Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

FF 2020
www.dirittofederale.admin.ch
La versione elettronica firmata
è quella determinante

Termine di referendum: 10 aprile 2021 (1° giorno feriale: 12 aprile 2021)

Legge federale sulla sicurezza delle informazioni in seno alla Confederazione

(Legge sulla sicurezza delle informazioni, LSIn)

del 18 dicembre 2020

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 il trattamento sicuro delle informazioni di competenza della Confederazione nonché l'impiego sicuro 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 organizzazioni della Confederazione;

b. la sicurezza interna ed esterna della Svizzera;

c. gli interessi della politica estera della Svizzera;

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

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

RS **126**
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. l'Assemblea federale;

b. il Consiglio federale;

c. i tribunali della Confederazione;

d. il Ministero pubblico della Confederazione e l'Autorità di vigilanza sul Ministero pubblico della Confederazione;

e. la Banca nazionale svizzera.

2 Si applica alle organizzazioni seguenti (organizzazioni assoggettate):

a. i Servizi del Parlamento;

b. l'Amministrazione federale;

c. le amministrazioni dei tribunali della Confederazione;

d. l'esercito;

e. le 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 per le organizzazioni di cui all'articolo 2 capoversi 3 e 4 LOGA a quelle che:

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

b. per l'adempimento dei loro compiti impiegano o accedono a mezzi informatici della Confederazione.

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 o privato che gestiscono infrastrutture critiche ma che non sono contemplate ai capoversi 1–3 si applicano gli articoli 74–80. La legislazione speciale può dichiarare applicabili altre disposizioni della presente legge.

Art. 3 Applicabilità ai Cantoni

1 Ai Cantoni si applicano unicamente le disposizioni concernenti:

a. le informazioni classificate, qualora essi trattino informazioni classificate della Confederazione; e

b. la sicurezza nell'impiego dei mezzi informatici, qualora essi accedano a mezzi informatici della Confederazione.

2 Le disposizioni di cui al capoverso 1 non si applicano se 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 disciplinata anche in altre leggi federali, le disposizioni della presente legge si applicano a titolo completivo.

Art. 5 Definizioni

Ai sensi della presente legge s'intende per:

a. *mezzi informatici:* mezzi delle tecnologie dell'informazione e della comunicazione, segnatamente applicazioni, sistemi d'informazione e collezioni di dati nonché installazioni, prodotti e servizi che servono all'elaborazione elettronica delle 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» o «protezione molto elevata»,
   3. l'accesso a zone di sicurezza, in particolare alle zone di protezione 2 o 3 di un'opera secondo la legislazione sulla protezione delle opere militari;

c. *infrastrutture critiche:* le infrastrutture per l'approvvigionamento di acqua potabile e di energia, le infrastrutture nei settori dell'informazione, della comunicazione e dei trasporti nonché altri processi, sistemi e installazioni essenziali per il funzionamento dell'economia e per il benessere della popolazione.

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 dalle perturbazioni.

4 Al riguardo, tengono conto dei principi di adeguatezza, economicità e facilità d'uso.

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 rispettivo 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 accettabile.

3 I rischi considerati accettabili devono essere formalmente accettati.

Art. 9 Collaborazione con terzi

1 Le autorità e organizzazioni assoggettate che collaborano con terzi provvedono affinché i requisiti e le misure previsti dalla 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 ridotte al minimo.

2 Le autorità assoggettate provvedono affinché in vista di eventuali violazioni gravi della sicurezza delle informazioni, tali da compromettere l'adempimento di compiti indispensabili della Confederazione, siano stabilite pianificazioni preventive e svolte 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 ridotta allo stretto necessario e per quanto possibile limitata nel tempo.

Art. 12 Competenze

1 Le autorità assoggettate designano le persone e i servizi competenti per la classificazione delle informazioni (servizi incaricati 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.

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 che:

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

b. dispongono 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 87.

Art. 15 Accesso a informazioni classificate nell'ambito di 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 di decidere 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 nell'impiego di mezzi informatici

Art. 16 Procedura di sicurezza

1 Le autorità assoggettate stabiliscono una procedura per garantire la sicurezza delle informazioni nell'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 rilascio del 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 od 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. la loro utilizzazione abusiva o la loro perturbazione 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;

b. la loro utilizzazione abusiva o la loro perturbazione 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 Per i mezzi informatici del livello di sicurezza «protezione molto elevata» l'efficacia delle misure 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 od 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 relative alle persone

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. seguano formazioni e formazioni continue adeguate al loro 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 allo scadere dell'autorizzazione d'accesso.

3 Come identificatore di persone possono inoltre utilizzare sistematicamente il numero d'assicurato di cui all'articolo 50*c* della legge federale del 20 dicembre 1946[6] sull'assicurazione per la vecchiaia e per i superstiti (numero d'assicurato AVS).

5 RS **172.010**
6 RS **831.10**

Art. 21 Criteri restrittivi per il rilascio di autorizzazioni

1 Le autorità e organizzazioni assoggettate provvedono affinché 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.

2 Le autorizzazioni sono revocate al termine del rapporto di lavoro o del contratto oppure all'adempimento del compito. 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 garantire una protezione fisica adeguata delle informazioni e dei mezzi informatici di cui sono responsabili contro gli abusi e le perturbazioni.

Art. 23 Zone di sicurezza

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

a. sono 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 l'introduzione di determinati oggetti, in particolare apparecchi per registrazioni audiovisive;

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

c. eseguire perquisizioni di borse e persone;

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

3 Nelle 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 operare impianti di telecomunicazione che provocano interferenze secondo l'articolo 34 capoverso 1ter della legge del 30 aprile 1997[7] sulle telecomunicazioni (LTC).

4 Sono fatte salve le prescrizioni particolari per le zone di sicurezza definite in virtù di trattati internazionali secondo l'articolo 87 nonché le prescrizioni applicabili alle

7 RS **784.10**

zone di protezione di opere secondo la legislazione sulla protezione delle opere militari.

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 questi 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 i sistemi d'informazione collegati, con registri di persone e di utenti nonché con altri sistemi di gestione delle identità di autorità assoggettate.

2 Lo scambio e l'armonizzazione sono limitati ai dati il cui trattamento è autorizzato nel rispettivo sistema.

Art. 26 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.

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

Art. 27 Scopo e contenuto del controllo

1 Il controllo di sicurezza relativo alle persone serve a valutare se l'esercizio di un'attività sensibile sotto il profilo della sicurezza da parte di una persona, nel quadro della sua funzione o di un mandato, possa costituire un rischio per la sicurezza delle informazioni.

2 A tal fine sono raccolti dati rilevanti per la sicurezza concernenti il modo 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 eserciti tali diritti per preparare o compiere attività che potrebbero pregiudicare considerevolmente gli interessi di cui all'articolo 1 capoverso 2.

Art. 28 Elenco delle funzioni

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

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

Art. 29 Persone da controllare

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

a. gli impiegati della Confederazione, i collaboratori esterni e i militari che esercitano una funzione prevista in un elenco secondo l'articolo 28;

b. gli impiegati cantonali che esercitano un'attività sensibile sotto il profilo della sicurezza;

c. i terzi che eseguono per un'autorità od 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 87.

2 Le persone alle quali un'autorità estera o un'organizzazione internazionale intende affidare l'esercizio di un'attività sensibile sotto il profilo della sicurezza sono sottoposte a un controllo di sicurezza se la Svizzera ha concluso con lo Stato o l'organizzazione internazionale interessati un trattato internazionale secondo l'articolo 87.

3 Le persone che esercitano una funzione che non figura ancora in un elenco secondo l'articolo 28 possono, previo consenso dell'autorità assoggettata, essere sottoposte in via eccezionale a un controllo di sicurezza. L'elenco in questione deve essere adeguato alla prima occasione.

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. magistrato cantonale eletto dal Popolo o dal parlamento cantonale.

Art. 30 Livelli di controllo

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

a. il controllo di sicurezza di base, alle 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. il controllo di sicurezza ampliato, alle 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. 31 Servizi competenti

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

a. avviare i controlli di sicurezza relativi alle persone (servizi promotori);

b. decidere di affidare l'esercizio dell'attività sensibile sotto il profilo della sicurezza (servizi decisori).

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

Art. 32 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. 33 Momento del controllo di sicurezza relativo alle persone

1 Per le persone di cui all'articolo 29 capoverso 1 lettere a e b, il controllo di sicurezza dev'essere avviato prima dell'attribuzione della funzione.

2 Per le persone di cui all'articolo 29 capoverso 1 lettera a la cui nomina compete al Consiglio federale, il controllo di sicurezza dev'essere concluso prima che la persona sia proposta per la nomina.

3 Per le persone di cui all'articolo 29 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 29 capoverso 1 lettera d, il controllo di sicurezza ha luogo nel momento previsto dal corrispondente trattato.

Art. 34 Raccolta dei dati

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

a. dal casellario giudiziale;

b. presso le autorità penali, tramite richiesta di informazioni e atti concernenti 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 precedenti controlli di sicurezza relativi alle persone;

g. da fonti pubblicamente accessibili.

2 Per il controllo di sicurezza ampliato, può inoltre raccogliere 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 audizione della persona da controllare.

3 Se dai dati raccolti 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 consenso di quest'ultima può procedere anche all'audizione di terzi; rende attenti detti terzi che essi sono liberi di fornire le informazioni o meno.

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. 35 Assistenza amministrativa

1 I dati che devono essere raccolti presso un'autorità estera o un'organizzazione internazionale lo sono per il tramite dell'autorità o dell'organizzazione competente secondo l'articolo 34.

2 Se dai dati raccolti risultano indizi concreti di 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 i dati personali rilevanti sotto il profilo della sicurezza.

Art. 36 Assunzione dei costi

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

2 I terzi per i quali la collaborazione implica un onere considerevole sono indennizzati.

3 La Confederazione si assume le spese dei controlli di sicurezza relativi alle persone effettuati sugli impiegati cantonali di cui all'articolo 29 capoverso 1 lettera b.

Art. 37 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 considerata non controllata.

Sezione 3: Valutazione del rischio per la sicurezza

Art. 38 Rischio per la sicurezza

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

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 che la persona presenta una delle caratteristiche seguenti:

a. mancanza di integrità personale o di affidabilità;

b. ricattabilità o corruttibilità; o

c. facoltà di giudizio o di decisione compromessa.

3 La valutazione del rischio per la sicurezza deve fondarsi, a prescindere dalla colpa della persona sottoposta al controllo, sulle circostanze oggettive inerenti alla sua situazione personale.

Art. 39 Risultato della valutazione

1 Quale risultato della valutazione, il servizio specializzato CSP rilascia una delle dichiarazioni seguenti, avente il significato indicato qui appresso:

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 accettabile 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 sufficienti relativi a un periodo di tempo adeguato.

2 Prima di rilasciare 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. 40 Comunicazione

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

2 Per le persone la cui nomina compete al Consiglio federale il servizio specializzato CSP comunica la sua dichiarazione al dipartimento proponente.

3 Il servizio specializzato CSP può comunicare la sua dichiarazione a un altro servizio decisore 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].

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

8 RS **510.10**

Sezione 4: Conseguenze della dichiarazione

Art. 41 Esercizio dell'attività sensibile sotto il profilo della sicurezza

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

2 Il servizio di cui all'articolo 31 capoverso 1 lettera b stabilisce, dopo aver preso atto 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. 42 Uso plurimo 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. 43 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 talune funzioni dell'esercito e della protezione civile.

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

Art. 44 Tutela giurisdizionale

1 Dopo aver ricevuto la dichiarazione secondo l'articolo 39 capoverso 1, la persona controllata ha 30 giorni di tempo per:

a. consultare i documenti relativi al controllo;

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

c. far apporre una menzione che rileva il carattere contestato dei dati.

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 39 capoverso 1 lettere b–d presso il Tribunale amministrativo federale entro 30 giorni dalla sua ricezione.

4 Se il servizio decisore è il Tribunale federale o il Tribunale amministrativo federale, 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. 45 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 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 34 e 35;
c. la valutazione del rischio per la sicurezza;
d. la dichiarazione secondo l'articolo 39 capoverso 1;
e. la decisione del servizio decisore;
f. dati e atti di procedure di ricorso;
g. elenchi e statistiche che contengono dati secondo le lettere a–f.

5 Il trattamento dei dati di cui al capoverso 4 al di fuori del sistema d'informazione dev'essere menzionato nel sistema d'informazione.

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

6 I dati di cui al capoverso 4 possono essere raccolti 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. 46 Diritti d'accesso e comunicazione dei dati

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

a. i servizi promotori, ai dati di cui all'articolo 45 capoverso 4 lettera b che hanno registrato essi stessi in occasione dell'avvio del controllo nonché ai dati di cui all'articolo 45 capoverso 4 lettere a, d ed e;

b. i servizi decisori, ai dati di cui all'articolo 45 capoverso 4 lettere a, d ed e;

c. gli incaricati della sicurezza delle informazioni secondo l'articolo 81, per l'adempimento dei loro compiti di controllo, ai dati di cui all'articolo 45 capoverso 4 lettere a, d ed e;

d. i servizi della Confederazione e dei Cantoni presso i quali vengono raccolti dati secondo l'articolo 37, ai dati di cui all'articolo 45 capoverso 4 lettera a.

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

a. il servizio specializzato di cui all'articolo 51 capoverso 2, per l'esecuzione della procedura di sicurezza relativa alle aziende secondo gli articoli 49–73, tramite il sistema d'informazione di cui all'articolo 70, ai dati di cui all'articolo 45 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 all'articolo 12 LSIM, ai dati di cui all'articolo 45 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 45 capoverso 4 lettere a ed e,

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

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 45 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 45 capoverso 4 lettere a ed e;

c. il servizio competente per le attestazioni di sicurezza internazionali di cui all'articolo 48 lettera c, ai dati di cui all'articolo 45 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 45 capoverso 4 lettere a ed e, sempre che sia necessario per il controllo dell'accesso a una zona di sicurezza.

4 Possono comunicare alle autorità e organizzazioni assoggettate elenchi e statistiche di cui all'articolo 45 capoverso 1 lettera g, sempre che sia necessario per l'adempimento dei rispettivi compiti di controllo secondo la presente legge.

Art. 47 Conservazione, archiviazione e distruzione dei dati

1 I servizi specializzati CSP possono registrare le audizioni secondo l'articolo 34 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. 48

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 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 45 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. 49 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, imprese subappaltatrici o loro parti (aziende), sempre che i mandati comportino l'esercizio di un'attività sensibile sotto il profilo della sicurezza (mandati sensibili).

Art. 50 Aziende interessate

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

a. le aziende alle quali un'autorità od organizzazione assoggettata intende assegnare un mandato sensibile;

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 66.

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. 51 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 PSA) comunica l'abbandono della procedura all'azienda e all'autorità od organizzazione aggiudicante (mandante).

Sezione 2: Avvio della procedura

Art. 52 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 PSA.

2 Le autorità assoggettate designano i servizi competenti per la presentazione della domanda.

3 Per le aziende di cui all'articolo 50 capoverso 1 lettera b, la domanda è presentata dall'autorità estera o dall'organizzazione internazionale competente.

Art. 53 Esame della domanda

1 Il servizio specializzato PSA 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 accettabile. Raccomanda misure in tal senso.

Art. 54 Definizione dei requisiti di sicurezza

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

Sezione 3: Valutazione delle aziende

Art. 55 Idoneità

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

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

3 Nell'effettuare la sua valutazione non è vincolato a istruzioni.

Art. 56 Raccolta dei dati

1 Per la valutazione dell'idoneità, il servizio specializzato PSA può raccogliere dati:

a. presso l'azienda;

b. presso il SIC;

c. da fonti pubblicamente accessibili.

2 Può chiedere a servizi esteri e internazionali di trasmettergli i corrispondenti dati. Le richieste a servizi d'informazioni esteri avvengono per il tramite del SIC.

Art. 57 Rischio per la sicurezza

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

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 impiegati dell'azienda indispensabili all'esecuzione del mandato sensibile è stata rilasciata una dichiarazione di rischio.

3 La valutazione del rischio per la sicurezza deve fondarsi, a prescindere dalla colpa, sulle circostanze oggettive inerenti all'azienda interessata.

Art. 58 Notifica della valutazione ed esclusione dalla procedura di aggiudicazione

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

2 Se il servizio specializzato PSA 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 esse. Il servizio specializzato PSA abbandona la procedura di sicurezza relativa alle aziende. Il mandante applica per analogia le misure secondo gli articoli 59, 60, 63 e 64.

Sezione 4: Piano in materia di sicurezza

Art. 59 Aggiudicazione e piano in materia di sicurezza

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

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

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

Art. 60 Controlli di sicurezza relativi alle persone

1 Gli impiegati dell'azienda ai quali si intende affidare l'esercizio di un'attività sensibile sotto il profilo della sicurezza sono sottoposti a un controllo di sicurezza relativo alle persone.

2 Il servizio specializzato PSA è competente per la decisione secondo l'articolo 41 capoverso 2. Se la procedura è abbandonata perché non vi è nessuna azienda idonea per l'esecuzione del mandato (art. 58 cpv. 3), la decisione è di competenza del mandante.

Sezione 5: Dichiarazione di sicurezza aziendale

Art. 61 Rilascio della dichiarazione di sicurezza aziendale

1 Il servizio specializzato PSA 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 Rifiuta di rilasciare la dichiarazione di sicurezza aziendale e abbandona la procedura di sicurezza relativa alle aziende se l'azienda non attua il piano in materia di sicurezza. Pronuncia 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 PSA; è fatto salvo l'articolo 58 capoverso 3.

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

Art. 62 Esecuzione di un mandato sensibile

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

Art. 63 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 PSA e al mandante tutti i cambiamenti e gli incidenti rilevanti sotto il profilo della sicurezza.

Art. 64 Controlli e misure di protezione

1 Il servizio specializzato PSA 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 PSA può adottare immediatamente le misure di protezione necessarie e in particolare mettere al sicuro documenti e materiale.

Art. 65 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 PSA verifica se il piano in materia di sicurezza dev'essere adeguato.

Art. 66 Attestazione internazionale di sicurezza aziendale

Il servizio specializzato PSA rilascia all'azienda interessata, su richiesta, un'attestazione internazionale di sicurezza aziendale.

Art. 67 Revoca della dichiarazione di sicurezza aziendale

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

a. l'azienda non adempie i propri obblighi secondo l'articolo 63;

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

2 Comunica la revoca all'azienda e al mandante mediante decisione.

3 Se la dichiarazione di sicurezza aziendale è revocata, il mandante ritira immediatamente il mandato; è fatto salvo l'articolo 58 capoverso 3. L'azienda non ha diritto ad alcun indennizzo.

Sezione 6: Ripetizione della procedura e tutela giurisdizionale

Art. 68 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. 69 Tutela giurisdizionale

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

a. consultare i documenti;

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

c. far apporre una menzione che rileva il carattere contestato dei dati;

d. interporre ricorso presso il Tribunale amministrativo federale.

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

17 RS **235.1**

Sezione 7: Trattamento dei dati personali

Art. 70 Sistema d'informazione per la procedura di sicurezza relativa alle aziende

1 Il servizio specializzato PSA 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 seguenti:

a. i dati secondo gli articoli 56 e 59 capoverso 3;
b. il risultato della valutazione secondo l'articolo 55 capoverso 2;
c. i risultati dei controlli di sicurezza relativi alle persone secondo l'articolo 60 capoverso 1 necessari per la procedura di sicurezza relativa alle aziende;
d. la decisione del servizio specializzato PSA secondo l'articolo 60 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 64;
g. dati e atti di procedure di ricorso.

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

Art. 71 Diritti d'accesso e comunicazione dei dati

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

a. i mandanti, ai dati di cui all'articolo 70 capoverso 3 lettere b e d–g;
b. le aziende interessate, sempre che siano state autorizzate dal Consiglio federale, in virtù dell'articolo 31 capoverso 1 lettera a, ad avviare controlli di sicurezza relativi alle persone nel rispettivo ambito di competenza, ai dati di cui all'articolo 70 capoverso 3 lettera d.

2 Il servizio specializzato PSA può inoltre comunicare ad altri servizi della Confederazione i dati di cui all'articolo 70 capoverso 3 lettere b–d, sempre che sia necessario per garantire la sicurezza delle informazioni.

Art. 72 Conservazione, archiviazione e distruzione dei dati

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

18 RS **235.1**

2 L'archiviazione dei dati è retta dalle disposizioni 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 del Consiglio federale

Art. 73

Il Consiglio federale disciplina:

a. i dettagli della procedura di sicurezza relativa alle aziende;
b. l'applicazione alle imprese subappaltatrici della procedura di sicurezza relativa alle aziende;
c. l'organizzazione del servizio specializzato PSA;
d. la sicurezza dei dati nel sistema d'informazione secondo l'articolo 70;
e. il controllo periodico del trattamento dei dati personali da parte di un organo esterno.

Capitolo 5: Infrastrutture critiche

Art. 74 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 che il danno sia limitato.

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 seguito del trattamento degli 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 tra di loro e con i servizi competenti della Confederazione.

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

Art. 75 Trattamento di dati personali

1 Per l'adempimento dei propri compiti, i servizi di cui all'articolo 74 capoverso 5 possono trattare elementi di indirizzo di cui all'articolo 3 lettera f LTC[19] e i relativi dati personali.

2 Possono trattare i dati di cui al capoverso 1 anche se questi contengono informazioni concernenti:

a. 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. 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. 76 Cooperazione a livello nazionale

1 I servizi di cui all'articolo 74 capoverso 5 possono comunicare ai gestori di infrastrutture critiche dati personali di cui all'articolo 75, 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 75, sempre che sia necessario per garantire la sicurezza delle informazioni di 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 74 capoverso 5 dati, inclusi dati personali, inerenti a un incidente determinato. I servizi di cui all'articolo 74 capoverso 5 possono trasmettere tali dati ai fini del perseguimento penale unicamente previo consenso esplicito del fornitore dei dati.

Art. 77 Cooperazione a livello internazionale

1 I servizi di cui all'articolo 74 capoverso 5 possono scambiare dati di cui all'articolo 75 con servizi esteri e internazionali competenti per la protezione di infrastrutture critiche se tali dati sono necessari per l'adempimento di compiti corrispondenti a quelli secondo l'articolo 74.

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

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

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

Art. 78 Sistema d'informazione per il sostegno alle infrastrutture critiche

1 I servizi di cui all'articolo 74 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. istruzioni per individuare e risolvere 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 contenere anche dati personali secondo l'articolo 75.

Art. 79 Conservazione e archiviazione dei dati

1 I servizi di cui all'articolo 74 capoverso 5 conservano i dati personali soltanto fino a che sono utili per prevenire minacce o individuare incidenti, ma al massimo per cinque anni.

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

Art. 80 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 74 capoverso 5 e il SIC;

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

c. la responsabilità in materia di protezione dei dati in relazione con il sistema d'informazione di cui all'articolo 78 e la sicurezza dei dati;

d. il controllo periodico del trattamento dei dati personali nel sistema d'informazione di cui all'articolo 78 da parte di un organo esterno.

Capitolo 6: Organizzazione ed esecuzione

Sezione 1: Organizzazione

Art. 81 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 hanno i compiti seguenti:

a. offrono consulenza e assistenza ai servizi competenti, nel rispettivo ambito, per l'adempimento dei compiti e degli obblighi secondo la presente legge;

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

c. verificano, su incarico della rispettiva autorità od 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 74 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. 82 Conferenza degli incaricati della sicurezza delle informazioni

1 La Conferenza degli incaricati della sicurezza delle informazioni è composta degli incaricati della sicurezza delle informazioni secondo l'articolo 81 capoverso 1, di due rappresentanti dei Cantoni e dell'Incaricato federale della protezione dei dati e della trasparenza.

2 Ha i compiti seguenti:

a. promuove l'esecuzione uniforme della presente legge;

b. partecipa alla standardizzazione dei requisiti e delle misure secondo l'articolo 85;

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 Adotta un proprio regolamento interno.

Art. 83 Servizio specializzato della Confederazione per la sicurezza delle informazioni

1 Il Servizio specializzato della Confederazione per la sicurezza delle informazioni ha i compiti seguenti:

a. offre consulenza e assistenza alle autorità assoggettate, ai loro incaricati della sicurezza delle informazioni e ai 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, mezzi, installazioni, oggetti e 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 è nel contempo capo 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. Può assegnargli ulteriori compiti a favore dell'Amministrazione federale e dell'esercito.

Sezione 2: Esecuzione

Art. 84 Disposizioni esecutive

1 Le autorità assoggettate emanano le disposizioni esecutive. 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 attribuisce 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. 85 Requisiti e misure standardizzati

1 Il Consiglio federale stabilisce, secondo lo stato della scienza e della tecnica, requisiti standardizzati nonché misure organizzative, tecniche, edili e riguardanti il personale 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. 86 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 Ogni Cantone designa 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. 87 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, vulnerabilità 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. 88 Valutazione

1 Il Consiglio federale provvede affinché l'applicazione, l'adeguatezza, l'efficacia e l'economicità della presente legge siano periodicamente verificate da un servizio indipendente quale il Controllo federale delle finanze.

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

Capitolo 7: Disposizioni finali

Art. 89 Modifica di altri atti normativi

La modifica di altri atti normativi è disciplinata nell'allegato 1.

Art. 90 Disposizioni transitorie

1 Le informazioni classificate secondo il diritto anteriore sono adeguate alle disposizioni del nuovo diritto in occasione del loro primo trattamento successivo all'entrata in vigore della presente legge.

2 I mezzi informatici sono classificati secondo le disposizioni della presente legge entro due anni dalla sua entrata in vigore. Le misure tecniche per garantire la sicurezza delle informazioni sono 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 valide per cinque anni dal loro rilascio.

Art. 91 Coordinamento con altri atti normativi

Il coordinamento con altri atti normativi è disciplinato nell'allegato 2.

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.

Consiglio degli Stati, 18 dicembre 2020	Consiglio nazionale, 18 dicembre 2020
Il presidente: Alex Kuprecht La segretaria: Martina Buol	Il presidente: Andreas Aebi Il segretario: Pierre-Hervé Freléchoz

Data della pubblicazione: 31 dicembre 2020[21]

Termine di referendum: 10 aprile 2021

21 FF **2020** 8755

Allegato 1
(art. 89)

Modifica di altri atti normativi

Le leggi federali qui appresso sono modificate come segue:

1. Legge federale del 21 marzo 1997[22] sulle misure per la salvaguardia della sicurezza interna

Art. 2 cpv. 2 lett. a

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 31 capoverso 2 della legge del 18 dicembre 2020[23] sulla sicurezza delle informazioni, mediante una procedura di richiamo. ...

2. Legge federale del 25 settembre 2015[24] sulle attività informative

Art. 6 cpv. 1 lett. a n. 4

1 Il SIC acquisisce e tratta informazioni al fine di:

a. individuare tempestivamente e sventare minacce per la sicurezza interna o esterna rappresentate:
   4. da attacchi a infrastrutture per l'approvvigionamento di acqua potabile e di energia, a infrastrutture nei settori dell'informazione, della comunicazione e dei trasporti nonché ad altri processi, sistemi e installazioni essenziali per il funzionamento dell'economia e il benessere della popolazione (infrastrutture critiche),

22 RS **120**
23 RS **126**
24 RS **121**

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 31 capoverso 2 della legge del 18 dicembre 2020[25] 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.

3. Legge del 26 giugno 1998[26] sull'asilo

Art. 29a Verifica dell'affidabilità

1 La SEM può far verificare l'affidabilità degli interpreti e dei traduttori prima e durante il loro mandato.

2 I servizi specializzati CSP di cui all'articolo 31 capoverso 2 della legge del 18 dicembre 2020[27] sulla sicurezza delle informazioni (LSIn) eseguono le verifiche dell'affidabilità. Le disposizioni della LSIn relative al controllo di sicurezza di base si applicano per analogia.

3 Se gli interpreti e i traduttori sono sottoposti contemporaneamente a un controllo di sicurezza relativo alle persone secondo la LSIn, le due procedure sono riunite.

4 I costi delle verifiche dell'affidabilità sono a carico della SEM.

Art. 29b

Ex art. 29a

4. Legge del 24 marzo 2000[28] sul personale federale

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

Se necessario per tutelare i suoi interessi, il datore di lavoro può esigere dai candidati a un impiego e dagli impiegati che presentino un estratto del casellario giudiziale e del registro delle esecuzioni.

25 RS **126**
26 RS **142.31**
27 RS **126**
28 RS **172.220.1**

Art. 20b Verifica dell'affidabilità

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

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

b. prendono decisioni ed esercitano compiti di vigilanza in affari finanziari o fiscali essenziali e in tale contesto potrebbero pregiudicare considerevolmente gli interessi finanziari della Confederazione;

c. esercitano compiti di perseguimento penale o di polizia e in tale contesto potrebbero pregiudicare considerevolmente gli interessi pubblici della Confederazione, in particolare la sicurezza dell'Amministrazione federale.

2 Limitano la verifica allo stretto necessario.

3 I servizi specializzati di cui all'articolo 31 capoverso 2 della legge del 18 dicembre 2020[29] 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.

5. Codice di procedura civile[30]

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;

29 RS **126**
30 RS **272**

6. Legge di procedura civile federale del 4 dicembre 1947[31]

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.

7. Codice penale[32]

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 18 dicembre 2020[33] 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 31 capoverso 2 LSIn[34] (servizi specializzati CSP);

31 RS **273**
32 RS **311.0**
33 RS **126**
34 RS **126**

[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, l e m.

8. Codice di procedura penale[35]

Art. 170 cpv. 1

[1] I funzionari ai sensi dell'articolo 110 capoverso 3 CP[36] 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.

9. Codice penale militare del 13 giugno 1927[37]

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.

10. Procedura penale militare del 23 marzo 1979[38]

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[39]) o essere obbligato a produrre documenti ufficiali. Del rimanente sono applicabili le disposizioni del diritto amministrativo federale e cantonale.

35 RS **312.0**
36 RS **311.0**
37 RS **321.0**
38 RS **322.1**
39 RS **311.0**

11. Legge federale del 13 giugno 2008[40] 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 31 capoverso 2 della legge del 18 dicembre 2020[41] 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.

12. Legge militare del 3 febbraio 1995[42]

Art. 1 cpv. 2 lett. c

2 Quando i loro mezzi non sono più sufficienti, appoggia le autorità civili in Svizzera:

c. nella protezione di persone e di oggetti degni di particolare protezione, in particolare di infrastrutture per l'approvvigionamento di acqua potabile e di energia, di infrastrutture nei settori dell'informazione, della comunicazione e dei trasporti nonché di altri processi, sistemi e installazioni essenziali per il funzionamento dell'economia e il benessere della popolazione (infrastrutture critiche);

Art. 14 Verifica dell'affidabilità

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

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

b. prendono decisioni ed esercitano compiti di vigilanza in affari finanziari essenziali e in tale contesto potrebbero pregiudicare considerevolmente gli interessi finanziari della Confederazione.

2 Il Consiglio federale designa le funzioni soggette alla verifica. Al riguardo si limita allo stretto necessario.

40 RS **361**
41 RS **126**
42 RS **510.10**

3 Il servizio specializzato di cui all'articolo 31 capoverso 2 della legge federale del 18 dicembre 2020[43] 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.

Art. 113 cpv. 6

6 La procedura è retta per analogia dalle disposizioni relative al controllo di sicurezza di base secondo l'articolo 30 lettera a LSIn[44]. 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

13. Legge federale del 3 ottobre 2008[45] sui sistemi d'informazione militari

Art. 14 cpv. 1 lett. g^bis^ e m

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:

g^bis^. dati concernenti l'esecuzione della verifica dell'affidabilità secondo l'articolo 14 della legge militare del 3 febbraio 1995[46] (LM), unitamente alla corrispondente decisione;

m. dati concernenti i procedimenti penali a carico di militari e persone soggette all'obbligo di leva e comunicazioni ai sensi dell'articolo 113 capoversi 7 e 8 LM sempre che sussistano seri segni o indizi che la persona interessata possa esporre a pericolo sé stessa o terzi con l'arma personale.

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

Abrogate

43 RS **126**
44 RS **126**
45 RS **510.91**
46 RS **510.10**

14. Legge federale del 21 marzo 2003[47] 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.

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

15. Legge del 23 marzo 2007[48] sull'approvvigionamento elettrico

Art. 20a Verifica dell'affidabilità

1 Ai fini della valutazione del rischio per la sicurezza, le persone alle quali la società nazionale di rete affida funzioni critiche o estremamente critiche sono sottoposte a una verifica periodica dell'affidabilità.

2 Il Consiglio federale designa i gruppi di persone soggetti alla verifica. Al riguardo si limita allo stretto necessario.

3 Il servizio specializzato secondo l'articolo 31 capoverso 2 della legge del 18 dicembre 2020[49] sulla sicurezza delle informazioni (LSIn) esegue la verifica dell'affidabilità. La procedura è retta per analogia dalle pertinenti disposizioni della LSIn.

4 La società nazionale di rete dispone lo svolgimento della verifica. Il risultato, corredato di una breve motivazione, le è comunicato.

16. Legge del 17 giugno 2016[50] sul casellario giudiziale

Art. 46 lett. e

Le seguenti autorità collegate possono consultare mediante procedura di richiamo tutti i dati figuranti nell'estratto 2 per autorità (art. 38), nella misura necessaria per adempiere i compiti elencati qui appresso:

e. i servizi specializzati competenti per l'esecuzione dei controlli di sicurezza relativi alle persone secondo l'articolo 31 capoverso 2 della legge del 18 dicembre 2020[51] sulla sicurezza delle informazioni (LSIn):
   1. per valutare il rischio nell'ambito dei controlli di sicurezza relativi alle persone secondo la LSIn,

47 RS **732.1**
48 RS **734.7**
49 RS **126**
50 RS **330**; FF **2016** 4315
51 RS **126**

2. per valutare il potenziale di pericolo o di abuso secondo la legge militare del 3 febbraio 1995[52],
3. per valutare il rischio nell'ambito di altri controlli previsti nella legislazione speciale;

Art. 51 lett. f

Abrogata

Art. 59 Comunicazioni all'Aggruppamento Difesa

1 Il Servizio del casellario giudiziale comunica senza indugio all'Aggruppamento Difesa, per gli scopi di cui al capoverso 2, i seguenti nuovi dati iscritti in VOSTRA che concernono persone soggette all'obbligo di leva e militari:

a. le sentenze originarie svizzere per un crimine o un delitto;
b. le sentenze originarie straniere;
c. le misure privative della libertà;
d. le decisioni concernenti l'insuccesso del periodo di prova.

2 L'Aggruppamento Difesa può utilizzare i dati comunicati per esaminare:

a. una decisione di non reclutamento, un'ammissione al reclutamento, un'esclusione dall'esercito, una riammissione nell'esercito, una degradazione o l'idoneità a una promozione o a una nomina secondo la LM[53];
b. i motivi d'impedimento per la cessione dell'arma personale secondo la LM.

3 La comunicazione è effettuata mediante un'interfaccia elettronica tra il Sistema di gestione del personale dell'esercito (PISA) e VOSTRA. I dati di cui al capoverso 1 sono selezionati e trasmessi in modo automatizzato in base al numero d'assicurato dell'interessato.

52 RS **510.10**
53 RS **510.10**

Allegato 2
(art. 91)

Coordinamento con altri atti normativi

1. Legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (LMSI)

Indipendentemente dal fatto che entri prima in vigore la presente modifica della LMSI[54] *(Allegato 1, n. 1) o la modifica della LMSI nel quadro della legge federale del 25 settembre 2020*[55] *sulle misure di polizia per la lotta al terrorismo (cifra I 1), all'atto della seconda di queste entrate in vigore o in caso di entrata in vigore simultanea delle due modifiche, l'articolo 24a capoverso 7, primo periodo LMSI avrà il tenore seguente:*

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, dell'AFD e dei servizi specializzati competenti per l'esecuzione dei controlli di sicurezza relativi alle persone secondo l'articolo 31 capoverso 2 della legge del 18 dicembre 2020[56] sulla sicurezza delle informazioni, mediante una procedura di richiamo. ...

2. Legge del 24 marzo 2000 sul personale federale (LPers)

Indipendentemente dal fatto che entri prima in vigore la presente modifica della LPers[57] *(Allegato 1, n. 4) o la modifica della LPers nel quadro della legge del 17 giugno 2016*[58] *sul casellario giudiziale (Allegato 1, n. 1), all'atto della seconda di queste entrate in vigore o in caso di entrata in vigore simultanea delle due modifiche, l'articolo 20a LPers avrà il tenore seguente:*

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

Se necessario per tutelare i suoi interessi, il datore di lavoro può esigere dai candidati a un impiego e dagli impiegati che presentino un estratto del casellario giudiziale e del registro delle esecuzioni.

54 RS **120**
55 FF **2020** 6795
56 RS **126**
57 RS **172.220.1**
58 RS **330**; FF **2016** 4315

3. Codice penale (CP)

All'entrata in vigore della legge del 17 giugno 2016[59] *sul casellario giudiziale le disposizioni qui appresso del CP*[60] *(Allegato 1, n. 7) avranno il tenore seguente:*

Art. 365 cpv. 2 lett. d

Privi di oggetto o abrogati

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

Privi di oggetto o abrogati

4. Legge del 17 giugno 2016 sul casellario giudiziale (LCaGi)

All'entrata in vigore della LCaGi[61] *l'art. 45 capoverso 6 lettera a della legge del 18 dicembre 2020*[62] *sulla sicurezza delle informazioni avrà il tenore seguente:*

Art. 45 cpv. 6 lett. a

6 I dati di cui al capoverso 4 possono essere raccolti automaticamente e sistematicamente mediante interrogazione dei seguenti sistemi d'informazione:

a. casellario giudiziale informatizzato VOSTRA conformemente alla legge del 17 giugno 2016[63] sul casellario giudiziale;

5. Legge federale del 25 settembre 2020 sulla protezione dei dati (LPD)

All'entrata in vigore della LPD[64] *le disposizioni qui appresso della legge del 18 dicembre 2020*[65] *sulla sicurezza delle informazioni avranno il tenore seguente:*

Art. 44 cpv. 2

2 La restrizione del diritto d'accesso è retta dall'articolo 26 della legge federale del 25 settembre 2020[66] sulla protezione dei dati (LPD).

59 RS **330**; FF **2016** 4315
60 RS **311.11**
61 RS **330**; FF **2016** 4315
62 RS **126**
63 RS **330**
64 RS **235.1**; FF **2020** 6695
65 RS **126**
66 RS **235.1**

Art. 45 cpv. 3

3 Nel sistema d'informazione possono essere trattati dati personali degni di particolare protezione secondo l'articolo 5 lettera c LPD[67], sempre che sia necessario per la valutazione del rischio per la sicurezza.

Art. 69 cpv. 2

2 La restrizione del diritto d'accesso è retta dall'articolo 26 LPD[68].

Art. 70 cpv. 2

2 Nel sistema d'informazione possono essere trattati dati personali degni di particolare protezione secondo l'articolo 5 lettera c LPD[69], sempre che sia necessario per l'esecuzione della procedura di sicurezza relativa alle aziende.

Art. 75 cpv. 4, secondo periodo

4 ... È fatto salvo l'articolo 20 LPD[70].

6. Legge federale del 13 giugno 2008[71] sui sistemi d'informazione di polizia della Confederazione (LSIP)

Indipendentemente dal fatto che entri prima in vigore la presente modifica della LSIP (Allegato 1, n. 11) o la modifica della LSIP nel quadro del decreto federale del 18 dicembre 2020[72] che approva e traspone nel diritto svizzero gli scambi di note tra la Svizzera e l'UE concernenti il recepimento delle basi legali dell'istituzione, dell'esercizio e dell'uso del sistema d'informazione Schengen (Allegato 1, n. 5), all'atto della seconda di queste entrate in vigore o in caso di entrata in vigore simultanea delle due modifiche, l'articolo 15 cpv. 4 lett. f LSIP avrà il seguente tenore:

Art. 15 cpv. 4 lett. f

Abrogata

67 RS **235.1**
68 RS **235.1**
69 RS **235.1**
70 RS **235.1**
71 RS **361**
72 FF **2020** 8813