. II 1 6305 all. n. 3]