Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Disegno

Legge federale sulla sicurezza delle informazioni in seno alla Confederazione

(Legge sulla sicurezza delle informazioni, LSIn)

del …

L'Assemblea federale della Confederazione Svizzera,

visti gli articoli 54 capoverso 1, 60 capoverso 1, 101, 102 capoverso 1 e 173 capoverso 1 lettere a e b nonché capoverso 2 della Costituzione federale[1];
visto il messaggio del Consiglio federale del 22 febbraio 2017[2],

decreta:

Capitolo 1: Disposizioni generali

Art. 1 Scopo

1 La presente legge ha lo scopo di garantire la sicurezza del trattamento delle informazioni di competenza della Confederazione nonché la sicurezza dei mezzi informatici della Confederazione.

2 Mira in tal modo a tutelare gli interessi pubblici seguenti:

a. la capacità di decisione e d'azione delle autorità e delle organizzazioni della Confederazione;

b. la sicurezza interna ed esterna della Svizzera;

c. gli interessi in materia di politica estera della Svizzera;

d. gli interessi in materia di politica economica, finanziaria e monetaria della Svizzera;

e. l'adempimento degli obblighi legali e contrattuali delle autorità e delle organizzazioni della Confederazione concernenti la protezione di informazioni.

RS …
1 RS **101**
2 FF **2017** 2563

Art. 2 Autorità e organizzazioni assoggettate

1 La presente legge si applica alle autorità seguenti (autorità assoggettate):

a. all'Assemblea federale;

b. al Consiglio federale;

c. ai tribunali della Confederazione;

d. al Ministero pubblico della Confederazione e alla sua autorità di vigilanza;

e. alla Banca nazionale svizzera.

2 Si applica alle organizzazioni seguenti (organizzazioni assoggettate):

a. ai Servizi del Parlamento;

b. all'Amministrazione federale;

c. alle amministrazioni dei tribunali della Confederazione;

d. all'esercito;

e. alle organizzazioni di cui all'articolo 2 capoverso 4 della legge del 21 marzo 1997[3] sull'organizzazione del Governo e dell'Amministrazione (LOGA), per i loro compiti amministrativi.

3 Il Consiglio federale può limitare il campo d'applicazione della presente legge alle organizzazioni di cui all'articolo 2 capoverso 3 e 4 LOGA che:

a. esercitano attività sensibili sotto il profilo della sicurezza; o

b. impiegano o accedono a mezzi informatici della Confederazione per adempiere i loro compiti.

4 Può limitare a talune disposizioni della presente legge il campo d'applicazione secondo il capoverso 3. Al riguardo, tiene conto dell'autonomia esecutiva delle organizzazioni interessate in virtù delle rispettive disposizioni organizzative.

5 Alle organizzazioni di diritto pubblico e privato che gestiscono infrastrutture critiche, ma che non sono contemplate ai capoversi 1–3, si applicano gli articoli 75–81 della presente legge. La legislazione speciale può dichiarare applicabili altre disposizioni della presente legge.

Art. 3 Applicabilità ai Cantoni

1 Le disposizioni concernenti le informazioni classificate e la sicurezza dei mezzi informatici si applicano ai Cantoni qualora trattino informazioni classificate della Confederazione o accedano a mezzi informatici di quest'ultima nel quadro della loro collaborazione con la Confederazione o dell'esecuzione del diritto federale.

2 Le disposizioni non si applicano quando i Cantoni garantiscono una sicurezza delle informazioni almeno equivalente.

3 RS **172.010**

Art. 4 Rapporto con altre leggi federali

1 La legge del 17 dicembre 2004[4] sulla trasparenza prevale sulla presente legge.

2 Nel caso di informazioni la cui protezione è parimenti disciplinata in altre leggi federali, le disposizioni della presente legge si applicano a titolo completivo.

Art. 5 Definizioni

Ai sensi della presente legge si intende per:

a. *mezzi informatici:* mezzi delle tecnologie dell'informazione e della comunicazione, segnatamente applicazioni, sistemi d'informazione e collezioni di dati nonché impianti, prodotti e servizi che servono all'elaborazione elettronica di informazioni;

b. *attività sensibile sotto il profilo della sicurezza:*
   1. il trattamento di informazioni classificate «confidenziale» o «segreto»,
   2. l'amministrazione, l'esercizio, la manutenzione e la verifica di mezzi informatici del livello di sicurezza «protezione elevata» oppure «protezione molto elevata»,
   3. l'accesso a zone di sicurezza, in particolare alle zone di protezione 2 o 3 di un impianto secondo la legislazione sulla protezione di impianti militari;

c. *infrastrutture critiche:* infrastrutture d'informazione, di comunicazione, energetiche, dei trasporti e altre infrastrutture indispensabili per il funzionamento della società, dell'economia e dello Stato.

Capitolo 2: Misure generali

Sezione 1: Principi

Art. 6 Sicurezza delle informazioni

1 Le autorità e organizzazioni assoggettate provvedono affinché le necessità di protezione delle informazioni per le quali sono competenti siano valutate sotto il profilo di un eventuale pregiudizio degli interessi di cui all'articolo 1 capoverso 2.

2 Provvedono affinché, conformemente alle rispettive necessità di protezione, tali informazioni:

a. siano accessibili soltanto alle persone autorizzate (confidenzialità);

b. siano disponibili quando sono necessarie (disponibilità);

c. non possano essere modificate senza autorizzazione o per inavvertenza (integrità);

d. siano trattate in maniera documentabile (tracciabilità).

4 RS **152.3**

3 Provvedono affinché i mezzi informatici che esse impiegano per l'adempimento dei loro compiti legali siano protetti dall'utilizzazione abusiva e dai disturbi.

4 Al riguardo, tengono conto dei principi di adeguatezza, economicità e praticità.

Art. 7 Responsabilità direttiva suprema

1 Le autorità assoggettate provvedono, nel rispettivo ambito di competenza, affinché la sicurezza delle informazioni sia organizzata, applicata e verificata secondo lo stato della scienza e della tecnica.

2 Stabiliscono:

a. i loro obiettivi in materia di sicurezza delle informazioni;

b. i parametri per la gestione dei rischi;

c. le conseguenze in caso di inosservanza delle prescrizioni.

Art. 8 Gestione dei rischi

1 Le autorità e organizzazioni assoggettate provvedono affinché nel loro ambito di competenza i rischi per la sicurezza delle informazioni siano costantemente valutati.

2 Adottano le misure necessarie per evitare i rischi o ridurli a un livello sostenibile.

3 I rischi considerati sostenibili devono essere formalmente accettati.

Art. 9 Collaborazione con terzi

1 Le autorità e le organizzazioni assoggettate che collaborano con terzi provvedono affinché i requisiti e le misure secondo la presente legge siano iscritti nelle convenzioni e nei contratti corrispondenti.

2 Provvedono a un'adeguata verifica dell'applicazione delle misure.

Art. 10 Procedura in caso di violazioni della sicurezza delle informazioni

1 Le autorità e organizzazioni assoggettate provvedono affinché le violazioni della sicurezza delle informazioni siano individuate tempestivamente, le loro cause accertate e le eventuali ripercussioni minimizzate.

2 Le autorità assoggettate provvedono affinché siano allestite pianificazioni preventive in vista di eventuali violazioni gravi della sicurezza delle informazioni, tali da compromettere l'adempimento di compiti indispensabili della Confederazione, e siano svolte le corrispondenti esercitazioni.

Sezione 2: Classificazione delle informazioni

Art. 11 Principi della classificazione

1 Le autorità e organizzazioni assoggettate provvedono affinché le informazioni che soddisfano i criteri di cui all'articolo 13 siano classificate.

2 La classificazione è limitata al minimo indispensabile e deve essere per quanto possibile limitata nel tempo.

Art. 12 Competenze

1 Le autorità assoggettate stabiliscono quali persone e servizi sono competenti per la classificazione delle informazioni (servizio incaricato della classificazione).

2 Le classificazioni possono essere modificate o soppresse soltanto dal servizio incaricato della classificazione o dal servizio al quale esso è subordinato.

3 Il Consiglio federale disciplina la declassificazione degli archivi.

Art. 13 Livelli di classificazione

1 Sono classificate «ad uso interno» le informazioni la cui conoscenza da parte di persone non autorizzate può pregiudicare gli interessi di cui all'articolo 1 capoverso 2 lettere a–d.

2 Sono classificate «confidenziale» le informazioni la cui conoscenza da parte di persone non autorizzate può pregiudicare considerevolmente gli interessi di cui all'articolo 1 capoverso 2 lettere a–d.

3 Sono classificate «segreto» le informazioni la cui conoscenza da parte di persone non autorizzate può pregiudicare gravemente gli interessi di cui all'articolo 1 capoverso 2 lettere a–d.

4 La menzione della classificazione è scritta in lettere maiuscole.

Art. 14 Accesso a informazioni classificate

1 Ottengono l'accesso a informazioni classificate soltanto le persone che offrono la garanzia di gestirle in modo appropriato e:

a. necessitano delle informazioni per l'adempimento di un compito legale; o

b. beneficiano di un'autorizzazione di accesso convenuta contrattualmente e necessitano delle informazioni per l'adempimento dei compiti loro affidati.

2 L'accesso ad archivi classificati è retto dalle disposizioni della legislazione in materia di archiviazione.

3 Sono fatte salve le limitazioni di accesso disciplinate da trattati internazionali secondo l'articolo 88.

Art. 15 Accesso a informazioni classificate disciplinato da procedure particolari

1 L'accesso a informazioni classificate in seno all'Assemblea federale, ai Servizi del Parlamento, ai tribunali e ai ministeri pubblici è retto dal rispettivo diritto procedurale applicabile.

2 Prima della decisione di concedere l'accesso a un'informazione secondo il capoverso 1, l'organo parlamentare o il tribunale competente può consultare il servizio incaricato della classificazione.

Sezione 3: Sicurezza in occasione dell'impiego di mezzi informatici

Art. 16 Procedura di sicurezza

1 Le autorità assoggettate stabiliscono una procedura per garantire la sicurezza delle informazioni in occasione dell'impiego di mezzi informatici (procedura di sicurezza).

2 La procedura di sicurezza comprende in particolare:

a. la valutazione della necessità di protezione delle informazioni prima dell'impiego di mezzi informatici;

b. l'applicazione delle misure di sicurezza e la relativa verifica;

c. la determinazione della competenza per il nullaosta di sicurezza relativo ai mezzi informatici;

d. la procedura in caso di mutamento dei rischi.

3 Per l'esecuzione della procedura di sicurezza è competente l'autorità o l'organizzazione assoggettata che decide l'impiego dei mezzi informatici.

Art. 17 Livelli di sicurezza

1 Il livello di sicurezza «protezione di base» si applica a tutti i mezzi informatici, salvo a quelli che devono essere attribuiti a un livello di sicurezza più elevato.

2 Ai mezzi informatici si applica il livello di sicurezza «protezione elevata» se:

a. una violazione della confidenzialità, della disponibilità, dell'integrità o della tracciabilità delle informazioni che trattano può pregiudicare considerevolmente gli interessi di cui all'articolo 1 capoverso 2;

b. l'utilizzazione abusiva o il disturbo di tali mezzi informatici può pregiudicare considerevolmente gli interessi di cui all'articolo 1 capoverso 2.

3 Ai mezzi informatici si applica il livello di sicurezza «protezione molto elevata» se:

a. una violazione della confidenzialità, della disponibilità, dell'integrità o della tracciabilità delle informazioni che trattano può pregiudicare gravemente gli interessi di cui all'articolo 1 capoverso 2; o

b. l'utilizzazione abusiva o il disturbo di tali mezzi informatici può pregiudicare gravemente gli interessi di cui all'articolo 1 capoverso 2.

Art. 18 Misure di sicurezza

1 Le autorità assoggettate stabiliscono i requisiti minimi per i livelli di sicurezza di cui all'articolo 17.

2 Tutti i mezzi informatici devono soddisfare i requisiti minimi del livello di sicurezza «protezione di base».

3 L'efficacia delle misure per i mezzi informatici del livello di sicurezza «protezione molto elevata» deve essere verificata periodicamente.

Art. 19 Sicurezza durante l'esercizio

1 Le autorità e organizzazioni assoggettate garantiscono la sicurezza dei mezzi informatici che gestiscono per loro stesse o su mandato di un'altra autorità o organizzazione.

2 Il trattamento di dati personali nell'ambito della sorveglianza delle reti è retto per analogia dagli articoli 57*i*–57*q* LOGA[5].

Sezione 4: Misure in materia di personale

Art. 20 Condizioni per l'accesso a informazioni e mezzi informatici della Confederazione

1 Le autorità e organizzazioni assoggettate provvedono affinché le persone che hanno accesso a informazioni, mezzi informatici, locali e altre infrastrutture della Confederazione:

a. siano scelte con cura;

b. siano identificate in funzione dei rischi;

c. siano formate e frequentino formazioni continue conformi al rispettivo livello;

d. se necessario, siano tenute a mantenere il segreto.

2 Possono impiegare metodi di verifica biometrici se è necessario per l'identificazione delle persone in funzione dei rischi. I dati biometrici sono distrutti al decadere dell'autorizzazione d'accesso.

Art. 21 Rilascio restrittivo di autorizzazioni

1 Le autorità e organizzazioni assoggettate provvedono affinché le autorizzazioni d'accesso a informazioni, mezzi informatici, locali e altre infrastrutture della Confederazione siano rilasciate soltanto alle persone che ne hanno bisogno per l'adempimento dei loro compiti.

5 RS **172.010**

2 Le autorizzazioni sono revocate non appena termina il rapporto di lavoro o il contratto oppure quando il compito è adempiuto. Possono essere bloccate o revocate senza preavviso se sussistono indizi concreti di un pericolo per la sicurezza.

Sezione 5: Protezione fisica

Art. 22 Principio

Le autorità e organizzazioni assoggettate provvedono a una protezione fisica adeguata delle informazioni e dei mezzi informatici di cui sono responsabili contro le utilizzazioni abusive e i disturbi.

Art. 23 Zone di sicurezza

1 Le autorità e organizzazioni assoggettate possono designare come zone di sicurezza locali e settori nei quali:

a. vengono trattate frequentemente informazioni classificate «confidenziale» o «segreto»; o

b. sono impiegati mezzi informatici del livello di sicurezza «protezione elevata» o «protezione molto elevata».

2 Sono autorizzate a:

a. proibire che siano portati con sé determinati oggetti, in particolare apparecchi per registrazioni audiovisive;

b. sorvegliare settori sensibili sotto il profilo della sicurezza con apparecchi per registrazioni audiovisive;

c. eseguire perquisizioni di oggetti e persone;

d. eseguire senza preavviso controlli di locali, anche in assenza degli impiegati.

3 In zone di sicurezza nelle quali sono trattate frequentemente informazioni classificate «segreto» oppure sono impiegati mezzi informatici del livello di sicurezza «protezione molto elevata», le autorità e organizzazioni assoggettate possono esercitare impianti di telecomunicazione che provocano interferenze secondo l'articolo 34 capoverso 1ter della legge del 30 aprile 1997[6] sulle telecomunicazioni (LTC).

4 Sono fatte salve le prescrizioni particolari per le zone di sicurezza conformemente ai trattati internazionali secondo l'articolo 88 nonché le prescrizioni per le zone di protezione di impianti secondo la legislazione sulla protezione di impianti militari.

6 RS **784.10**

Sezione 6: Sistemi di gestione delle identità

Art. 24 Impiego di sistemi di gestione delle identità

1 Ai fini della gestione centralizzata dei dati per l'identificazione delle persone che hanno accesso a informazioni, mezzi informatici, locali e altre infrastrutture, le autorità assoggettate possono gestire appositi sistemi d'informazione (sistemi di gestione delle identità).

2 I sistemi di gestione delle identità verificano l'identità e le caratteristiche relative alle autorizzazioni di persone, macchine e sistemi. Trasmettono il risultato ai sistemi d'informazione collegati affinché possano accertare le autorizzazioni.

3 Le autorità assoggettate designano un servizio responsabile per ogni sistema di gestione delle identità.

Art. 25 Scambio e armonizzazione dei dati

1 I sistemi di gestione delle identità possono scambiare e armonizzare dati con sistemi d'informazione collegati, registri del personale e degli utenti nonché altri sistemi di gestione delle identità di autorità assoggettate.

2 Lo scambio e l'armonizzazione sono limitati ai dati che possono essere trattati nel rispettivo sistema.

Art. 26 Utilizzo del numero d'assicurato AVS

1 Ai fini della corretta attribuzione nel quadro dell'armonizzazione di dati personali, il servizio responsabile può utilizzare temporaneamente nel sistema di gestione delle identità il numero d'assicurato di cui all'articolo 50*c* della legge federale del 20 dicembre 1946[7] su l'assicurazione per la vecchiaia e per i superstiti (numero d'assicurato AVS), allo scopo di generare da detto numero un numero personale secondo una procedura unidirezionale e irreversibile.

2 Il numero d'assicurato AVS è cancellato immediatamente dopo la generazione del numero personale.

Art. 27 Disposizioni esecutive

Le autorità assoggettate emanano disposizioni esecutive concernenti in particolare:

a. la protezione e la sicurezza dei dati;
b. i dati personali trattati;
c. lo scambio e l'armonizzazione di dati con altri sistemi;
d. la verbalizzazione e la trasmissione dei relativi dati ai sistemi d'informazione collegati;
e. il controllo periodico del trattamento dei dati personali da parte di un organo esterno.

7 RS **831.10**

Capitolo 3: Controllo di sicurezza relativo alle persone
Sezione 1: Disposizioni generali

Art. 28 Scopo e contenuto del controllo

1 Il controllo di sicurezza relativo alle persone serve a valutare se sussiste un rischio per la sicurezza delle informazioni qualora una persona, nel quadro della sua funzione o di un mandato, eserciti un'attività sensibile sotto il profilo della sicurezza.

2 A tal fine vengono trattati dati rilevanti per la sicurezza concernenti la condotta di vita della persona da controllare, in particolare le sue relazioni personali strette e quelle familiari, la sua situazione finanziaria e i suoi rapporti con l'estero.

3 I dati concernenti l'esercizio dei diritti costituzionali possono essere trattati unicamente qualora sussista un sospetto concreto che la persona da controllare si serva dell'esercizio di tali diritti per dissimulare la preparazione o l'esecuzione di attività che potrebbero pregiudicare considerevolmente gli interessi di cui all'articolo 1 capoverso 2.

Art. 29 Elenco delle funzioni

1 Le autorità assoggettate emanano, per il rispettivo ambito di competenza, un elenco delle funzioni che richiedono l'esercizio di un'attività sensibile sotto il profilo della sicurezza.

2 Verificano periodicamente la correttezza dell'elenco e lo adeguano.

Art. 30 Persone da controllare

1 Sono sottoposte a un controllo di sicurezza relativo alle persone:

a. le persone che esercitano una funzione prevista in un elenco secondo l'articolo 29;

b. gli impiegati di un Cantone che esercitano un'attività sensibile sotto il profilo della sicurezza nel quadro della collaborazione con la Confederazione o dell'esecuzione del diritto federale;

c. le persone che eseguono per un'autorità o organizzazione assoggettata un mandato che implica l'esercizio di un'attività sensibile sotto il profilo della sicurezza;

d. le persone che devono essere sottoposte a un controllo di sicurezza in virtù di un trattato internazionale secondo l'articolo 88.

2 Se un'autorità estera o un'organizzazione internazionale intende affidare a una persona l'esercizio di un'attività sensibile sotto il profilo della sicurezza, detta persona è sottoposta a un controllo di sicurezza se la Svizzera ha concluso con lo Stato o l'organizzazione internazionale interessati un trattato internazionale secondo l'articolo 88.

3 Le persone che esercitano una funzione che non figura ancora in un elenco secondo l'articolo 29 possono essere sottoposte in via eccezionale a un controllo di sicurezza,

previo consenso dell'autorità assoggettata. L'elenco in questione deve essere adeguato al più presto.

4 I candidati alle seguenti funzioni non sono assoggettati al controllo di sicurezza relativo alle persone:

a. membro dell'Assemblea federale;
b. membro del Consiglio federale o cancelliere della Confederazione;
c. giudice di un tribunale della Confederazione;
d. procuratore generale della Confederazione;
e. membro dell'autorità di vigilanza sul Ministero pubblico della Confederazione;
f. generale;
g. membro di un governo cantonale o giudice di un tribunale cantonale.

Art. 31 Livelli di controllo

Le autorità assoggettate attribuiscono le attività sensibili sotto il profilo della sicurezza a uno dei livelli di controllo seguenti:

a. controllo di sicurezza di base: per le attività sensibili sotto il profilo della sicurezza il cui esercizio contrario alle prescrizioni o non appropriato può pregiudicare considerevolmente gli interessi di cui all'articolo 1 capoverso 2;
b. controllo di sicurezza ampliato: per le attività sensibili sotto il profilo della sicurezza il cui esercizio contrario alle prescrizioni o non appropriato può pregiudicare gravemente gli interessi di cui all'articolo 1 capoverso 2.

Sezione 2: Esecuzione

Art. 32 Servizi competenti

1 Le autorità assoggettate e i Cantoni designano i servizi competenti per:

a. l'avvio dei controlli di sicurezza relativi alle persone (servizi promotori);
b. la decisione in merito all'esercizio dell'attività sensibile sotto il profilo della sicurezza (servizi decidenti).

2 Per l'esecuzione dei controlli di sicurezza relativi alle persone il Consiglio federale istituisce uno o più servizi specializzati (servizi specializzati CSP). Nella loro valutazione essi non sono vincolati a istruzioni.

Art. 33 Consenso e collaborazione

1 I controlli di sicurezza relativi alle persone possono essere eseguiti unicamente con il consenso della persona da controllare.

2 Le persone soggette all'obbligo di leva, i militari e i militi della protezione civile possono essere sottoposti al controllo di sicurezza senza il loro consenso.

3 La persona da controllare è tenuta a collaborare all'accertamento dei fatti.

Art. 34 Momento del controllo di sicurezza relativo alle persone

1 Per le persone di cui all'articolo 30 capoverso 1 lettere a e b, il controllo di sicurezza dev'essere avviato prima del conferimento della funzione.

2 Per le persone di cui all'articolo 30 capoverso 1 lettera a che devono essere proposte al Consiglio federale per la nomina, il controllo di sicurezza dev'essere concluso prima che la persona sia proposta per la nomina.

3 Per le persone di cui all'articolo 30 capoverso 1 lettera c, il controllo di sicurezza dev'essere concluso prima che sia affidato loro l'esercizio dell'attività sensibile sotto il profilo della sicurezza.

4 Per le persone di cui all'articolo 30 capoverso 1 lettera d, il controllo di sicurezza ha luogo nel momento previsto dal corrispondente trattato.

Art. 35 Acquisizione dei dati

1 Per il controllo di sicurezza di base, il servizio specializzato CSP competente può acquisire dati sulla persona da controllare dalle fonti seguenti:

a. dal casellario giudiziale;
b. presso le autorità penali, tramite richiesta di informazioni e atti su procedimenti penali in corso, conclusi o abbandonati;
c. presso gli organi di sicurezza della Confederazione, il Servizio delle attività informative della Confederazione (SIC), gli organi dell'esercito nonché altri organi della Confederazione, sempre che trattino dati necessari per la valutazione del rischio per la sicurezza;
d. dai registri e dagli atti degli organi di sicurezza dei Cantoni e della polizia;
e. dai registri delle autorità di esecuzione e fallimento;
f. dagli atti di controlli di sicurezza relativi alle persone precedenti;
g. da fonti pubblicamente accessibili.

2 Per il controllo di sicurezza ampliato, può inoltre acquisire dati dalle fonti seguenti:

a. presso le autorità fiscali federali e cantonali;
b. dai registri dei controlli degli abitanti;
c. presso istituti finanziari e banche con i quali la persona da controllare intrattiene relazioni d'affari;
d. mediante l'audizione della persona da controllare.

3 Se dai dati acquisiti risultano indizi concreti di un rischio per la sicurezza oppure se per la valutazione non sono disponibili dati sufficienti relativi a un periodo di tempo adeguato, il servizio specializzato CSP può procedere all'audizione della

persona da controllare. Con il suo consenso può procedere anche all'audizione di terzi; indica a detti terzi che rilasciano informazioni a titolo volontario.

4 I dati relativi a terzi che sono indissolubilmente connessi con dati relativi alla persona da controllare possono essere trattati unicamente se è indispensabile per la valutazione del rischio per la sicurezza. Il servizio specializzato CSP informa i terzi interessati in merito a tale trattamento.

Art. 36 Assistenza amministrativa

1 Se i dati devono essere acquisiti presso un'autorità estera o un'organizzazione internazionale, ciò avviene tramite l'autorità o l'organizzazione competente secondo l'articolo 35.

2 Se dai dati acquisiti risultano indizi concreti concernenti la criminalità organizzata o internazionale, il servizio specializzato CSP consulta gli uffici centrali di polizia giudiziaria della Confederazione. Tali uffici comunicano al servizio specializzato CSP unicamente dati personali rilevanti sotto il profilo della sicurezza.

Art. 37 Assunzione dei costi

1 Le autorità e organizzazioni di diritto pubblico presso le quali è consentito acquisire dati o che devono collaborare alla procedura sono tenute a collaborare gratuitamente.

2 Se per terzi la collaborazione implica un onere considerevole, essi sono indennizzati.

3 La Confederazione si assume le spese dei controlli di sicurezza degli impiegati dei Cantoni di cui all'articolo 30 capoverso 1 lettera b.

Art. 38 Abbandono della procedura

1 Il servizio specializzato CSP abbandona la procedura di controllo se la persona da controllare revoca il suo consenso o non entra più in considerazione per la funzione o il mandato.

2 Comunica l'abbandono della procedura di controllo alla persona interessata e al servizio promotore. La persona interessata è di conseguenza considerata non controllata.

Sezione 3: Valutazione del rischio per la sicurezza

Art. 39 Rischio per la sicurezza

1 Sussiste un rischio per la sicurezza se, sulla base dei dati acquisiti, vi sono indizi concreti che la persona controllata con elevata probabilità eserciterà in maniera contraria alle prescrizioni o non appropriata l'attività sensibile sotto il profilo della sicurezza.

2 La probabilità di un esercizio contrario alle prescrizioni o non appropriato dell'attività sensibile sotto il profilo della sicurezza può essere considerata elevata in particolare quando sussistono indizi concreti relativi alle caratteristiche personali seguenti:

a. mancanza di integrità personale o di affidabilità;

b. ricattabilità o corruttibilità; o

c. facoltà di giudizio o di decisione compromessa.

3 Il rischio per la sicurezza deve fondarsi, a prescindere dalla colpa della persona sottoposta al controllo, su circostanze oggettive inerenti alla situazione personale di questa.

Art. 40 Risultato della valutazione

1 Quale risultato della valutazione, il servizio specializzato CSP rilascia una delle dichiarazioni sottostanti, avente il significato indicato di seguito:

a. dichiarazione di sicurezza: non sussiste alcun rischio per la sicurezza;

b. dichiarazione di sicurezza con riserva: sussiste un rischio per la sicurezza che può essere ridotto a un livello sostenibile definendo determinate condizioni. Il servizio specializzato CSP raccomanda tali condizioni;

c. dichiarazione di rischio: sussiste un rischio per la sicurezza;

d. dichiarazione di constatazione: per la valutazione del rischio per la sicurezza non sono disponibili dati in quantità sufficiente relativi a un periodo di tempo adeguato.

2 Prima del rilascio di una dichiarazione secondo il capoverso 1 lettere b–d, il servizio specializzato CSP offre alla persona sottoposta al controllo la possibilità di esprimersi al riguardo.

Art. 41 Comunicazione

1 Il servizio specializzato CSP comunica per scritto la sua dichiarazione alla persona controllata e al servizio decidente.

2 Nel caso di persone sottoposte alla nomina da parte del Consiglio federale, il servizio specializzato CSP comunica la sua dichiarazione al dipartimento proponente.

3 Può comunicare la sua dichiarazione a un altro servizio decidente se la persona controllata:

a. è soggetta a un controllo di sicurezza relativo alle persone secondo la presente legge per un'altra attività sensibile sotto il profilo della sicurezza;

b. è soggetta a una verifica dell'affidabilità secondo un'altra legge federale;

c. in quanto militare è soggetta a una valutazione secondo l'articolo 113 della legge militare del 3 febbraio 1995[8].

8 RS **510.10**

4 Se già prima della conclusione della valutazione il servizio specializzato CSP dispone di indizi concreti secondo i quali potrebbe sussistere un rischio per la sicurezza, può informare per scritto in merito alle constatazioni provvisorie i servizi di cui ai capoversi 1–3 nonché la persona sottoposta al controllo.

Sezione 4: Conseguenze della dichiarazione

Art. 42 Esercizio dell'attività sensibile sotto il profilo della sicurezza

1 Le dichiarazioni dei servizi specializzati CSP hanno carattere di raccomandazione.

2 Il servizio decidente stabilisce, sulla base della dichiarazione, se la persona controllata può esercitare l'attività sensibile sotto il profilo della sicurezza.

3 Può vincolare l'esercizio dell'attività sensibile sotto il profilo della sicurezza a determinate condizioni.

4 Comunica la propria decisione al servizio specializzato CSP.

Art. 43 Utilizzo molteplice di una dichiarazione

È possibile rinunciare all'esecuzione del controllo di sicurezza relativo alle persone se alla persona interessata è già stata rilasciata una dichiarazione per un livello di controllo almeno equivalente:

a. per un'altra attività sensibile sotto il profilo della sicurezza secondo la presente legge;

b. nel quadro di una verifica dell'affidabilità secondo un'altra legge federale.

Art. 44 Ripetizione

1 Il controllo di sicurezza relativo alle persone è ripetuto come segue:

a. il controllo di sicurezza di base: al più presto dopo cinque e al più tardi dopo dieci anni;

b. il controllo di sicurezza ampliato: al più presto dopo tre e al più tardi dopo cinque anni.

2 Il Consiglio federale può rinunciare alla ripetizione del controllo di sicurezza di base per quanto riguarda determinate funzioni dell'esercito e della protezione civile.

3 Se il servizio promotore o il servizio decidente ha motivo di presumere che dall'ultimo controllo sono emersi nuovi rischi, può chiedere al servizio specializzato CSP competente, con motivazione scritta, la ripetizione del controllo di sicurezza relativo alle persone.

Art. 45 Tutela giurisdizionale

1 Dopo aver ricevuto la dichiarazione secondo l'articolo 40 capoverso 1, la persona controllata ha 30 giorni di tempo per:

a. consultare i documenti del controllo;

b. esigere la rettifica di dati errati o la distruzione di dati non più attuali;

c. far apporre una menzione di contestazione.

2 La restrizione del diritto d'accesso è retta dall'articolo 9 della legge federale del 19 giugno 1992[9] sulla protezione dei dati (LPD).

3 La dichiarazione costituisce un atto materiale secondo l'articolo 25*a* della legge federale del 20 dicembre 1968[10] sulla procedura amministrativa. La persona controllata può interporre ricorso contro una dichiarazione secondo l'articolo 40 capoverso 1 lettere b–d presso il Tribunale amministrativo federale entro 30 giorni dalla sua comunicazione.

4 Se il Tribunale federale o il Tribunale amministrativo federale sono il servizio decidente, si applica per analogia l'articolo 36 capoversi 2 e 4 della legge del 24 marzo 2000[11] sul personale federale.

5 Del rimanente, la procedura di ricorso è retta dalle disposizioni generali sull'amministrazione della giustizia federale.

Sezione 5: Trattamento di dati personali

Art. 46 Sistema d'informazione per i controlli di sicurezza relativi alle persone

1 I servizi specializzati CSP gestiscono un sistema d'informazione per l'esecuzione dei controlli di sicurezza relativi alle persone.

2 Ciascun servizio specializzato CSP è responsabile della liceità del trattamento dei dati personali contenuti nel sistema d'informazione.

3 Nel sistema d'informazione possono essere trattati dati personali degni di particolare protezione e profili della personalità secondo l'articolo 3 lettere c e d LPD[12], sempre che sia necessario per la valutazione del rischio per la sicurezza.

4 Il sistema d'informazione contiene i dati e le indicazioni seguenti:

a. dati sull'identità delle persone da sottoporre al controllo o controllate, compreso il numero d'assicurato AVS e il numero del passaporto;

b. i dati secondo gli articoli 35 e 36;

c. la valutazione del rischio per la sicurezza;

d. la dichiarazione secondo l'articolo 40 capoverso 1;

e. la decisione del servizio decidente;

9 RS **235.1**
10 RS **172.021**
11 RS **172.220.1**
12 RS **235.1**

f. dati e atti di procedure di ricorso;

g. elenchi e statistiche che contengono dati secondo le lettere a–f.

5 Se dati secondo il capoverso 4 vengono trattati all'esterno del sistema d'informazione, ciò dev'essere menzionato nel sistema d'informazione.

6 I dati secondo il capoverso 4 possono essere acquisiti automaticamente e sistematicamente mediante interrogazione dei seguenti sistemi d'informazione:

a. casellario giudiziale informatizzato VOSTRA conformemente agli articoli 365–371*a* del Codice penale[13];

b. registro nazionale di polizia di cui all'articolo 17 della legge federale del 13 giugno 2008[14] sui sistemi d'informazione di polizia della Confederazione;

c. INDEX SIC di cui all'articolo 51 della legge federale del 25 settembre 2015[15] sulle attività informative.

Art. 47 Diritti d'accesso e comunicazione dei dati

1 I servizi seguenti hanno accesso, mediante procedura di richiamo, ai dati contenuti nel sistema d'informazione menzionati qui appresso:

a. servizi promotori: ai dati di cui all'articolo 46 capoverso 4 lettera b che hanno registrato essi stessi in occasione dell'avvio del controllo nonché ai dati di cui all'articolo 46 capoverso 4 lettere a, d ed e;

b. servizi decidenti: ai dati di cui all'articolo 46 capoverso 4 lettere a, d ed e;

c. incaricati della sicurezza delle informazioni secondo l'articolo 82 per l'adempimento dei loro compiti di controllo: ai dati di cui all'articolo 46 capoverso 4 lettere a, d ed e;

d. servizi della Confederazione e dei Cantoni presso i quali vengono acquisiti dati secondo l'articolo 38: ai dati di cui all'articolo 46 capoverso 4 lettera a.

2 I servizi seguenti hanno accesso, tramite un'interfaccia, ai dati nel sistema d'informazione menzionati qui appresso:

a. il servizio specializzato di cui all'articolo 52 capoverso 2 per l'esecuzione della procedura di sicurezza relativa alle aziende secondo gli articoli 50–74, tramite il sistema d'informazione di cui all'articolo 71: ai dati di cui all'articolo 46 capoverso 4 lettere a, d ed e;

b. l'Aggruppamento Difesa:

1. per l'adempimento dei suoi compiti secondo l'articolo 13 della legge federale del 3 ottobre 2008[16] sui sistemi d'informazione militari (LSIM), tramite il sistema di gestione del personale dell'esercito di cui

13 RS **311.0**
14 RS **361**
15 RS **121**
16 RS **510.91**

all'articolo 12 LSIM: ai dati di cui all'articolo 46 capoverso 4 lettere a, d ed e,

2. per l'adempimento dei suoi compiti secondo l'articolo 19 LSIM, tramite il sistema d'informazione per il reclutamento di cui all'articolo 18 LSIM: ai dati di cui all'articolo 46 capoverso 4 lettere a ed e,
3. per l'adempimento dei suoi compiti secondo l'articolo 157 LSIM, tramite il sistema d'informazione per le richieste di visita di cui all'articolo 156 LSIM: ai dati di cui all'articolo 46 capoverso 4 lettere a ed e,
4. per l'adempimento dei suoi compiti secondo l'articolo 163 LSIM, tramite il sistema d'informazione per i controlli dell'accesso di cui all'articolo 162 LSIM: ai dati di cui all'articolo 46 capoverso 4 lettere a ed e;

c. il servizio competente per le attestazioni di sicurezza internazionali di cui all'articolo 49 lettera c: ai dati di cui all'articolo 46 capoverso 4 lettere a, d ed e.

3 I servizi specializzati CSP possono inoltre comunicare ad altri servizi della Confederazione dati di cui all'articolo 46 capoverso 4 lettere a ed e, se tali dati sono necessari per il controllo dell'accesso a una zona di sicurezza.

4 I servizi specializzati CSP possono comunicare alle autorità e organizzazioni assoggettate elenchi e statistiche di cui all'articolo 46 capoverso 1 lettera g, sempre che sia necessario per l'adempimento dei rispettivi compiti di controllo secondo la presente legge.

Art. 48 Conservazione, archiviazione e distruzione dei dati

1 I servizi specializzati CSP possono registrare audizioni secondo l'articolo 35 capoversi 2 lettera d e 3 con apparecchiature tecniche e conservare le registrazioni su supporti di dati.

2 Conservano i dati fintanto che la persona interessata esercita l'attività sensibile sotto il profilo della sicurezza, ma al massimo per dieci anni.

3 L'archiviazione dei dati è retta dalle prescrizioni della legislazione in materia di archiviazione.

4 Se la procedura di controllo è abbandonata oppure la persona controllata non assume la funzione prevista o rifiuta il mandato, tutti i dati e i documenti connessi con il controllo di sicurezza relativo alle persone sono distrutti al più tardi dopo tre mesi.

Sezione 6: Disposizioni del Consiglio federale

Art. 49

Il Consiglio federale disciplina:

a. la procedura del controllo di sicurezza relativo alle persone;
b. l'organizzazione dei servizi specializzati CSP;

c. le modalità di rilascio delle attestazioni di sicurezza internazionali per le persone che operano nel contesto internazionale;

d. la responsabilità della protezione dei dati in relazione con il sistema d'informazione di cui all'articolo 46 e la sicurezza dei dati;

e. il controllo periodico del trattamento dei dati personali da parte di un organo esterno.

Capitolo 4: Procedura di sicurezza relativa alle aziende

Sezione 1: Disposizioni generali

Art. 50 Scopo della procedura

La procedura di sicurezza relativa alle aziende ha lo scopo di garantire la sicurezza delle informazioni in occasione dell'adempimento di mandati pubblici da parte di imprese e imprese subappaltatrici o loro parti (aziende), nella misura in cui i mandati comportano l'esercizio di un'attività sensibile sotto il profilo della sicurezza (mandati sensibili).

Art. 51 Aziende interessate

1 Possono essere sottoposte alla procedura di sicurezza relativa alle aziende:

a. le aziende destinate a eseguire un mandato sensibile di un'autorità o organizzazione assoggettata;

b. le aziende con sede in Svizzera che si candidano per un mandato per il quale necessitano di un'attestazione di sicurezza aziendale secondo l'articolo 67.

2 La procedura può essere eseguita soltanto con il consenso dell'azienda.

3 Le aziende di cui al capoverso 1 lettera b assumono i costi della procedura.

Art. 52 Abbandono della procedura

1 La procedura di sicurezza relativa alle aziende è abbandonata se l'azienda:

a. revoca il suo consenso o non collabora alla procedura;

b. ritira la sua offerta;

c. non entra più in considerazione per il mandato.

2 Il servizio specializzato competente per l'esecuzione della procedura di sicurezza relativa alle aziende (servizio specializzato SA) comunica l'abbandono della procedura all'azienda e all'autorità o organizzazione aggiudicante (mandante).

Sezione 2: Avvio della procedura di sicurezza relativa alle aziende

Art. 53 Domanda di avvio della procedura

1 Le autorità e organizzazioni assoggettate che intendono assegnare un mandato sensibile domandano l'avvio della procedura al servizio specializzato SA.

2 Le autorità assoggettate stabiliscono quali servizi sono competenti per la presentazione della domanda.

3 Per le aziende di cui all'articolo 51 capoverso 1 lettera b, la domanda è presentata dall'autorità estera o dall'organizzazione internazionale competente.

Art. 54 Esame della domanda

1 Il servizio specializzato SA esamina la domanda e avvia la procedura.

2 Può, d'intesa con il mandante, rinunciare all'avvio della procedura se con altre misure il rischio per la sicurezza può essere ridotto a un livello sostenibile. Esso raccomanda misure in tal senso.

Art. 55 Definizione dei requisiti di sicurezza

Il servizio specializzato SA definisce, d'intesa con il mandante, i requisiti in materia di sicurezza delle informazioni per la procedura di aggiudicazione e l'adempimento del mandato.

Sezione 3: Valutazione delle aziende

Art. 56 Idoneità

1 Il mandante comunica al servizio specializzato SA quali aziende entrano in considerazione per l'esecuzione del mandato sensibile.

2 Il servizio specializzato SA valuta se tali aziende sono idonee per l'esecuzione del mandato sensibile oppure se sussiste un rischio per la sicurezza.

3 Nella sua valutazione non è vincolato a istruzioni.

Art. 57 Acquisizione dei dati

1 Per la valutazione dell'idoneità, il servizio specializzato SA può acquisire dati:

a. presso l'azienda;

b. presso il SIC;

c. da fonti pubblicamente accessibili.

2 Può chiedere a servizi esteri e internazionali l'invio dei corrispondenti dati. Le richieste a servizi informazioni esteri avvengono per il tramite del SIC.

Art. 58 Rischio per la sicurezza

1 Sussiste un rischio per la sicurezza se, sulla base dei dati acquisiti, vi sono indizi concreti che con elevata probabilità l'azienda eseguirà in maniera contraria alle prescrizioni o non appropriata il mandato sensibile.

2 La probabilità di un'esecuzione contraria alle prescrizioni o non appropriata del mandato sensibile può essere considerata elevata in particolare se:

a. l'azienda manca d'integrità o affidabilità;

b. l'azienda è controllata da Stati esteri o da organizzazioni estere di diritto pubblico o privato oppure è sotto il loro influsso e tale controllo o influsso è incompatibile con la tutela degli interessi di cui all'articolo 1 capoverso 2;

c. per persone appartenenti all'azienda indispensabili all'esecuzione del mandato sensibile è stata rilasciata una dichiarazione di rischio.

3 Il rischio per la sicurezza deve fondarsi, a prescindere dalla colpa, su circostanze oggettive inerenti all'azienda interessata.

Art. 59 Notifica della valutazione ed esclusione dalla procedura di aggiudicazione

1 Il servizio specializzato SA comunica la sua valutazione al mandante e la notifica all'azienda mediante una decisione.

2 Se il servizio specializzato SA giunge alla conclusione che l'esecuzione del mandato sensibile presenta un rischio per la sicurezza, il mandante esclude l'azienda dalla procedura di aggiudicazione.

3 Se presso tutte le aziende prese in considerazione l'esecuzione del mandato sensibile presenta un rischio per la sicurezza, il mandante può comunque assegnare il mandato a una di tali aziende. Il servizio specializzato SA abbandona la procedura di sicurezza relativa alle aziende. Il mandante applica per analogia le misure secondo gli articoli 60, 61, 64 e 65.

Sezione 4: Piano in materia di sicurezza

Art. 60 Aggiudicazione e piano in materia di sicurezza

1 Il mandante comunica al servizio specializzato SA quale azienda ha ottenuto il mandato.

2 L'azienda allestisce un piano in materia di sicurezza secondo le direttive del servizio specializzato SA.

3 Il servizio specializzato SA esamina il piano in materia di sicurezza. Può acquisire i dati necessari per scritto oppure mediante un'ispezione dell'azienda.

Art. 61 Controlli di sicurezza relativi alle persone

1 Il personale dell'azienda destinato a esercitare un'attività sensibile sotto il profilo della sicurezza è sottoposto a un controllo di sicurezza relativo alle persone.

2 Il servizio specializzato SA è competente per la decisione di cui all'articolo 42 capoverso 2. Se la procedura viene abbandonata perché non vi è nessuna azienda idonea per l'esecuzione del mandato (art. 59 cpv. 3), la decisione è di competenza del mandante.

Sezione 5: Dichiarazione di sicurezza aziendale

Art. 62 Rilascio della dichiarazione di sicurezza aziendale

1 Il servizio specializzato SA rilascia all'azienda una dichiarazione di sicurezza aziendale sotto forma di decisione non appena l'azienda ha attuato in maniera comprovata il piano in materia di sicurezza.

2 Esso rifiuta di rilasciare all'azienda la dichiarazione di sicurezza aziendale e abbandona la procedura di sicurezza relativa alle aziende se quest'ultima non attua il piano in materia di sicurezza. Emana una decisione corrispondente.

3 Le decisioni secondo i capoversi 1 e 2 sono comunicate al mandante.

4 Il mandante è vincolato alla decisione del servizio specializzato SA; è fatto salvo l'articolo 59 capoverso 3.

5 La durata di validità della dichiarazione di sicurezza aziendale è di cinque anni.

Art. 63 Esecuzione del mandato sensibile

Il mandante può autorizzare l'esecuzione del mandato sensibile soltanto dopo che il servizio specializzato SA ha rilasciato la dichiarazione di sicurezza aziendale.

Art. 64 Obblighi dell'azienda

1 Le aziende titolari di una dichiarazione di sicurezza aziendale devono applicare in permanenza le misure del piano in materia di sicurezza.

2 Annunciano senza indugio al servizio specializzato SA e al mandante tutti i cambiamenti e gli incidenti rilevanti sotto il profilo della sicurezza.

Art. 65 Controlli e misure di protezione

1 Il servizio specializzato SA è autorizzato a:

a. ispezionare senza preavviso i settori nei quali è eseguito il mandato sensibile;

b. consultare i documenti rilevanti per il mandato.

2 Se sussistono indizi concreti che in un'azienda la sicurezza delle informazioni è minacciata, il servizio specializzato SA può adottare immediatamente le misure di protezione necessarie e in particolare mettere al sicuro documenti e materiale.

Art. 66 Procedura semplificata in caso di aggiudicazione di altri mandati sensibili

Le aziende titolari di una dichiarazione di sicurezza aziendale sono considerate idonee per altri mandati sensibili. Il servizio specializzato SA verifica se il piano in materia di sicurezza dev'essere adeguato.

Art. 67 Attestazione di sicurezza aziendale internazionale

Su richiesta dell'azienda interessata, il servizio specializzato SA rilascia un'attestazione di sicurezza aziendale internazionale.

Art. 68 Revoca della dichiarazione di sicurezza aziendale

1 Il servizio specializzato SA revoca la dichiarazione di sicurezza aziendale se:

a. l'azienda non adempie i propri obblighi secondo l'articolo 64;

b. nel quadro di una ripetizione della procedura emerge un rischio per la sicurezza.

2 Comunica la sua decisione all'azienda e al mandante.

3 Se viene revocata la dichiarazione di sicurezza aziendale, il mandante ritira immediatamente il mandato; è fatto salvo l'articolo 59 capoverso 3. L'azienda non ha diritto ad alcun indennizzo.

Sezione 6: Ripetizione della procedura e tutela giurisdizionale

Art. 69 Ripetizione della procedura

La procedura di sicurezza relativa alle aziende è ripetuta se:

a. al momento della scadenza della validità della dichiarazione di sicurezza aziendale è in corso l'esecuzione di un mandato sensibile;

b. vi sono indizi concreti che in seguito a cambiamenti sostanziali in seno all'azienda sono emersi nuovi rischi per la sicurezza.

Art. 70 Tutela giurisdizionale

1 Dopo la notifica di una decisione del servizio specializzato SA, l'azienda ha 30 giorni di tempo per:

a. consultare i documenti;

b. esigere la rettifica dei dati errati o la distruzione di dati non più attuali;

c. far apporre una menzione di contestazione;

d. interporre ricorso presso il Tribunale amministrativo federale.

2 La restrizione del diritto d'accesso è retta dall'articolo 9 LPD[17].

Sezione 7: Trattamento dei dati personali

Art. 71 Sistema d'informazione per la procedura di sicurezza relativa alle aziende

1 Il servizio specializzato SA gestisce un sistema d'informazione per l'esecuzione e la gestione della procedura di sicurezza relativa alle aziende.

2 Nel sistema d'informazione possono essere trattati dati personali degni di particolare protezione e profili della personalità secondo l'articolo 3 lettere c e d LPD[18], sempre che sia necessario per l'esecuzione della procedura di sicurezza relativa alle aziende.

3 Il sistema d'informazione contiene i dati e le indicazioni seguenti:

a. i dati secondo gli articoli 57 e 60 capoverso 3;

b. il risultato della valutazione secondo l'articolo 56 capoverso 2;

c. i risultati dei controlli di sicurezza relativi alle persone secondo l'articolo 61 capoverso 1 necessari per la procedura di sicurezza relativa alle aziende;

d. la decisione del servizio specializzato SA secondo l'articolo 61 capoverso 2;

e. i nomi di tutte le aziende titolari di una dichiarazione di sicurezza aziendale;

f. le misure risultanti da eventuali controlli secondo l'articolo 65;

g. dati e atti di procedure di ricorso.

4 Il servizio specializzato SA è responsabile della sicurezza del sistema d'informazione e della liceità del trattamento dei dati personali.

Art. 72 Diritti d'accesso e comunicazione dei dati

1 I servizi seguenti hanno accesso, mediante procedura di richiamo, ai dati menzionati qui appresso:

a. i mandanti: ai dati di cui all'articolo 71 capoverso 3 lettere b e d–g;

b. le aziende interessate, sempre che siano state autorizzate dal Consiglio federale, in virtù dell'articolo 32 capoverso 1 lettera a, ad avviare controlli di sicurezza relativi alle persone nel rispettivo ambito di competenza: ai dati di cui all'articolo 71 capoverso 3 lettera d.

17 RS **235.1**
18 RS **235.1**

2 Il servizio specializzato SA può inoltre comunicare ad altri servizi della Confederazione dati di cui all'articolo 71 capoverso 3 lettere b–d, sempre che sia necessario per garantire la sicurezza delle informazioni.

Art. 73 Conservazione, archiviazione e distruzione dei dati

1 Il servizio specializzato SA conserva i dati fintanto che l'azienda interessata è in possesso di una dichiarazione di sicurezza aziendale, ma al massimo per dieci anni.

2 L'archiviazione dei dati è retta dalle prescrizioni della legislazione in materia di archiviazione.

3 Se la procedura di sicurezza relativa alle aziende è abbandonata, tutti i relativi dati e atti sono distrutti al più tardi dopo tre mesi.

Sezione 8: Disposizioni emanate dal Consiglio federale

Art. 74

Il Consiglio federale disciplina:

a. la procedura di sicurezza relativa alle aziende nel dettaglio;
b. l'applicazione della procedura di sicurezza relativa alle aziende a imprese subappaltatrici;
c. l'organizzazione del servizio specializzato SA;
d. la sicurezza dei dati nel sistema d'informazione secondo l'articolo 71;
e. il controllo periodico del trattamento dei dati personali da parte di un organo esterno.

Capitolo 5: Infrastrutture critiche

Art. 75 Compiti della Confederazione

1 La Confederazione sostiene i gestori di infrastrutture critiche per garantire che le interruzioni delle reti e dei sistemi nonché gli abusi siano rari, di breve durata, gestibili e poco dannosi.

2 Il sostegno nell'ambito della sicurezza delle informazioni comprende:

a. l'identificazione e la valutazione tempestive di minacce, pericoli, vulnerabilità e lacune nella sicurezza;
b. l'individuazione di incidenti;
c. la tutela e il ripristino della sicurezza delle informazioni dopo un incidente;
d. il trattamento ulteriore di incidenti.

3 La Confederazione gestisce un servizio nazionale di preallerta e un punto di contatto per misure preventive e reattive nell'ambito della sicurezza tecnica delle informazioni.

4 Provvede affinché i gestori di infrastrutture critiche possano scambiare informazioni in modo sicuro con i servizi della Confederazione competenti e tra di loro.

5 Il Consiglio federale designa i servizi della Confederazione competenti per tali compiti.

Art. 76 Trattamento di dati personali

1 Per l'adempimento dei propri compiti, i servizi di cui all'articolo 75 capoverso 5 possono trattare elementi di indirizzo di cui all'articolo 3 lettera f LTC[19] e i dati personali connessi.

2 Possono parimenti trattare i dati di cui al capoverso 1 quando:

a. contengono informazioni concernenti opinioni religiose, filosofiche o politiche; il trattamento è ammesso unicamente qualora sia necessario per la valutazione di minacce e pericoli concreti nell'ambito della sicurezza delle informazioni;

b. contengono informazioni concernenti procedimenti e sanzioni di carattere amministrativo o penale.

3 I dati personali possono essere trattati all'insaputa delle persone interessate.

4 In caso di indizi concreti di usurpazione d'identità o di utilizzazione non autorizzata di elementi di indirizzo, le persone interessate devono essere informate. Sono fatti salvi gli articoli 18*a* capoverso 4 lettera b e 18*b* LPD[20].

Art. 77 Collaborazione in Svizzera

1 I servizi di cui all'articolo 75 capoverso 5 possono comunicare ai gestori di infrastrutture critiche dati personali di cui all'articolo 76, sempre che sia appropriato per garantire la sicurezza delle informazioni.

2 Possono comunicare ai fornitori e ai gestori di servizi informatici e di comunicazione dati personali di cui all'articolo 76, sempre che sia necessario per garantire la sicurezza delle informazioni d'infrastrutture critiche.

3 I gestori di infrastrutture critiche nonché i fornitori e i gestori di servizi informatici e di comunicazione possono comunicare ai servizi di cui all'articolo 75 capoverso 5 dati inerenti a un incidente determinato, inclusi dati personali. I servizi di cui all'articolo 75 capoverso 5 possono trasmettere tali dati ai fini del perseguimento penale unicamente previo consenso esplicito del fornitore dei dati.

19 RS **784.10**
20 RS **235.1**

Art. 78 Cooperazione internazionale

1 I servizi di cui all'articolo 75 capoverso 5 possono scambiare dati di cui all'articolo 76 con servizi esteri e internazionali competenti per la protezione di infrastrutture critiche se tali dati sono necessari a questi ultimi per l'adempimento di compiti corrispondenti ai compiti secondo l'articolo 75.

2 Lo scambio di dati secondo il capoverso 1 è ammesso soltanto se i servizi esteri e internazionali garantiscono che i dati sono trattati per i fini previsti da tale disposizione.

3 Se i dati sono necessari per un procedimento legale all'estero, si applicano le disposizioni dell'assistenza amministrativa e dell'assistenza giudiziaria.

Art. 79 Sistema d'informazione per il sostegno alle infrastrutture critiche

1 I servizi di cui all'articolo 75 capoverso 5 gestiscono un sistema d'informazione per garantire lo scambio sicuro di informazioni con i gestori di infrastrutture critiche.

2 Il sistema d'informazione contiene le informazioni seguenti:

a. descrizioni e valutazioni di minacce e pericoli;

b. consegne per individuare e fronteggiare tecnicamente gli incidenti;

c. analisi di incidenti e raccomandazioni in materia di sicurezza;

d. analisi delle vulnerabilità dei mezzi informatici;

e. corrispondenza.

3 Le informazioni di cui al capoverso 2 possono anche contenere dati personali secondo l'articolo 76.

Art. 80 Conservazione e archiviazione dei dati

1 I servizi di cui all'articolo 75 capoverso 5 conservano dati personali soltanto fintanto che sono utili a sventare pericoli o individuare incidenti, ma al massimo per cinque anni.

2 L'archiviazione dei dati è retta dalle prescrizioni della legislazione in materia di archiviazione.

Art. 81 Disposizioni del Consiglio federale

Il Consiglio federale disciplina:

a. la ripartizione dei compiti, la collaborazione e lo scambio di informazioni tra i servizi di cui all'articolo 75 capoverso 5 e il SIC;

b. la comunicazione di informazioni a gestori di infrastrutture critiche, terzi nonché servizi esteri e internazionali;

c. la responsabilità in materia di protezione dei dati in relazione con il sistema d'informazione di cui all'articolo 79 e la sicurezza dei dati;

d. il controllo periodico del trattamento dei dati personali nel sistema d'informazione secondo l'articolo 79 da parte di un organo esterno.

Capitolo 6: Organizzazione ed esecuzione

Sezione 1: Organizzazione

Art. 82 Incaricati della sicurezza delle informazioni

1 Le autorità e organizzazioni seguenti designano per il rispettivo ambito di competenza un incaricato della sicurezza delle informazioni e un sostituto:

a. il Consiglio federale;

b. la Delegazione amministrativa dell'Assemblea federale;

c. i tribunali della Confederazione;

d. il Ministero pubblico della Confederazione;

e. la Banca nazionale svizzera;

f. i dipartimenti e la Cancelleria federale.

2 Gli incaricati della sicurezza delle informazioni assumono i compiti seguenti:

a. consigliano e assistono i servizi competenti del rispettivo ambito nell'adempimento dei compiti e degli obblighi secondo la presente legge;

b. dirigono, per incarico della rispettiva autorità o organizzazione, l'organizzazione specialistica in materia di sicurezza delle informazioni e la relativa gestione dei rischi;

c. verificano, per incarico della rispettiva autorità o organizzazione, il rispetto delle direttive in materia di sicurezza delle informazioni, redigono rapporti e propongono le misure necessarie;

d. possono annunciare incidenti rilevanti sotto il profilo della sicurezza al servizio specializzato della Confederazione per la sicurezza delle informazioni e ai servizi di cui all'articolo 75 capoverso 5.

3 Agli incaricati della sicurezza delle informazioni non sono attribuiti compiti suscettibili di generare un conflitto d'interessi con i compiti di cui al capoverso 2.

Art. 83 Conferenza degli incaricati della sicurezza delle informazioni

1 La conferenza degli incaricati della sicurezza delle informazioni è composta dagli incaricati della sicurezza delle informazioni secondo l'articolo 82 capoverso 1, da due rappresentanti dei Cantoni e dall'incaricato federale della protezione dei dati e della trasparenza.

2 Assume i compiti seguenti:

a. promuove l'esecuzione uniforme della presente legge;

b. partecipa alla standardizzazione dei requisiti e delle misure secondo l'articolo 86;

c. offre consulenza al servizio specializzato della Confederazione per la sicurezza delle informazioni in tutte le questioni relative al coordinamento dell'esecuzione e in questioni d'importanza strategica;

d. provvede allo scambio di informazioni, in particolare in relazione con la gestione dei rischi nonché con problemi e incidenti nell'ambito della sicurezza delle informazioni;

e. provvede al coordinamento con altri servizi che adempiono compiti nell'ambito della sicurezza delle informazioni.

3 La conferenza adotta un proprio regolamento interno.

Art. 84 Servizio specializzato della Confederazione per la sicurezza delle informazioni

1 Il servizio specializzato della Confederazione per la sicurezza delle informazioni assume i compiti seguenti:

a. consiglia e assiste le autorità assoggettate, i loro incaricati della sicurezza delle informazioni e i Cantoni nell'esecuzione della presente legge;

b. può formulare raccomandazioni in caso di minacce per la sicurezza delle informazioni della Confederazione;

c. può eseguire verifiche su richiesta delle autorità assoggettate;

d. può valutare, su richiesta delle autorità assoggettate, i rischi per la sicurezza delle informazioni connessi con l'impiego di nuove tecnologie;

e. può verificare su richiesta delle autorità e organizzazioni assoggettate se i loro processi, i loro mezzi, le loro installazioni, i loro oggetti e le loro prestazioni soddisfano i requisiti in materia di sicurezza delle informazioni;

f. può dirigere e coordinare, su richiesta delle autorità assoggettate, la sicurezza delle informazioni nel quadro di progetti importanti che coinvolgono più autorità;

g. è l'interlocutore per i contatti specialistici con servizi svizzeri, esteri e internazionali;

h. redige annualmente per il Consiglio federale un rapporto sullo stato della sicurezza delle informazioni della Confederazione.

2 L'incaricato del Consiglio federale per la sicurezza delle informazioni dirige il servizio specializzato della Confederazione per la sicurezza delle informazioni.

3 Il Consiglio federale disciplina l'organizzazione del servizio specializzato della Confederazione per la sicurezza delle informazioni. Può assegnargli ulteriori compiti a favore dell'Amministrazione federale e dell'esercito.

Sezione 2: Esecuzione

Art. 85 Disposizioni esecutive

1 Le autorità assoggettate sono incaricate di emanare le disposizioni esecutive della presente legge. Il Consiglio federale può delegare alla Cancelleria federale l'emanazione di disposizioni esecutive per gli affari del Consiglio federale.

2 Nel caso dell'Assemblea federale, le competenze che la presente legge assegna alle autorità assoggettate sono assunte dalla sua Delegazione amministrativa.

3 Le disposizioni esecutive del Consiglio federale si applicano per analogia alle autorità assoggettate, sempre che esse non emanino disposizioni esecutive proprie.

Art. 86 Requisiti e misure standardizzati

1 Il Consiglio federale stabilisce, secondo lo stato della scienza e della tecnica, requisiti standardizzati nonché misure organizzative, di personale, tecniche ed edili standardizzate per garantire la sicurezza delle informazioni.

2 Può delegare tale compito.

3 I requisiti e le misure standardizzati hanno carattere di raccomandazione, sempre che non siano dichiarati vincolanti dalle autorità assoggettate.

Art. 87 Cantoni

1 I Cantoni provvedono alla verifica periodica dell'applicazione e dell'efficacia della sicurezza delle informazioni secondo l'articolo 3.

2 Informano il servizio specializzato della Confederazione per la sicurezza delle informazioni sull'esito delle verifiche secondo il capoverso 1.

3 Designano ciascuno un servizio quale interlocutore delle autorità assoggettate per le questioni inerenti alla sicurezza delle informazioni.

4 Il Consiglio federale stabilisce in quali casi i Cantoni possono ricorrere alle prestazioni dei servizi specializzati secondo la presente legge per la loro sicurezza delle informazioni. Le prestazioni sono soggette al pagamento di un emolumento. Il Consiglio federale stabilisce l'ammontare degli emolumenti.

Art. 88 Trattati internazionali

Il Consiglio federale è autorizzato a concludere trattati internazionali nel campo della sicurezza delle informazioni per:

a. lo scambio di informazioni su pericoli, punti deboli e incidenti in tale ambito, in particolare per quanto riguarda le infrastrutture critiche;

b. lo scambio di informazioni classificate;

c. l'esecuzione di controlli di sicurezza relativi alle persone e di procedure di sicurezza relative alle aziende;

d. il riconoscimento di dichiarazioni di sicurezza;

e. l'esecuzione di controlli.

Art. 89 Valutazione

1 Il Consiglio federale provvede affinché l'applicazione, l'adeguatezza, l'efficacia e l'economicità della presente legge siano periodicamente verificate.

2 Redige periodicamente un rapporto per le commissioni competenti dell'Assemblea federale.

Capitolo 7: Disposizioni finali

Art. 90 Modifica di altri atti normativi

La modifica di altri atti normativi è disciplinata nell'allegato.

Art. 91 Disposizioni transitorie

1 La classificazione delle informazioni classificate secondo il diritto anteriore è adeguata alle disposizioni del nuovo diritto in occasione del loro primo trattamento dopo l'entrata in vigore della presente legge.

2 I mezzi informatici devono essere classificati secondo le disposizioni della presente legge entro due anni dalla sua entrata in vigore. Le misure tecniche per garantire la sicurezza delle informazioni devono essere concretizzate entro sei anni dall'entrata in vigore della presente legge.

3 Le dichiarazioni di sicurezza e di rischio rilasciate secondo il diritto anteriore nel quadro di controlli di sicurezza relativi alle persone e le dichiarazioni di sicurezza aziendale rilasciate secondo il diritto anteriore rimangono valevoli per cinque anni dal loro rilascio.

Art. 92 Referendum ed entrata in vigore

1 La presente legge sottostà a referendum facoltativo.

2 Il Consiglio federale ne determina l'entrata in vigore.

Allegato
(art. 90)

Modifica di altri atti normativi

Gli atti normativi qui appresso sono modificati come segue:

1. Legge federale del 21 marzo 1997[21] sulle misure per la salvaguardia della sicurezza interna

Art. 2 cpv. 4 lett. c

Abrogata

Sezione 4 (art. 19–21)

Abrogata

Art. 24a cpv. 7, primo periodo

7 Il sistema d'informazione è a disposizione dei servizi di fedpol competenti per l'esecuzione della presente legge, delle autorità di polizia dei Cantoni, del Servizio centrale svizzero in materia di tifoseria violenta (Servizio centrale), delle autorità doganali e dei servizi specializzati competenti per l'esecuzione dei controlli di sicurezza relativi alle persone secondo l'articolo 32 capoverso 2 della legge del …[22] sulla sicurezza delle informazioni, mediante una procedura di richiamo. …

2. Legge federale del 25 settembre 2015[23] sulle attività informative

Art. 51 cpv. 4 lett. d

4 Le seguenti persone hanno accesso mediante procedura di richiamo ai dati di INDEX SIC indicati di seguito:

d. i collaboratori dei servizi specializzati competenti per l'esecuzione dei controlli di sicurezza relativi alle persone secondo l'articolo 32 capoverso 2 della legge del …[24] sulla sicurezza delle informazioni, ai dati di cui al capoverso 3 lettera a per l'esecuzione di controlli di sicurezza relativi alle persone, per verifiche dell'affidabilità e per la valutazione del potenziale di violenza.

21 RS **120**
22 RS …; FF **2017** 2563 2711
23 FF **2015** 5925
24 RS …; FF **2017** 2563 2711

3. Legge del 24 marzo 2000[25] sul personale federale

Art. 20a Estratto del casellario giudiziale e del registro delle esecuzioni

I datori di lavoro possono esigere dai candidati a un impiego e dai loro impiegati un estratto del casellario giudiziale e del registro delle esecuzioni se ciò è necessario per la tutela degli interessi del datore di lavoro.

Art. 20b Verifica dell'affidabilità

1 I datori di lavoro secondo l'articolo 3 capoverso 1 lettere a, b, e ed f possono richiedere la verifica dell'affidabilità dei candidati a un impiego nonché dei loro impiegati, se nel quadro della loro funzione questi ultimi sono destinati:

a. a rappresentare regolarmente la Svizzera all'estero e in tale contesto potrebbero pregiudicare considerevolmente l'immagine della Confederazione;

b. a prendere decisioni e a esercitare compiti di vigilanza in affari finanziari o fiscali essenziali e in tale contesto potrebbero pregiudicare considerevolmente gli interessi finanziari della Confederazione.

2 Nell'ambito della verifica si limitano al minimo indispensabile.

3 I servizi specializzati secondo l'articolo 32 capoverso 2 della legge del …[26] sulla sicurezza delle informazioni (LSIn) eseguono le verifiche dell'affidabilità. La procedura si fonda per analogia sulle pertinenti disposizioni della LSIn.

4 Se i candidati a un impiego e gli impiegati sono sottoposti contemporaneamente a un controllo di sicurezza relativo alle persone secondo la LSIn, le due procedure sono riunite.

4. Codice di procedura civile[27]

Art. 166 cpv. 1 lett. c

1 Un terzo può rifiutarsi di cooperare:

c. all'accertamento di fatti confidatigli nella sua qualità ufficiale o di cui è venuto a conoscenza nell'esercizio della sua funzione, se è un funzionario ai sensi dell'articolo 110 capoverso 3 CP o membro di un'autorità, oppure di cui è venuto a conoscenza nell'esercizio della sua attività ausiliaria per un funzionario o un'autorità; egli è però tenuto a deporre se sottostà a un obbligo di denuncia o è stato autorizzato a deporre dall'autorità a lui preposta;

25 RS **172.220.1**
26 RS …; FF **2017** 2563 2711
27 RS **272**

5. Legge di procedura civile federale del 4 dicembre 1947[28]

Art. 42 cpv. 3

3 Per quanto concerne l'obbligo dei funzionari e dei loro ausiliari di deporre su fatti di cui hanno avuto notizia nell'esercizio delle loro funzioni o della loro attività ausiliaria, sono applicabili le disposizioni restrittive del diritto amministrativo federale o cantonale.

6. Codice penale svizzero[29]

Art. 320 Violazione del segreto d'ufficio

1. Chiunque rivela un segreto, che gli è confidato nella sua qualità di membro di una autorità o di funzionario o di cui ha notizia per la sua carica o funzione oppure in qualità di ausiliario di un funzionario o di un'autorità, è punito con una pena detentiva sino a tre anni o con una pena pecuniaria.

La rivelazione del segreto è punibile anche dopo la cessazione della carica, della funzione o dell'attività ausiliaria.

2. La rivelazione fatta col consenso scritto dell'autorità superiore non è punibile.

Art. 365 cpv. 2 lett. d

2 Il casellario ha lo scopo di assistere le autorità federali e cantonali nell'adempimento dei compiti seguenti:

d. valutazione del rischio per la sicurezza nel quadro dei controlli di sicurezza relativi alle persone secondo la legge del …[30] sulla sicurezza delle informazioni (LSIn) e nel quadro delle verifiche dell'affidabilità secondo la legislazione speciale;

Art. 367 cpv. 2 lett. i, 2bis lett. b e 4

2 Le autorità seguenti possono, mediante procedura di richiamo, accedere ai dati personali concernenti le sentenze di cui all'articolo 366 capoversi 1, 2 e 3 lettere a e b:

i. i servizi specializzati competenti per l'esecuzione dei controlli di sicurezza relativi alle persone secondo l'articolo 32 capoverso 2 LSIn[31] (servizi specializzati CSP);

28 RS **273**
29 RS **311.0**
30 RS …; FF **2017** 2563 2711
31 RS …; FF **2017** 2563 2711

[2bis] Le autorità seguenti possono, mediante procedura di richiamo, accedere anche ai dati personali concernenti le sentenze di cui all'articolo 366 capoverso 3 lettera c:

b. i servizi specializzati CSP;

[4] I dati personali concernenti procedimenti penali pendenti possono essere trattati soltanto dalle autorità di cui al capoverso 2 lettere a–e, i, j e l.

7. Codice di procedura penale[32]

Art. 170 cpv. 1

[1] I funzionari ai sensi dell'articolo 110 capoverso 3 CP[33] e i loro ausiliari come pure i membri di autorità e i loro ausiliari hanno facoltà di non deporre in merito a segreti loro confidati in virtù della loro veste ufficiale o di cui sono venuti a conoscenza nell'esercizio delle loro funzioni o della loro attività ausiliaria.

8. Codice penale militare del 3 giugno 1927[34]

Art. 77 Violazione del segreto di servizio

1. Chi rivela un segreto che gli è stato confidato nella sua qualità di militare o di funzionario o di cui ha avuto notizia in tale qualità o in qualità di ausiliario di uno di questi detentori del segreto, è punito con una pena detentiva sino a tre anni o con una pena pecuniaria.

Nei casi poco gravi si applica una pena disciplinare.

2. La rivelazione del segreto è punibile anche dopo la cessazione della qualità di militare, della funzione o dell'attività ausiliaria.

9. Procedura penale militare del 23 marzo 1979[35]

Art. 77 cpv. 2

[2] Nessun funzionario o suo ausiliario può, senza il consenso dell'autorità da cui dipende, essere interrogato come testimone su un segreto d'ufficio (art. 320 CP[36]) o essere obbligato a produrre documenti ufficiali. Sono del resto applicabili le disposizioni del diritto amministrativo federale e cantonale.

32 RS **312.0**
33 RS **311.0**
34 RS **321.0**
35 RS **322.1**
36 RS **311.0**

10. Legge federale del 13 giugno 2008[37] sui sistemi d'informazione di polizia della Confederazione

Art. 15 cpv. 4 lett. f

Abrogata

Art. 17 cpv. 4, frase introduttiva e lett. l

4 Hanno accesso a questi dati mediante procedura di richiamo:

l. i servizi specializzati competenti per l'esecuzione dei controlli di sicurezza relativi alle persone secondo l'articolo 32 capoverso 2 della legge del …[38] sulla sicurezza delle informazioni, ai fini della valutazione del rischio per la sicurezza nel quadro di un controllo di sicurezza relativo alle persone, di una verifica dell'affidabilità o di una valutazione del potenziale di violenza.

11. Legge militare del 3 febbraio 1995[39]

Art. 14 Verifica dell'affidabilità

1 I militari possono essere sottoposti a una verifica dell'affidabilità se nel quadro della loro funzione:

a. sono destinati a rappresentare regolarmente la Svizzera all'estero e in tale contesto potrebbero pregiudicare considerevolmente l'immagine della Confederazione;

b. sono destinati a prendere decisioni e a esercitare compiti di vigilanza in affari finanziari essenziali e in tale contesto potrebbero pregiudicare considerevolmente gli interessi finanziari della Confederazione.

2 Il Consiglio federale stabilisce quali funzioni sono soggette alla verifica. Al riguardo si limita al minimo indispensabile.

3 Il servizio specializzato secondo l'articolo 32 capoverso 2 della legge federale del …[40] sulla sicurezza delle informazioni (LSIn) esegue le verifiche dell'affidabilità. La procedura è retta per analogia dalle pertinenti disposizioni della LSIn.

4 Se i militari sono sottoposti contemporaneamente a un controllo di sicurezza relativo alle persone secondo la LSIn, le due procedure sono riunite.

37 RS **361**
38 RS …; FF **2017** 2563 2711
39 RS **510.10**
40 RS …; FF **2017** 2563 2711

Art. 113 cpv. 6

6 La procedura è retta per analogia dalle disposizioni relative al controllo di sicurezza di base secondo l'articolo 31 lettera a LSIn[41]. Se contemporaneamente deve essere eseguito un controllo di sicurezza di base anche per altri motivi, le due procedure sono riunite.

Art. 150 cpv. 4

Abrogato

12. Legge federale del 3 ottobre 2008[42] sui sistemi d'informazione militari

Art. 14 cpv. 1 lett. i

1 Il PISA contiene i seguenti dati delle persone soggette all'obbligo di leva, delle persone soggette all'obbligo di prestare servizio militare, del personale previsto per il promovimento della pace nonché di civili assistiti dalla truppa o chiamati a partecipare a un impiego di durata limitata dell'esercito:

i. dati concernenti l'esecuzione della verifica dell'affidabilità secondo l'articolo 14 della legge militare del 3 febbraio 1995[43] (LM), con decisione.

Art. 17 cpv. 1 lett. a

1 I dati del PISA concernenti reati, decisioni e misure penali possono essere conservati soltanto se, sulla base di tali dati:

a. è stata emanata una decisione di non reclutamento, esclusione o degradazione ai sensi della LM[44];

Capitolo 5, sezioni 1 e 2 (art. 144–155)

Abrogate

13. Legge federale del 21 marzo 2003[45] sull'energia nucleare

Art. 5 cpv. 3 e 3bis

3 Per impedire che la sicurezza interna di impianti nucleari e materiali nucleari sia ridotta da effetti non autorizzati o che materiali nucleari siano sottratti, vanno presi provvedimenti di sicurezza esterna.

41 RS …; FF **2017** 2563 2711
42 RS **510.91**
43 RS **510.10**
44 RS **510.10**
45 RS **732.1**

3bis La classificazione e il trattamento delle informazioni sono rette dalle disposizioni della legislazione sulla sicurezza delle informazioni in seno alla Confederazione.

14. Legge del 23 marzo 2007[46] sull'approvvigionamento elettrico

Art. 20a Verifica dell'affidabilità

1 Ai fini della valutazione del rischio per la sicurezza, gli impiegati della società nazionale di rete che adempiono compiti essenziali per la sicurezza della rete di trasporto a livello nazionale e il suo esercizio affidabile e performante sono sottoposti a una verifica della loro affidabilità.

2 Il Consiglio federale stabilisce quali gruppi di persone sono soggetti alla verifica. Al riguardo si limita al minimo indispensabile.

3 Il servizio specializzato secondo l'articolo 32 capoverso 2 della legge del …[47] sulla sicurezza delle informazioni (LSIn) esegue la verifica dell'affidabilità. La procedura è retta per analogia dalle pertinenti disposizioni della LSIn.

4 Gli esiti della verifica sono comunicati alla direzione della società nazionale di rete, all'Ufficio federale e alla ElCom.

15. Legge del 3 ottobre 2003[48] sulla Banca nazionale

Art. 16, rubrica e cpv. 5

Confidenzialità e sicurezza delle informazioni

5 Per il rimanente si applicano le disposizioni della legge federale del 19 giugno 1992[49] sulla protezione dei dati e della legge del …[50] sulla sicurezza delle informazioni.

46 RS **734.7**
47 RS …; FF **2017** 2563 2711
48 RS **951.11**
49 RS **235.1**
50 RS …; FF **2017** 2563 2711