
Legge federale 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 federale¹;

visto il messaggio del Consiglio federale del ...²,

decreta:

Capitolo 1: Disposizioni generali

Art. 1 Scopo

¹ La presente legge ha lo scopo di garantire la gestione sicura di informazioni nonché l'impiego sicuro di tecnologie dell'informazione e della comunicazione.

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

- a. la capacità di decisione e d'azione delle autorità federali;
- 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 impegni legali e contrattuali delle autorità federali per la protezione di informazioni.

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;

RU ...

¹ RS 101

² FF ...

- 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 diritto pubblico e privato che, nel quadro dell'adempimento di compiti amministrativi ai sensi dell'articolo 2 capoverso 4 della legge del 21 marzo 1997³ sull'organizzazione del Governo e dell'Amministrazione, esercitano attività sensibili sotto il profilo della sicurezza;
- f. alle autorità e ai servizi cantonali che, per incarico della Confederazione e sotto la sua vigilanza, esercitano attività sensibili sotto il profilo della sicurezza.

³ Sono considerate attività sensibili sotto il profilo della sicurezza:

- a. il trattamento di informazioni classificate «CONFIDENZIALE» o «SEGRETO» oppure la gestione del materiale classificato in maniera corrispondente (art. 14 cpv. 2 e 3);
- b. l'amministrazione, l'esercizio, la manutenzione o la verifica di mezzi delle tecnologie dell'informazione e della comunicazione (mezzi TIC) del livello di sicurezza «protezione elevata» oppure «protezione molto elevata» (art. 21 cpv. 2 e 3);
- c. 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 (art. 31).

Art. 3 Rapporto con la legislazione speciale

¹ È fatta salva la legge del 17 dicembre 2004⁴ sulla trasparenza.

² Se le informazioni devono essere protette in virtù di altre leggi federali, le disposizioni della presente legge si applicano a titolo complementivo.

³ L'applicazione della presente legge a organizzazioni di diritto pubblico e privato che gestiscono infrastrutture indispensabili per il funzionamento della società, dell'economia e dello Stato (infrastrutture critiche) si fonda sulla legislazione speciale.

³ RS 172.010

⁴ RS 152.3

Capitolo 2: Misure generali per la sicurezza delle informazioni

Sezione 1: Principi

Art. 4 Sicurezza delle informazioni

¹ Le autorità e organizzazioni assoggettate provvedono affinché le necessità di protezione delle informazioni per le quali sono competenti siano valutate nell'ottica di un eventuale pregiudizio per gli 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).

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

⁴ Al riguardo, perseguono un approccio basato sui rischi e considerano i principi dell'adeguatezza, dell'economicità e della praticità.

Art. 5 Massima responsabilità direttiva

¹ Le autorità assoggettate provvedono, nel rispettivo ambito di competenza, affinché:

- a. la sicurezza delle informazioni sia organizzata, attuata e verificata secondo lo stato della dottrina e della tecnica;
- b. la sicurezza delle informazioni sia coordinata tra gli ambiti specialistici.

² Stabiliscono i compiti degli organi interessati.

³ Stabiliscono inoltre:

- 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.

⁴ Provvedono affinché i quadri e il personale siano informati regolarmente e conformemente al rispettivo livello.

Art. 6 Gestione dei rischi

¹ Le autorità e organizzazioni assoggettate provvedono affinché i rischi per la sicurezza delle informazioni nel loro ambito di competenza e nella collaborazione con terzi siano costantemente identificati, analizzati, valutati e verificati.

² Provvedono affinché sotto il profilo organizzativo, del personale, tecnico ed edile siano adottate le misure necessarie per evitare i rischi identificati o ridurli a un livello sostenibile.

³ Provvedono affinché i rischi che devono essere sostenuti siano comprovatamente comunicati e accettati.

⁴ La gestione dei rischi nell'ambito della sicurezza delle informazioni dev'essere integrata nel processo generale di gestione dei rischi.

Art. 7 Requisiti e misure di sicurezza

¹ Nella definizione dei requisiti e delle misure di sicurezza le autorità e le organizzazioni assoggettate si orientano ai requisiti e alle misure standard secondo l'articolo 88.

² Le misure di sicurezza si fondano sullo stato della dottrina e della tecnica.

Art. 8 Collaborazione con terzi

¹ Le autorità e organizzazioni assoggettate provvedono affinché, in occasione della collaborazione con terzi, i requisiti e le misure secondo la presente legge siano stabiliti nelle convenzioni e nei contratti corrispondenti.

² Verificano l'applicazione delle misure.

Art. 9 Procedura in caso di violazione della sicurezza delle informazioni

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

Art. 10 Pianificazioni preventive

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, e siano svolte le corrispondenti esercitazioni.

Art. 11 Controlli

¹ Le autorità e organizzazioni assoggettate provvedono affinché il rispetto delle prescrizioni della presente legge sia periodicamente verificato.

² Le autorità assoggettate incaricano periodicamente un organo indipendente di verificare l'efficacia delle misure adottate nel loro ambito di competenza.

Sezione 2: Classificazione delle informazioni

Art. 12 Principi della classificazione

¹ Le autorità e organizzazioni assoggettate provvedono affinché le informazioni che soddisfano i criteri di cui all'articolo 14 siano classificate di conseguenza.

² La classificazione è limitata al minimo indispensabile.

³ È limitata nel tempo se è prevedibile che essa sarà necessaria soltanto fino a un determinato momento.

⁴ Ogni classificazione è periodicamente verificata.

Art. 13 Competenze

¹ Le autorità assoggettate stabiliscono quali persone o 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 suo organo superiore.

Art. 14 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.

Art. 15 Accesso a informazioni classificate

¹ Ottengono l'accesso a informazioni classificate della Confederazione soltanto le persone che offrono la garanzia di gestire in modo appropriato le informazioni classificate 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 Sono fatte salve le limitazioni di accesso disciplinate da trattati internazionali secondo l'articolo 90.

Art. 16 Trattamento di informazioni classificate

¹ Le informazioni classificate sono protette dalla conoscenza da parte di persone non autorizzate per l'intero periodo durante il quale sono considerate degne di protezione.

² Devono contenere un'indicazione relativa al servizio incaricato della classificazione.

³ Il trattamento di informazioni classificate provenienti dall'estero si fonda sul corrispondente trattato internazionale secondo l'articolo 90.

Art. 17 Comunicazione di informazioni classificate in procedure particolari

¹ La comunicazione di informazioni classificate in seno all'Assemblea federale, ai Servizi del Parlamento, ai tribunali e ai ministeri pubblici si fonda sul rispettivo diritto procedurale applicabile.

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

Art. 18 Misure di protezione provvisorie

¹ Le autorità e organizzazioni assoggettate provvedono affinché il servizio incaricato della classificazione riceva una comunicazione quando:

- a. informazioni classificate sono minacciate o utilizzate abusivamente oppure sono state smarrite;
- b. delle informazioni sono state classificate manifestamente in modo errato oppure, per errore, non sono state classificate.

² Adottano le misure necessarie per proteggere provvisoriamente le informazioni in questione.

Sezione 3: Sicurezza in occasione dell'impiego di mezzi TIC**Art. 19** Procedura di sicurezza

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

² Per l'esecuzione della procedura di sicurezza è competente l'autorità o l'organizzazione assoggettata che, per l'adempimento dei propri compiti legali, conferisce il mandato per l'esercizio di mezzi TIC oppure provvede essa stessa all'esercizio di mezzi TIC.

³ La procedura di sicurezza dev'essere ripetuta in caso di modifica dei rischi.

Art. 20 Analisi delle necessità di protezione e valutazione dei rischi

¹ Le organizzazioni e autorità assoggettate provvedono, in occasione della pianificazione dell'impiego di mezzi TIC, affinché siano valutate le necessità in materia di sicurezza delle informazioni.

² Le autorità e organizzazioni assoggettate che intendono impiegare nuove tecnologie provvedono a valutare i rischi per la sicurezza delle informazioni ad esse connessi. Comunicano la valutazione dei rischi al servizio specializzato della Confederazione per la sicurezza delle informazioni.

Art. 21 Livelli di sicurezza dei mezzi TIC

¹ Il livello di sicurezza «protezione di base» si applica a tutti i mezzi TIC, sempre che essi non debbano essere attribuiti a un livello di sicurezza più elevato.

² Il livello di sicurezza «protezione elevata» si applica ai mezzi TIC:

- a. per i quali una violazione della confidenzialità, della disponibilità, dell'integrità o della tracciabilità delle informazioni che sono destinati a trattare può pregiudicare considerevolmente gli interessi di cui all'articolo 1 capoverso 2; o
- b. il cui disturbo o la cui utilizzazione abusiva può pregiudicare considerevolmente gli interessi di cui all'articolo 1 capoverso 2.

³ Il livello di sicurezza «protezione molto elevata» si applica ai mezzi TIC:

- a. per i quali una violazione della confidenzialità, della disponibilità, dell'integrità o della tracciabilità delle informazioni che sono destinati a trattare può pregiudicare gravemente gli interessi di cui all'articolo 1 capoverso 2; o
- b. il cui disturbo o la cui utilizzazione abusiva può pregiudicare gravemente gli interessi di cui all'articolo 1 capoverso 2.

Art. 22 Requisiti di sicurezza del livello di sicurezza «protezione di base»

¹ Le autorità assoggettate stabiliscono i requisiti minimi per i mezzi TIC del livello di sicurezza «protezione di base».

² Tali requisiti minimi devono essere soddisfatti da tutti i mezzi TIC.

Art. 23 Concetto in materia di sicurezza delle informazioni

¹ Le autorità e organizzazioni assoggettate provvedono affinché sia eseguita un'analisi dei rischi e allestito un concetto in materia di sicurezza delle informazioni per i mezzi TIC dei livelli di sicurezza «protezione elevata» e «protezione molto elevata».

² Il concetto in materia di sicurezza delle informazioni deve essere verificato dall'incaricato della sicurezza delle informazioni competente e approvato dall'autorità o organizzazione assoggettata.

³ Deve essere costantemente aggiornato.

Art. 24 Verifiche della conformità e dell'efficacia

¹ Prima di impiegare un mezzo TIC occorre verificare se la procedura di sicurezza è stata eseguita in maniera giuridicamente conforme e se le misure decise sono state attuate.

² Prima di impiegare un mezzo TIC del livello di sicurezza «protezione molto elevata» occorre inoltre verificare l'efficacia delle misure attuate.

Art. 25 Nullaosta di sicurezza

¹ Dopo l'esecuzione della procedura di sicurezza, le autorità e organizzazioni assoggettate rilasciano il nullaosta per l'impiego del mezzo TIC.

² Con il nullaosta di sicurezza l'autorità o organizzazione accetta i rischi residui.

Art. 26 Inventario dei mezzi TIC

Le autorità e organizzazioni assoggettate provvedono affinché i loro mezzi TIC siano inventariati.

Art. 27 Sicurezza nell'esercizio

Le autorità e organizzazioni assoggettate che gestiscono mezzi TIC provvedono affinché nell'esercizio di tali mezzi sia garantita la sicurezza delle informazioni.

Sezione 4: Misure in materia di personale**Art. 28** Requisiti in materia di personale nella gestione di informazioni e mezzi TIC della Confederazione

Le autorità e organizzazioni assoggettate provvedono affinché le persone che, nel quadro dei loro compiti o di un mandato, gestiscono informazioni o mezzi TIC della Confederazione:

- a. siano scelte con cura;
- b. siano formate e frequentino formazioni continue conformi al rispettivo livello;
- c. se necessario, siano tenute a mantenere il segreto.

Art. 29 Rilascio restrittivo di autorizzazioni

¹ Le autorità e organizzazioni assoggettate provvedono affinché, per la gestione di informazioni e mezzi TIC nonché l'accesso a locali, siano rilasciate alle persone interessate soltanto le autorizzazioni necessarie per l'adempimento dei rispettivi compiti.

² Le autorizzazioni sono revocate non appena termina il rapporto di lavoro, il contratto o l'adempimento di un compito. Possono essere bloccate o revocate senza

preavviso se sussistono indizi concreti di un pericolo per la sicurezza delle informazioni.

³ Le autorità e organizzazioni assoggettate provvedono alla verifica periodica delle autorizzazioni.

Sezione 5: Protezione fisica di informazioni e mezzi TIC

Art. 30 Principi

¹ Le autorità e organizzazioni assoggettate provvedono, nei rispettivi locali, a una protezione fisica adeguata delle loro informazioni e dei loro mezzi TIC nei confronti di accessi non autorizzati nonché di danneggiamenti e disturbi.

² Provvedono affinché informazioni e mezzi TIC in settori pubblicamente accessibili siano adeguatamente protetti.

Art. 31 Zone di sicurezza

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

- a. vengono trattate frequentemente informazioni classificate «CONFIDENZIALE» o «SEGRETO»; o
- b. sono in esercizio mezzi TIC del livello di sicurezza «protezione elevata» o «protezione molto elevata».

² Provvedono affinché l'accesso alle zone di sicurezza sia concesso esclusivamente a persone identificate e autorizzate.

³ Sempre che sia necessario per garantire la sicurezza delle informazioni, nelle zone di sicurezza le autorità e organizzazioni assoggettate sono autorizzate a:

- a. impiegare metodi di verifica biometrici;
- b. proibire che siano presi con sé determinati oggetti, in particolare apparecchi di registrazione;
- c. sorvegliare settori sensibili sotto il profilo della sicurezza con apparecchi tecnici di registrazione;
- d. eseguire controlli di borse e persone;
- e. eseguire senza preavviso controlli di locali, anche in assenza degli impiegati.

⁴ In zone di sicurezza nelle quali sono trattate frequentemente informazioni classificate «SEGRETO» oppure sono in esercizio mezzi TIC del livello di sicurezza «protezione molto elevata», le autorità e organizzazioni assoggettate sono inoltre autorizzate a esercitare impianti di telecomunicazione che provocano interferenze

secondo l'articolo 34 capoverso 1^{er} della legge del 30 aprile 1997⁵ sulle telecomunicazioni.

⁵ Sono fatte salve le prescrizioni particolari per le zone di sicurezza conformemente ai trattati internazionali secondo l'articolo 90 nonché le prescrizioni per le zone di protezione di impianti secondo la legislazione sulla protezione di impianti militari.

Capitolo 3: Controllo di sicurezza relativo alle persone

Sezione 1: Scopo del controllo, persone da sottoporre al controllo e livelli di controllo

Art. 32 Scopo del controllo

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

Art. 33 Elenco delle funzioni con attività sensibili sotto il profilo della sicurezza

Le autorità assoggettate emanano, per il loro ambito di competenza, un elenco delle funzioni per l'adempimento dei cui compiti è necessario esercitare un'attività sensibile sotto il profilo della sicurezza.

Art. 34 Persone da sottoporre al controllo

¹ È eseguito un controllo di sicurezza relativo alle persone nei casi di:

- a. persone destinate a esercitare una funzione che figura in un elenco secondo l'articolo 33;
- b. persone che, per un'autorità o organizzazione assoggettata, sono destinate a eseguire un mandato che implica l'esercizio di un'attività sensibile sotto il profilo della sicurezza;
- c. persone che, sulla base di un trattato internazionale secondo l'articolo 90, devono essere sottoposte a un controllo di sicurezza relativo alle persone.

² Se un'autorità estera o 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 relativo alle persone se la Svizzera ha concluso con il Paese o l'organizzazione internazionale interessati un trattato internazionale secondo l'articolo 90.

³ Nel caso di persone che esercitano o sono destinate a esercitare una funzione che dovrebbe figurare in un elenco secondo l'articolo 33, ma che non vi figura ancora,

⁵ RS 784.10

può essere eseguito un controllo di sicurezza relativo alle persone con il consenso dell'autorità assoggettata. L'elenco delle funzioni dev'essere adeguato alla prossima occasione.

⁴ Nella loro qualità di membri di un'autorità non sono assoggettati al controllo di sicurezza relativo alle persone:

- a. i membri dell'Assemblea federale;
- b. i membri del Consiglio federale e il cancelliere della Confederazione;
- c. i giudici dei tribunali della Confederazione;
- d. il procuratore generale della Confederazione;
- e. i membri dell'autorità di vigilanza sul Ministero pubblico della Confederazione;
- f. i membri dei governi e dei tribunali cantonali.

Art. 35 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. 36 Servizi promotori

Le autorità assoggettate stabiliscono i servizi competenti per l'avvio dei controlli di sicurezza relativi alle persone (servizi promotori).

Art. 37 Consenso

¹ Un controllo di sicurezza relativo alle persone può essere eseguito unicamente con il consenso della persona da sottoporre al controllo.

² I controlli di sicurezza relativi alle persone per funzioni dell'esercito e della protezione civile possono essere eseguiti senza il consenso delle persone da sottoporre al controllo.

Art. 38 Momento del controllo di sicurezza relativo alle persone

¹ Nel caso di persone secondo l'articolo 34 capoverso 1 lettera a, il controllo di sicurezza relativo alle persone dev'essere avviato prima del conferimento della funzione.

² Nel caso di persone secondo l'articolo 34 capoverso 1 lettera a che devono essere proposte al Consiglio federale per la nomina, il controllo di sicurezza relativo alle persone dev'essere concluso prima che la persona sia proposta per la nomina.

³ Nel caso di persone secondo l'articolo 34 capoverso 1 lettera b, il controllo di sicurezza relativo alle persone dev'essere concluso prima che sia affidato loro l'esercizio dell'attività sensibile sotto il profilo della sicurezza.

⁴ Il momento del controllo di sicurezza relativo alle persone per coloro che devono essere sottoposti al controllo sulla base di trattati internazionali secondo l'articolo 90 si fonda sulle disposizioni del corrispondente trattato.

Art. 39 Acquisizione dei dati

¹ Per il controllo di sicurezza di base, i servizi specializzati per i controlli di sicurezza relativi alle persone (servizi specializzati CSP) competenti per la valutazione del rischio per la sicurezza possono acquisire dati sulla persona da sottoporre al controllo:

- a. dal casellario giudiziale;
- b. presso i competenti organi di perseguimento penale e tribunali, relativamente a procedimenti penali in corso, conclusi o abbandonati nonché ai relativi atti giudiziari e istruttori;
- c. presso gli organi di sicurezza della Confederazione, il Servizio delle attività informative della Confederazione, gli organi dell'esercito nonché altri organi della Confederazione, sempre che trattino dati necessari per la valutazione del rischio per la sicurezza;
- d. da registri e atti degli organi di sicurezza dei Cantoni e della polizia competente;
- e. dai registri delle autorità di esecuzione e fallimento;
- f. dagli atti di controlli di sicurezza relativi alle persone già avvenuti;
- g. da fonti pubblicamente accessibili.

² Per il controllo di sicurezza ampliato, i servizi specializzati CSP possono inoltre acquisire dati sulla persona da sottoporre al controllo:

- 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 interessata intrattiene relazioni d'affari;
- d. mediante l'audizione della persona interessata.

³ I servizi specializzati CSP possono chiedere a servizi esteri l'invio di dati corrispondenti ai dati secondo i capoversi 1 e 2.

⁴ Per la valutazione del rischio per la sicurezza, i servizi specializzati CSP devono potersi basare su una quantità sufficiente di dati relativi a un periodo di tempo adeguato.

⁵ Se dall'acquisizione dei dati risultano indicazioni su una circostanza rilevante in materia di sicurezza oppure per la valutazione non sono disponibili dati in quantità sufficiente relativi a un periodo di tempo adeguato, i servizi specializzati CSP possono interrogare al riguardo la persona da sottoporre al controllo. Con il consenso di quest'ultima possono interrogare anche terzi; essi non sono tenuti a dare informazioni.

⁶ Dati relativi a terzi che sono indissolubilmente connessi con i dati relativi alla persona da sottoporre al controllo possono essere trattati nella misura in cui ciò è indispensabile per la valutazione del rischio per la sicurezza. I servizi specializzati CSP informano i terzi interessati in merito a tale trattamento.

Art. 40 Assunzione dei costi

¹ Le autorità e organizzazioni di diritto pubblico presso i quali è consentito acquisire dati o che devono collaborare alla procedura, sono tenuti a fornire gratuitamente il loro concorso.

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

Art. 41 Abbandono della procedura

¹ I servizi specializzati CSP abbandonano la procedura di controllo se:

- a. la persona da sottoporre al controllo revoca il suo consenso o non collabora al controllo;
- b. per un altro motivo, la persona da sottoporre al controllo non entra più in considerazione per la funzione o il mandato.

² I servizi specializzati CSP comunicano l'abbandono della procedura di controllo alla persona interessata e al servizio promotore. La persona interessata è di conseguenza considerata «non controllata».

³ Se la procedura di controllo è abbandonata, tutti i dati e gli atti già acquisiti sono distrutti.

Sezione 3: Valutazione del rischio per la sicurezza

Art. 42 Rischio per la sicurezza

¹ Sussiste un rischio per la sicurezza se, sulla base dei dati acquisiti, vi sono indizi concreti che la persona sottoposta al controllo 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 relativi alle caratteristiche personali seguenti:

- a. mancanza di integrità personale o di affidabilità;
- b. ricattabilità o corrottibilità; o
- c. facoltà di giudizio o di decisione compromessa.

³ Il rischio per la sicurezza deve fondarsi, indipendentemente dalla colpa della persona sottoposta al controllo, su fatti connessi alla situazione personale di quest'ultima.

⁴ Per la valutazione del rischio per la sicurezza, i servizi specializzati CSP non sono vincolati a istruzioni.

Art. 43 Risultato della valutazione

¹ I servizi specializzati CSP rilasciano una delle dichiarazioni seguenti:

- 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 tuttavia essere adeguatamente ridotto mediante condizioni. I servizi specializzati CSP raccomandano le relative 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, i servizi specializzati CSP offrono alla persona sottoposta al controllo l'opportunità di esprimersi al riguardo.

Art. 44 Comunicazione della valutazione

¹ I servizi specializzati CSP comunicano per scritto la loro dichiarazione alla persona controllata nonché al servizio competente per l'attribuzione dell'attività sensibile sotto il profilo della sicurezza (servizio competente per l'attribuzione).

² Nel caso di persone nominate dal Consiglio federale, i servizi specializzati CSP comunicano le loro dichiarazioni al dipartimento proponente, a destinazione del Consiglio federale.

³ I servizi specializzati CSP possono informare sul risultato della valutazione i rispettivi servizi competenti per l'attribuzione 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 soggetto a una valutazione del potenziale di violenza secondo l'articolo 113 della legge militare del 3 febbraio 1995⁶ (LM).

⁴ I servizi specializzati CSP possono inoltre informare sul risultato della valutazione il servizio competente secondo l'articolo 113 LM per la cessione o il ritiro dell'arma militare personale.

Art. 45 Comunicazione di riscontri prima della conclusione del controllo di sicurezza relativo alle persone

Se già prima della conclusione della valutazione i servizi specializzati CSP dispongono di indizi concreti secondo i quali potrebbe sussistere un rischio per la sicurezza e vi è urgenza, possono informare per scritto in merito ai riscontri acquisiti fino a quel momento le autorità o i servizi secondo l'articolo 44 nonché la persona sottoposta al controllo.

Sezione 4: Conseguenze della valutazione

Art. 46 Esercizio dell'attività sensibile sotto il profilo della sicurezza

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

² Il servizio competente per l'attribuzione decide, dopo aver preso conoscenza della valutazione, 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.

Art. 47 Obbligo di comunicazione

L'autorità competente per l'attribuzione comunica per scritto al servizio specializzato CSP competente se:

- a. attribuisce l'esercizio dell'attività sensibile sotto il profilo della sicurezza a una persona per la quale è stata rilasciata una dichiarazione secondo l'articolo 43 capoverso 1 lettere c o d; o
- b. in occasione dell'attribuzione dell'attività sensibile sotto il profilo della sicurezza deroga alle condizioni raccomandate dal servizio specializzato CSP.

⁶ RS 510.10

Art. 48 Utilizzazione di una dichiarazione per altre attività

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

- a. un'altra attività sensibile sotto il profilo della sicurezza secondo la presente legge;
- b. un'attività secondo altre leggi federali per il cui esercizio è necessario una verifica dell'affidabilità.

Art. 49 Attestazione di sicurezza relativa alle persone nel contesto internazionale

Su richiesta, il servizio specializzato CSP competente rilascia un'attestazione di sicurezza relativa alle persone nel contesto internazionale se alla persona interessata ha rilasciato una corrispondente dichiarazione di sicurezza.

Art. 50 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 Se il servizio promotore o il servizio competente per l'attribuzione ha motivo di presumere che dall'ultimo controllo sono emersi nuovi rischi, può in ogni momento chiedere al competente servizio specializzato CSP, con motivazione scritta, la ripetizione del controllo di sicurezza relativo alle persone.

Art. 51 Tutela giurisdizionale

¹ Dopo il ricevimento della dichiarazione secondo l'articolo 43 capoverso 1, la persona controllata ha dieci giorni di tempo per:

- a. consultare i documenti del controllo;
- b. esigere la rettifica dei dati errati;
- c. esigere, nel caso di atti dei servizi specializzati, la soppressione di dati obsoleti;
- d. far apporre una menzione di contestazione.

² Per la limitazione della comunicazione delle informazioni si applica l'articolo 9 della legge federale del 19 giugno 1992⁷ sulla protezione dei dati (LPD).

⁷ RS 235.1

³ I servizi specializzati CSP emanano una decisione in merito ai risultati del loro controllo se la persona controllata lo richiede entro 30 giorni dal ricevimento della dichiarazione.

Sezione 5: Trattamento di dati personali

Art. 52 Sistema d'informazione per i controlli di sicurezza relativi alle persone

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

² Ciascun servizio specializzato CSP è responsabile, per i dati personali che tratta nel sistema d'informazione, che tale trattamento sia legale, appropriato e proporzionale.

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 LPD⁸, sempre che sia necessario per la valutazione del rischio per la sicurezza.

⁴ Il sistema d'informazione contiene i dati seguenti:

- a. dati sull'identità delle persone da sottoporre al controllo o controllate;
- b. i dati acquisiti secondo l'articolo 39 per il controllo di sicurezza relativo alle persone;
- c. la valutazione del rischio per la sicurezza;
- d. il risultato della valutazione secondo l'articolo 43 capoverso 1 con l'identità, l'indirizzo, il numero di assicurato AVS, il livello di controllo, la data e la data di scadenza;
- e. la decisione del servizio competente per l'attribuzione;
- f. dati e atti di eventuali procedure di ricorso;
- g. elenchi e statistiche che contengono i dati secondo le lettere a-f.

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

Art. 53 Comunicazione dei dati

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

- a. i servizi specializzati CSP: a tutti i dati di cui all'articolo 52 capoverso 4;
- b. i servizi promotori secondo l'articolo 36: ai dati di cui all'articolo 52 capoverso 4 lettera b che hanno registrato essi stessi in occasione dell'avvio del controllo nonché ai dati di cui all'articolo 52 capoverso 4 lettere a, d ed e;

- c. i servizi competenti per l'attribuzione secondo l'articolo 44 capoverso 1: ai dati di cui all'articolo 52 capoverso 4 lettere a, d e e;
- d. gli incaricati della sicurezza delle informazioni secondo l'articolo 84, per l'adempimento dei loro compiti di controllo: ai dati di cui all'articolo 52 capoverso 4 lettere a, d e e;
- e. i servizi della Confederazione e dei Cantoni presso i quali sono acquisiti dati secondo l'articolo 39, in qualità di mandato di fornitura dei corrispondenti dati: i dati di cui all'articolo 52 capoverso 4 lettera a.

² I servizi seguenti hanno accesso, tramite un'interfaccia, ai dati di cui all'articolo 52 capoverso 4 lettera d per gli scopi indicati qui appresso:

- a. il servizio specializzato SA secondo l'articolo 59, tramite un'interfaccia con il sistema d'informazione secondo l'articolo 77, per l'esecuzione della procedura di sicurezza relativa alle aziende;
- b. lo Stato maggiore dell'esercito, tramite un'interfaccia con il sistema d'informazione secondo gli articoli 156-161 della legge federale del 3 ottobre 2008⁹ sui sistemi d'informazione militari (LSIM), per il trattamento di domande di visite all'estero con accesso a informazioni classificate;
- c. lo Stato maggiore di condotta dell'esercito:
 - 1. tramite un'interfaccia con il sistema d'informazione secondo gli articoli 162-167 LSIM, per il controllo dell'accesso alle zone di sicurezza secondo l'articolo 31 o a impianti secondo la legislazione sulla protezione degli impianti militari,
 - 2. tramite un'interfaccia con il sistema d'informazione secondo gli articoli 12-17 LSIM, per l'adempimento dei suoi compiti legali secondo l'articolo 13 LSIM,
 - 3. tramite un'interfaccia con il sistema d'informazione secondo gli articoli 18-23 LSIM, per l'esecuzione del reclutamento delle persone soggette all'obbligo di leva e del personale previsto per il promovimento della pace.

³ Il servizio specializzato CSP può inoltre comunicare elettronicamente ad altre organizzazioni della Confederazione dati di cui all'articolo 52 capoverso 3 lettera d, se tali dati sono necessari per il controllo dell'accesso a zone di sicurezza secondo l'articolo 31.

⁴ I servizi specializzati CSP possono comunicare alle autorità e organizzazioni assoggettate elenchi e statistiche secondo il capoverso 1 lettera g, sempre che tali dati siano necessari per l'adempimento dei rispettivi compiti di controllo secondo la presente legge. Gli elenchi e le statistiche possono contenere soltanto dati personali provenienti dagli ambiti di competenza dell'autorità o organizzazione interessata.

⁹ RS 510.91

Art. 54 Conservazione e distruzione dei dati

¹ I servizi specializzati CSP possono registrare le audizioni secondo l'articolo 39 capoversi 2 lettera d e 5 con apparecchi tecnici e conservare le registrazioni su corrispondenti supporti di dati.

² Conservano i dati fintanto che la persona interessata esercita la funzione o elabora il mandato, ma al più tardi per dieci anni.

³ Se una persona controllata non assume la funzione prevista o rifiuta di elaborare il mandato previsto, tutti i dati e gli atti vengono distrutti.

⁴ I servizi specializzati CSP distruggono inoltre senza indugio i dati:

- a. che non corrispondono allo scopo del trattamento;
- b. il cui trattamento non è lecito per altri motivi; o
- c. sono inesatti.

⁵ Nel caso di dati conservati al di fuori del sistema d'informazione, i servizi specializzati CSP distruggono contemporaneamente le corrispondenti menzioni di trattamento di cui all'articolo 52 capoverso 5.

⁶ È fatta salva l'archiviazione dei dati secondo le prescrizioni della legislazione sull'archiviazione.

Sezione 6: Disposizioni complete del Consiglio federale**Art. 55**

Il Consiglio federale emana disposizioni complete su:

- a. la procedura del controllo di sicurezza relativo alle persone;
- b. l'organizzazione dei servizi specializzati CSP;
- c. la responsabilità della protezione dei dati in relazione con il sistema d'informazione di cui all'articolo 52;
- d. la sicurezza dei dati;
- e. il controllo indipendente periodico del trattamento legale dei dati personali.

Capitolo 4: Procedura di sicurezza relativa alle aziende**Sezione 1: Disposizioni generali****Art. 56** Scopo della procedura

La procedura di sicurezza relativa alle aziende ha lo scopo di tutelare la sicurezza delle informazioni in occasione dell'aggiudicazione di mandati pubblici a imprese o loro parti (aziende), nella misura in cui tali mandati comportano l'esercizio di

un'attività sensibile sotto il profilo della sicurezza (mandati sensibili sotto il profilo della sicurezza).

Art. 57 Aziende interessate

¹ È eseguita una procedura di sicurezza relativa alle aziende nel caso di aziende:

- a. destinate a eseguire un mandato, sensibile sotto il profilo della sicurezza, di un'autorità o organizzazione assoggettata;
- b. che hanno sede in Svizzera e si candidano per mandati di autorità estere o internazionali per la cui esecuzione è necessaria un'attestazione di sicurezza relativa alle aziende secondo l'articolo 73.

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. 58 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 ottiene l'aggiudicazione; o
- d. per un altro motivo non entra più in considerazione per il mandato.

² Se la procedura è abbandonata, tutti i relativi dati e atti sono distrutti.

Sezione 2: Avvio della procedura, requisiti di sicurezza

Art. 59 Domanda di avvio della procedura

¹ Se intendono assegnare un mandato sensibile sotto il profilo della sicurezza, le autorità e organizzazioni assoggettate domandano l'avvio della procedura al servizio specializzato per la sicurezza aziendale (servizio specializzato SA), competente per l'esecuzione della procedura di sicurezza relativa alle aziende.

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

³ Nel caso di mandati esteri o internazionali, la domanda è presentata dall'autorità estera o internazionale competente.

Art. 60 Esame della domanda

¹ Se le condizioni per l'esecuzione di una procedura di sicurezza relativa alle aziende sono adempite, il servizio specializzato SA avvia la procedura.

² Il servizio specializzato SA può rinunciare all'avvio della procedura se il rischio per la sicurezza può essere adeguatamente ridotto con altre misure. Esso raccomanda misure in tal senso.

Art. 61 Definizione dei requisiti di sicurezza

Dopo l'avvio della procedura, il servizio specializzato SA, d'intesa con l'autorità o organizzazione che aggiudica il mandato (mandante), definisce i requisiti in materia di sicurezza delle informazioni per la procedura di aggiudicazione nonché per l'adempimento del mandato.

Sezione 3: Idoneità delle aziende in relazione alla sicurezza delle informazioni

Art. 62 Valutazione dell'idoneità

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

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

³ Nella valutazione dell'idoneità delle aziende, il servizio specializzato SA non è vincolato a istruzioni.

Art. 63 Acquisizione dei dati

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

- a. presso l'azienda;
- b. presso il Servizio delle attività informative della Confederazione;
- c. da fonti pubblicamente accessibili.

² Può chiedere a servizi esteri l'invio di dati che corrispondono ai dati secondo il capoverso 1.

Art. 64 Rischio per la sicurezza

¹ Sussiste un rischio per la sicurezza quando, sulla base dei dati acquisiti, vi sono indizi concreti che l'azienda con elevata probabilità eserciterà in maniera contraria alle prescrizioni o non appropriata l'attività sensibile in materia di sicurezza.

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

- a. l'azienda presenta un'integrità o un'affidabilità carenti;

- 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 dell'azienda indispensabili all'esecuzione del mandato sensibile sotto il profilo della sicurezza è stata rilasciata una dichiarazione di rischio secondo l'articolo 43 capoverso 1 lettera c.

³ Il rischio per la sicurezza, a prescindere da una colpa, dev'essere motivato da circostanze e situazioni effettive dell'azienda interessata.

Art. 65 Notifica della valutazione e 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 sotto il profilo della sicurezza rappresenta un rischio per la sicurezza, il mandante esclude l'azienda interessata dalla procedura di aggiudicazione.

Sezione 4: Concetto in materia di sicurezza, dichiarazione di sicurezza aziendale

Art. 66 Concetto in materia di sicurezza

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

² Il servizio specializzato SA allestisce un concetto in materia di sicurezza per l'azienda.

³ Può acquisire i dati necessari al riguardo per scritto oppure mediante una visita dell'azienda.

Art. 67 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 secondo l'articolo 46 capoverso 2.

Art. 68 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 concetto in materia di sicurezza.

² Rifiuta di rilasciare all'azienda la dichiarazione di sicurezza aziendale e abbandona la procedura di sicurezza relativa alle aziende se essa non attua il concetto in materia di sicurezza. Esso emana una corrispondente decisione.

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

⁴ La dichiarazione di sicurezza aziendale è valida cinque anni.

Sezione 5: Conseguenze della dichiarazione di sicurezza aziendale

Art. 69 Esecuzione del mandato sensibile sotto il profilo della sicurezza

Il mandante è vincolato alla decisione del servizio specializzato SA. Può autorizzare l'esecuzione del mandato sensibile sotto il profilo della sicurezza soltanto dopo il rilascio della dichiarazione di sicurezza aziendale.

Art. 70 Obblighi dell'azienda

¹ Le aziende titolari di una dichiarazione di sicurezza aziendale devono applicare in permanenza le misure del concetto 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. 71 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 sotto il profilo della sicurezza;
- b. consultare 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 materiali.

Art. 72 Procedura semplificata in caso di aggiudicazione di altri mandati sensibili sotto il profilo della sicurezza

¹ In caso di aggiudicazione di altri mandati sensibili sotto il profilo della sicurezza, le aziende titolari di una dichiarazione di sicurezza aziendale sono considerate idonee ai sensi dell'articolo 62.

² Qualora una tale azienda si aggiudicasse il mandato, il servizio specializzato SA verifica se il concetto in materia di sicurezza in vigore dev'essere adeguato.

Art. 73 Attestazione di sicurezza relativa alle aziende nel contesto internazionale

Su richiesta dell'azienda interessata, il servizio specializzato SA rilascia un'attestazione di sicurezza relativa alle aziende nel contesto internazionale.

Sezione 6: Revoca della dichiarazione di sicurezza aziendale, ripetizione della procedura e tutela giurisdizionale

Art. 74 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 70;
- b. nel quadro di una ripetizione della procedura emerge un rischio per la sicurezza.

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

Art. 75 Ripetizione della procedura

La procedura di sicurezza relativa alle aziende è ripetuta se:

- a. dopo la scadenza della dichiarazione di sicurezza aziendale è ancora pendente un mandato sensibile sotto il profilo della sicurezza;
- b. vi è un motivo concreto per presumere che in seguito a cambiamenti sostanziali in seno all'azienda sono emersi nuovi rischi per la sicurezza.

Art. 76 Tutela giurisdizionale

¹ Dopo la notifica delle decisioni del servizio specializzato SA, gli organi dell'azienda hanno dieci giorni di tempo per:

- a. consultare i documenti;
- b. esigere la rettifica dei dati errati;
- c. esigere, nel caso di atti del servizio specializzato SA, la soppressione di dati obsoleti;
- d. far apporre una menzione di contestazione.

² Per la limitazione della comunicazione delle informazioni si applica l'articolo 9 della legge federale del 19 giugno 1992¹⁰ sulla protezione dei dati (LPD).

³ Contro le decisioni del servizio specializzato SA è ammesso il ricorso al Tribunale amministrativo federale.

¹⁰ RS 235.1

Sezione 7: Trattamento dei dati personali

Art. 77 Sistema d'informazione per la procedura di sicurezza relativa alle aziende

¹ Il servizio specializzato SA impiega un sistema d'informazione per l'esecuzione della procedura di sicurezza relativa alle aziende e dei corrispondenti controlli di sicurezza relativi alle persone.

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 LPD¹¹, sempre che ciò sia necessario per l'esecuzione della procedura di sicurezza relativa alle aziende.

³ Il sistema d'informazione contiene i dati seguenti:

- a. i dati acquisiti per la procedura di sicurezza relativa alle aziende secondo gli articoli 63 e 66 capoverso 3;
- b. il risultato della valutazione secondo l'articolo 62 capoverso 2;
- c. i risultati dei controlli di sicurezza relativi alle persone necessari per la procedura di sicurezza relativa alle aziende secondo l'articolo 67 capoverso 1;
- d. la decisione del servizio specializzato SA secondo l'articolo 67 capoverso 2;
- e. i nomi di tutte le aziende titolari di una dichiarazione di sicurezza aziendale, compresa la data del rilascio;
- f. le misure risultanti da eventuali controlli secondo l'articolo 71;
- g. dati e atti di eventuali procedure di ricorso.

⁴ Il servizio specializzato SA è responsabile della sicurezza del sistema d'informazione nonché del trattamento legale, adeguato e proporzionale dei dati personali.

Art. 78 Comunicazione dei dati

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

- a. i mandanti secondo l'articolo 61: ai dati di cui all'articolo 77 capoverso 3 lettere b e d-g;
- b. le aziende interessate, sempre che siano state autorizzate dal Consiglio federale, sulla base dell'articolo 36, ad avviare controlli di sicurezza relativi alle persone nel rispettivo ambito di competenza: ai dati di cui all'articolo 77 capoverso 3 lettere c e d.

¹¹ RS 235.1

Art. 79 Conservazione e distruzione dei dati

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

² Distrugge senza indugio i dati che:

- a. non corrispondono allo scopo del trattamento;
- b. il cui trattamento non è ammesso per altri motivi; oppure
- c. sono inesatti.

³ È fatta salva l'archiviazione dei dati secondo le prescrizioni della legislazione sull'archiviazione.

Sezione 8: Disposizioni complete del Consiglio federale**Art. 80**

Il Consiglio federale emana disposizioni complete su:

- a. la procedura di sicurezza relativa alle aziende;
- b. il trattamento dei dati, il sistema d'informazione e la sicurezza dei dati;
- c. l'organizzazione del servizio specializzato SA.

Capitolo 5: Sicurezza delle informazioni nelle infrastrutture critiche**Art. 81** Compiti della Confederazione

¹ Nel campo della sicurezza delle informazioni, la Confederazione sostiene i gestori di infrastrutture critiche, in particolare:

- a. nell'identificazione tempestiva e nella valutazione di minacce e pericoli;
- b. nell'individuazione di incidenti;
- c. nella tutela e nel ripristino della sicurezza delle informazioni dopo un incidente;
- d. nell'analisi di incidenti.

² Gestisce un servizio nazionale di preallerta e un punto di contatto per misure preventive e reattive nell'ambito della sicurezza tecnica delle informazioni.

³ Provvede affinché i gestori di infrastrutture critiche possano scambiare in maniera sicura, con i competenti servizi della Confederazione e tra loro, informazioni su minacce, rischi e incidenti.

Art. 82 Trattamento di dati personali

¹ Per sventare pericoli, i servizi competenti ai sensi dell'articolo 81 possono trattare dati personali, in particolare elementi d'indirizzo nel settore delle telecomunicazioni, e comunicarli alle autorità e organizzazioni assoggettate, ai servizi competenti dei Cantoni e a terzi, sempre che sia necessario per l'adempimento dei rispettivi compiti. Il trattamento può avvenire all'insaputa delle persone interessate.

² Il capoverso 1 si applica anche a dati personali degni di particolare protezione connessi con procedimenti e sanzioni di carattere amministrativo o penale.

³ I gestori di mezzi TIC e i fornitori di servizi TIC, all'insaputa delle persone interessate, possono comunicare ai servizi competenti ai sensi dell'articolo 81 dati personali secondo il capoverso 1 inerenti al singolo incidente. Tali dati non possono essere utilizzati per procedimenti giudiziari.

Art. 83 Disposizioni complete del Consiglio federale

Il Consiglio federale emana disposizioni complete su:

- a. la ripartizione dei compiti e la collaborazione tra i servizi che assumono i compiti secondo l'articolo 81 e il Servizio delle attività informative della Confederazione;
- b. lo scambio di informazioni di intelligence da parte dei servizi di cui alla lettera a e la comunicazione di tali informazioni a gestori di infrastrutture critiche;
- c. il trattamento dei dati da parte dei servizi che assumono i compiti secondo l'articolo 81, nonché la sicurezza dei dati.

Capitolo 6: Organizzazione ed esecuzione**Sezione 1: Organizzazione****Art. 84** 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 loro ambito nell'adempimento dei rispettivi compiti e obblighi secondo la presente legge;

- b. dirigono per incarico della rispettiva autorità o organizzazione l'organizzazione specialistica in materia di sicurezza delle informazioni nonché la gestione dei rischi;
- c. verificano regolarmente il rispetto delle direttive in materia di sicurezza delle informazioni, redigono rapporti e propongono alle rispettive autorità le misure necessarie;
- d. possono annunciare incidenti rilevanti sotto il profilo della sicurezza al servizio specializzato della Confederazione per la sicurezza delle informazioni, alla conferenza degli incaricati della sicurezza delle informazioni nonché ai servizi che assumono i compiti secondo l'articolo 81.

³ Non è consentito attribuire agli incaricati della sicurezza delle informazioni compiti tali da determinare un conflitto di interessi con i compiti secondo il capoverso 2.

Art. 85 Conferenza degli incaricati della sicurezza delle informazioni

¹ Gli incaricati della sicurezza delle informazioni secondo l'articolo 84 capoverso 1 formano una conferenza.

² La conferenza assume i compiti seguenti:

- a. promuove l'esecuzione uniforme della presente legge da parte di tutte le autorità;
- b. 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;
- c. 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;
- d. provvede al coordinamento con l'incaricato federale della protezione dei dati e della trasparenza nonché con altri servizi che assumono compiti nell'ambito della sicurezza delle informazioni.

³ La conferenza emana un regolamento interno.

Art. 86 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 e i loro incaricati della sicurezza delle informazioni nell'esecuzione della presente legge, in particolare nella direzione della sicurezza delle informazioni e nella gestione dei rischi;
- b. raccomanda misure immediate in caso di minaccia per la sicurezza delle informazioni della Confederazione;
- c. esegue controlli e verifiche su incarico delle autorità assoggettate;

- d. valuta, su incarico delle autorità assoggettate, i rischi per la sicurezza delle informazioni in occasione dell'impiego di nuove tecnologie;
- e. su richiesta delle autorità e organizzazioni assoggettate, verifica, per quanto riguarda aspetti rilevanti sotto il profilo della sicurezza, l'idoneità di determinati processi, mezzi, installazioni, oggetti e prestazioni;
- f. dirige e coordina, su richiesta delle autorità assoggettate, l'ambito della sicurezza delle informazioni in occasione di progetti importanti che coinvolgono più autorità;
- g. è l'interlocutore per i contatti specializzati nel campo della sicurezza delle informazioni con servizi svizzeri, esteri e internazionali;
- h. redige annualmente per il Consiglio federale un rapporto sullo stato della sicurezza delle informazioni in seno alla Confederazione.

² L'incaricato del Consiglio federale per la sicurezza delle informazioni è contemporaneamente il responsabile del 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.

Sezione 2: Esecuzione

Art. 87 Disposizioni esecutive

¹ Le autorità assoggettate sono incaricate di emanare le disposizioni esecutive necessarie per l'esecuzione 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, per il proprio ambito di competenza, non emanino disposizioni esecutive proprie secondo il capoverso 1.

⁴ Il Consiglio federale stabilisce per via di ordinanza quali organizzazioni secondo l'articolo 2 capoverso 2 lettera e applicano totalmente o parzialmente la presente legge.

Art. 88 Requisiti e misure standard

¹ Il Consiglio federale stabilisce, secondo lo stato della dottrina e della tecnica, requisiti di sicurezza standardizzati nonché misure organizzative, di personale, tecniche ed edili standardizzate in materia di sicurezza delle informazioni.

² Può delegare tale compito al servizio specializzato della Confederazione per la sicurezza delle informazioni o a altri servizi competenti sotto il profilo tecnico.

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

Art. 89 Cantoni

¹ I Cantoni provvedono affinché le autorità e i servizi cantonali che esercitano attività sensibili sotto il profilo della sicurezza su mandato della Confederazione e sotto la vigilanza di quest'ultima applichino le misure secondo la presente legge.

² Il Consiglio federale disciplina:

- a. i controlli di sicurezza relativi alle persone per gli organi cantonali;
- b. il controllo delle misure secondo il capoverso 1.

³ Per le questioni inerenti alla sicurezza delle informazioni, i Cantoni designano ciascuno un servizio quale interlocutore delle autorità federali.

Art. 90 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, carenze e incidenti in tale ambito, in particolare per quanto riguarda le infrastrutture critiche;
- b. lo scambio di informazioni classificate;
- c. l'esecuzione reciproca di controlli di sicurezza relativi alle persone e di procedure di sicurezza relative alle aziende;
- d. il riconoscimento reciproco di dichiarazioni di sicurezza;
- e. l'esecuzione di controlli reciproci.

Art. 91 Valutazione

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

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

Capitolo 7: Disposizioni finali

Art. 92 Modifica di altri atti normativi

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

Art. 93 Disposizioni transitorie

¹ Le dichiarazioni di sicurezza relative alle persone e le dichiarazioni di sicurezza aziendali secondo il diritto anteriore mantengono la loro validità fino alla loro scadenza.

² Il Consiglio federale stabilisce i termini transitori per l'adeguamento:

- a. delle prescrizioni sulla classificazione;
- b. delle prescrizioni sulla sicurezza nell'impiego di mezzi TIC.

Art. 94 Referendum ed entrata in vigore

¹ La presente legge sottostà a referendum facoltativo.

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

Avamprogetto del 26.3.2014

Allegato
(art. 92)

Modifica di altri atti normativi

1. Legge federale del 21 marzo 1997¹² sulle misure per la salvaguardia della sicurezza interna

Art. 2 cpv. 4 lett. c

Abrogata

Art. 19-21

Abrogati

2. Legge del 26 giugno 1998¹³ sull'archiviazione

Art. 6 cpv. 2

² Prima della consegna all'Archivio federale i documenti classificati devono essere declassificati secondo le disposizioni della legislazione sulla sicurezza delle informazioni.

3. Legge del 24 marzo 2000¹⁴ 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 dagli impiegati la presentazione di un estratto del casellario giudiziale e del registro delle esecuzioni qualora ciò sia necessario per la tutela degli interessi del datore di lavoro.

Art. 20b Verifica dell'affidabilità

¹ Il Consiglio federale può far verificare l'affidabilità dei candidati a un impiego e degli impiegati 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;

¹² RS 120

¹³ RS 152.1

¹⁴ RS 172.220.1

- b. sono destinati a esercitare competenze decisionali o compiti di vigilanza in affari finanziari o fiscali essenziali e in tale contesto potrebbero pregiudicare considerevolmente gli interessi finanziari della Confederazione.

² Il Consiglio federale stabilisce quali funzioni sono soggette alla verifica. In tale ambito si limita al minimo indispensabile per la tutela degli interessi della Confederazione.

³ La procedura di verifica si fonda per analogia sulle disposizioni concernenti il controllo di sicurezza relativo alle persone della legge federale del ... ¹⁵ sulla sicurezza delle informazioni.

⁴ Se i candidati a un impiego e gli impiegati di cui al capoverso 1 sono sottoposti contemporaneamente a un controllo di sicurezza relativo alle persone secondo la legge federale sulla sicurezza delle informazioni, le due procedure sono riunite.

4. Codice penale svizzero del 21 dicembre 1937¹⁶

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 federale del ... ¹⁷ sulla sicurezza delle informazioni e verifiche dell'affidabilità secondo la legislazione speciale;

Art. 367 cpv. 2 lett. i e cpv. 2^{bis} lett. b

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 per i controlli di sicurezza relativi alle persone secondo la legge federale sulla sicurezza delle informazioni;

^{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 per i controlli di sicurezza relativi alle persone secondo la legge federale sulla sicurezza delle informazioni;

5. Legge federale del 13 giugno 2008¹⁸ sui sistemi d'informazione di polizia della Confederazione

¹⁵ RS ...

¹⁶ RS 311.0

¹⁷ RS ...

Art. 15 cpv. 4 lett. f

⁴ Nell'adempimento dei loro compiti, le autorità seguenti possono consultare i dati del sistema informatizzato mediante procedura di richiamo:

- f. i servizi specializzati per i controlli di sicurezza relativi alle persone secondo la legge federale del ... ¹⁹ sulla sicurezza delle informazioni, per la valutazione del rischio per la sicurezza nel quadro di un controllo di sicurezza relativo alle persone, una verifica dell'affidabilità o una valutazione del potenziale di violenza;

Art. 17 cpv. 4 lett. l

⁴ Hanno accesso a questi dati mediante procedura di richiamo informatizzata:

- l. i servizi specializzati per i controlli di sicurezza relativi alle persone secondo la legge federale del ... ²⁰ sulla sicurezza delle informazioni, per la valutazione del rischio per la sicurezza nel quadro di un controllo di sicurezza relativo alle persone, una verifica dell'affidabilità o una valutazione del potenziale di violenza;

6. Legge federale del 3 febbraio 1995²¹ sull'esercito e sull'amministrazione militare

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 esercitare competenze decisionali o 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. In tale ambito si limita al minimo indispensabile per la tutela degli interessi della Confederazione.

³ La procedura di verifica si fonda per analogia sulle disposizioni concernenti il controllo di sicurezza relativo alle persone della legge federale del ... ²² sulla sicurezza delle informazioni.

¹⁸ RS 361

¹⁹ RS ...

²⁰ RS ...

²¹ RS 510.10

⁴ Se i militari di cui al capoverso 1 sono sottoposti contemporaneamente a un controllo di sicurezza relativo alle persone secondo la legge federale sulla sicurezza delle informazioni, le due procedure sono riunite.

Art. 113 cpv. 5

⁵ La procedura si fonda per analogia sulle disposizioni relative al controllo di sicurezza di base secondo l'articolo 35 lettera a della legge federale del ...²³ sulla sicurezza delle informazioni. 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

7. Legge federale del 3 ottobre 2008²⁴ sui sistemi d'informazione militari

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

Abrogate

8. Legge federale del 21 marzo 2003²⁵ sull'energia nucleare

Art. 5 cpv. 3

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. Nella misura del necessario, questi provvedimenti sono classificati ed elaborati secondo le disposizioni della legge federale del ...²⁶ sulla sicurezza delle informazioni.

Art. 24 Verifica dell'affidabilità

¹ Ai fini della valutazione del rischio per la sicurezza, le persone che adempiono compiti essenziali in materia di sicurezza nucleare interna o esterna sono sottoposte a una verifica della loro affidabilità.

²² RS ...

²³ RS ...

²⁴ RS **510.91**

²⁵ RS **732.1**

²⁶ RS ...

² Il Consiglio federale stabilisce quali gruppi di persone sono soggetti alla verifica.

³ La procedura di verifica si fonda per analogia sulle disposizioni concernenti il controllo di sicurezza relativo alle persone della legge federale del ...²⁷ sulla sicurezza delle informazioni.

⁴ I dati della verifica possono essere comunicati al proprietario dell'impianto e all'autorità di vigilanza.

9. Legge del 23 marzo 2007²⁸ sull'approvvigionamento elettrico

Titolo prima dell'art. 25

Capitolo 6: Obbligo d'informare, segreto d'ufficio e di affari, verifica dell'affidabilità, tassa di vigilanza

Art. 26a 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. In tale ambito si limita al minimo indispensabile.

³ La procedura di verifica si fonda per analogia sulle disposizioni concernenti il controllo di sicurezza relativo alle persone della legge federale del ...²⁹ sulla sicurezza delle informazioni.

⁴ I dati della verifica possono essere comunicati alla direzione della società nazionale di rete, all'Ufficio federale e alla ElCom.

²⁷ RS ...

²⁸ RS 734.7

²⁹ RS ...

10. Legge federale del 3 ottobre 2003³⁰ sulla Banca nazionale svizzera

Art. 16, rubrica e cpv. 5

Confidenzialità e sicurezza delle informazioni

⁵ La Banca nazionale svizzera applica nel proprio ambito la legge federale del ... ³¹ sulla sicurezza delle informazioni. Del rimanente si applicano le disposizioni della legge federale del 19 giugno 1992 sulla protezione dei dati.

³⁰ RS **951.11**

³¹ RS ...

Avamprogetto del 26.3.2014