Legge federale sulla sicurezza delle informazioni (LSIn) [1]

del 18 dicembre 2020 (Stato 1° aprile 2025)

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[2];
visto il messaggio del Consiglio federale del 22 febbraio 2017[3],
decreta:

Capitolo 1: Disposizioni generali

Art. 1 Scopo

[1] La presente legge ha lo scopo di:

a. garantire il trattamento sicuro delle informazioni di competenza della Confederazione nonché l'impiego sicuro dei mezzi informatici della Confederazione;

b. aumentare la capacità della Svizzera di fronteggiare le ciberminacce.[4]

[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.

Art. 2 Autorità e organizzazioni assoggettate

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

RU **2022** 232

1 Nuovo testo giusta la cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).
2 RS **101**
3 FF **2017** 2563
4 Nuovo testo giusta la cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

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[5] 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 73*a*–79.[6] 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.

5 RS **172.010**

6 Nuovo testo del per. giusta la cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

Art. 4 Rapporto con altre leggi federali

[1] La legge del 17 dicembre 2004[7] sulla trasparenza (LTras) prevale sulla presente legge.[8]

[1bis] Le informazioni provenienti da terzi di cui l'Ufficio federale della cibersicurezza (UFCS) viene a conoscenza nella sua attività di ricezione e analisi di segnalazioni secondo il capitolo 5 non possono essere rese accessibili secondo la LTras. Non sono considerati terzi le autorità, le organizzazioni e le persone menzionate all'articolo 2 capoverso 1 LTras. [9]

[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;

d.[10] *ciberincidente:* un evento che si verifica nell'utilizzo di mezzi informatici e che compromette la confidenzialità, la disponibilità o l'integrità delle informazioni o la tracciabilità del loro trattamento;

7 RS **152.3**

8 Nuovo testo giusta la cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

9 Introdotto dalla cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 168; 173; FF **2023** 84).

10 Introdotta dalla cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

e.[11] *ciberattacco:* un ciberincidente provocato intenzionalmente;

f.[12] *ciberminaccia:* qualsiasi circostanza o evento che ha il potenziale di provocare un ciberincidente;

g.[13] *vulnerabilità:* una ciberminaccia riconducibile a punti deboli o errori nei mezzi informatici.

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).

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;

11 Introdotta dalla cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

12 Introdotta dalla cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

13 Introdotta dalla cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (FF **2023** 84; RU **2024** 257; **2025** 173).

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.

Art. 10*a*[14] Trattamento di dati personali

1 Le autorità e organizzazioni assoggettate possono trattare i dati personali utili a garantire la sicurezza delle informazioni, in particolare nei sistemi d'informazione previsti a tale scopo (applicazioni ISMS).

2 Possono scambiarsi i dati personali di cui al capoverso 1 reciprocamente nonché con organizzazioni di diritto pubblico svizzere, internazionali ed estere, sempre che:

a. ciò sia utile al fine di garantire la sicurezza delle informazioni;

b. non sia violato alcun obbligo legale o contrattuale di serbare il segreto;

c. siano rispettate le disposizioni della legislazione federale sulla protezione dei dati; e

d. queste organizzazioni assumano compiti legali nell'ambito della sicurezza delle informazioni corrispondenti a quelli dell'autorità o dell'organizzazione che ha trasmesso la comunicazione.

14 Introdotto dalla cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

3 Le autorità e organizzazioni assoggettate possono collegare tra loro i propri sistemi d'informazione, in particolare le applicazioni ISMS, e scambiarsi dati automaticamente o su richiesta tramite interfacce.

4 Possono gestire moduli digitali finalizzati alla presentazione e al trattamento di richieste e segnalazioni nell'ambito della sicurezza delle informazioni e collegarli alle proprie applicazioni ISMS o ad altri sistemi d'informazione.

5 Se necessario per far fronte a violazioni della sicurezza delle informazioni o per eliminare vulnerabilità, le autorità e organizzazioni assoggettate possono eseguire con i dati personali degni di particolare protezione ai sensi dell'articolo 5 lettera c della legge federale del 25 settembre 2020[15] sulla protezione dei dati (LPD) di persone che sono o potrebbero essere coinvolte in tali violazioni o vulnerabilità o che sono o potrebbero esserne interessate le operazioni seguenti:

a. trattarli;

b. scambiarseli reciprocamente o scambiarli con organizzazioni di diritto pubblico svizzere, internazionali ed estere, sempre che la condizione di cui al capoverso 2 lettera b sia soddisfatta.

6 Le autorità e organizzazioni assoggettate possono conservare i dati personali degni di particolare protezione fino a due anni dopo aver affrontato la violazione della sicurezza delle informazioni o dopo che è stata eliminata la vulnerabilità, ma al massimo per dieci anni.

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

8 Il trattamento dei dati personali da parte del UFCS[16] nel quadro dell'adempimento dei suoi compiti è retto dagli articoli 75–79.

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).

15 RS **235.1**

16 Nuova espressione giusta la cifra I dell'O del 7 mar. 2025, in vigore dal 1° apr. 2025 (RU **2024** 168). Di detta mod. è tenuto conto in tutto il presente testo.

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[17].

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 AVS di cui all'articolo 50*c* della legge federale del 20 dicembre 1946[18] sull'assicurazione per la vecchiaia e per i superstiti.[19]

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.

17 RS **172.010**
18 RS **831.10**
19 Nuovo testo giusta l'all. n. 40 della LF del 18 dic. 2020 (Utilizzazione sistematica del numero AVS da parte delle autorità), in vigore dal 1° gen. 2024 (RU **2021** 758; **2023** 650; FF **2019** 6043).

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[20] 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 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).

20 RS **784.10**

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;

e^bis.[21] capo dell'Incaricato federale della protezione dei dati e della trasparenza;

f. generale;

g. magistrato cantonale eletto dal Popolo o dal parlamento cantonale.

21 Introdotta dalla cifra I della LF del 17 giu. 2022 (Capo dell'Incaricato federale della protezione dei dati e della trasparenza), in vigore dal 1° gen. 2024 (RU **2023** 734; FF **2022** 345, 432).

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[22].

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.

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.

22 RS **510.10**

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 26 LPD[23].[24]

3 La dichiarazione costituisce un atto materiale secondo l'articolo 25*a* della legge federale del 20 dicembre 1968[25] 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[26] sul personale federale.

23 RS **235.1**
24 Nuovo testo giusta la cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).
25 RS **172.021**
26 RS **172.220.1**

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. Quest'ultimo serve per l'esecuzione:

a. dei controlli di sicurezza relativi alle persone;

b. delle valutazioni del potenziale di pericolo o di abuso per quanto riguarda l'arma personale;

c. dei controlli dell'affidabilità;

d. dei controlli dell'attendibilità.[27]

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 secondo l'articolo 5 lettera c LPD[28], sempre che sia necessario per la valutazione del rischio per la sicurezza.[29]

3bis Con i dati del sistema d'informazione può essere eseguita una profilazione, compresa una profilazione a rischio elevato, secondo la LPD per analizzare, valutare, qualificare o prevedere i seguenti aspetti personali di una persona fisica concernenti gli scopi del trattamento secondo il capoverso 1:

a. rischio per la sicurezza;

b. potenziale di pericolo e di abuso per quanto riguarda l'arma personale.[30]

4 Il sistema d'informazione contiene i dati seguenti:

a.[31] dati sull'identità delle persone da sottoporre al controllo o controllate, compreso il numero 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;

27 Nuovo testo giusta la cifra II n. 2 della LF del 17 giu. 2022, in vigore dal 1° gen. 2024 (RU **2023** 117, 650; FF **2021** 3046).
28 RS **235.1**
29 Nuovo testo giusta l'all. 2 n. 5, in vigore dal 1° gen. 2024 (RU **2022** 232; **2023** 650; FF **2017** 2563).
30 Introdotto dalla cifra II n. 2 della LF del 17 giu. 2022, in vigore dal 1° gen. 2024 (RU **2023** 117, 650; FF **2021** 3046).
31 Nuovo testo giusta l'all. n. 40 della LF del 18 dic. 2020 (Utilizzazione sistematica del numero AVS da parte delle autorità), in vigore dal 1° gen. 2024 (RU **2021** 758; **2023** 650; FF **2019** 6043).

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.

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

a.[32] casellario giudiziale informatizzato VOSTRA conformemente alla legge del 17 giugno 2016[33] sul casellario giudiziale;

b. registro nazionale di polizia di cui all'articolo 17 della legge federale del 13 giugno 2008[34] sui sistemi d'informazione di polizia della Confederazione;

c. INDEX SIC di cui all'articolo 51 della legge federale del 25 settembre 2015[35] sulle attività informative;

d.[36] le banche dati dell'Ufficio centrale Armi secondo l'articolo 32*a* capoverso 1 della legge del 20 giugno 1997[37] sulle armi.

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,

32 Nuovo testo giusta l'all. 2 n. 4, in vigore dal 1° gen. 2024 (RU **2022** 232; **2023** 650; FF **2017** 2563).
33 RS **330**
34 RS **361**
35 RS **121**
36 Introdotta dalla cifra II n. 2 della LF del 17 giu. 2022, in vigore dal 1° gen. 2024 (RU **2023** 117, 650; FF **2021** 3046).
37 RS **514.54**

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[38] 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,
   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.

38 RS **510.91**

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 26 LPD[39].[40]

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 secondo l'articolo 5 lettera c LPD[41], sempre che sia necessario per l'esecuzione della procedura di sicurezza relativa alle aziende.[42]

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.

39 RS **235.1**
40 Nuovo testo giusta l'all. 2 n. 5, in vigore dal 1° gen. 2024 (RU **2022** 232; **2023** 650; FF **2017** 2563).
41 RS **235.1**
42 Nuovo testo giusta l'all. 2 n. 5, in vigore dal 1° gen. 2024 (RU **2022** 232; **2023** 650; FF **2017** 2563).

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.

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: Misure della Confederazione per la protezione della Svizzera dalle ciberminacce[43]

Sezione 1: Disposizioni generali[44]

Art. 73*a*[45] Principio

1 Per proteggere la Svizzera dalle ciberminacce, il UFCS effettua analisi tecniche al fine di valutare e contrastare ciberincidenti e ciberminacce, nonché di indentificare ed eliminare vulnerabilità.

2 Sulla base delle analisi, il UFCS svolge in particolare i seguenti compiti:

a. sensibilizzare e avvisare il pubblico riguardo alle ciberminacce;

b. avvisare le autorità, le organizzazioni e le persone interessate in caso di ciberminacce imminenti o di ciberattacchi in corso;

c. pubblicare informazioni sulla cibersicurezza e raccomandazioni per l'adozione di misure preventive e reattive contro i ciberincidenti;

d. ricevere e trattare le segnalazioni riguardanti ciberincidenti e ciberminacce;

e. sostenere i gestori di infrastrutture critiche.

Art. 73*b*[46] Segnalazioni

1 Il UFCS è il destinatario delle segnalazioni riguardanti ciberincidenti e ciberminacce. Le segnalazioni possono essere anonime.

2 Il UFCS analizza le segnalazioni in relazione alla loro rilevanza per la protezione della Svizzera dalle ciberminacce. Su richiesta, il UFCS emana una raccomandazione su come procedere, sempre che non siano necessari ulteriori analisi e chiarimenti.

3 Se viene a conoscenza di vulnerabilità, il UFCS informa immediatamente il produttore dell'hardware o del software interessato e gli fissa un congruo termine per eliminarle. Gli indica che un'inosservanza può essere sanzionata secondo il diritto in materia di appalti pubblici (art. 44 cpv. 1 lett. f^{bis} della legge federale del 21 giugno 2019[47] sugli appalti pubblici) e che il UFCS, allo scadere del termine, può rendere pubblica la vulnerabilità ai sensi dell'articolo 73*c* capoverso 2.

43 Nuovo testo giusta la cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

44 Introdotta dalla cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

45 Introdotto dalla cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

46 Introdotto dalla cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

47 RS **172.056.1**

Art. 73*c*[48] Pubblicazione di informazioni provenienti da segnalazioni

[1] Il UFCS può pubblicare informazioni relative a ciberincidenti, sempre che ciò serva alla protezione contro le ciberminacce. Queste informazioni possono contenere dati relativi alla persona fisica o giuridica interessata soltanto se quest'ultima vi acconsente e se i dati concernono le caratteristiche d'identificazione e gli elementi d'indirizzo che sono stati utilizzati in modo abusivo.

[2] Il UFCS può pubblicare informazioni relative a vulnerabilità indicando l'hardware o il software interessato, sempre che il produttore vi acconsenta o non abbia eliminato la vulnerabilità entro il termine di cui all'articolo 73*b* capoverso 3.

Art. 73*d*[49] Inoltro di informazioni

[1] Il UFCS può inoltrare informazioni provenienti da segnalazioni ad autorità e organizzazioni attive nel settore della cibersicurezza. Queste informazioni possono contenere dati personali soltanto se la persona interessata vi acconsente.

[2] Se dalla segnalazione di un ciberincidente o dalla sua analisi emergono informazioni necessarie a individuare tempestivamente e sventare minacce per la sicurezza interna o esterna, a valutare la situazione di minaccia o ad assicurare un servizio di preallerta informativa per la protezione di infrastrutture critiche secondo l'articolo 6 capoversi 1 lettera a, 2 e 5 della legge federale del 25 settembre 2015[50] sulle attività informative (LAIn), il UFCS inoltra queste informazioni al SIC.

[3] I collaboratori del UFCS che nell'ambito di una segnalazione o della sua analisi constatano indizi di un possibile reato lo denunciano unicamente al direttore del UFCS, in deroga all'articolo 22*a* capoverso 1 della legge del 24 marzo 2000[51] sul personale federale. Se la gravità del possibile reato lo esige, il direttore del UFCS può sporgere denuncia presso le autorità di perseguimento penale.

[4] Il UFCS può inoltrare informazioni che rivelano segreti protetti dal diritto penale unicamente secondo quanto disposto dall'articolo 320 del Codice penale[52].

Art. 74[53] Sostegno ai gestori di infrastrutture critiche

[1] Il UFCS sostiene i gestori di infrastrutture critiche nella protezione contro le ciberminacce.

[2] Mette loro a disposizione gratuitamente per l'utilizzo su base volontaria in particolare i seguenti strumenti:

48 Introdotto dalla cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).
49 Introdotto dalla cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).
50 RS **121**
51 RS **172.220.1**
52 RS **311.0**
53 Nuovo testo giusta la cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

a. un sistema di comunicazione per lo scambio sicuro delle informazioni;

b. informazioni tecniche sulle ciberminacce attuali e raccomandazioni per l'adozione di misure preventive e reattive contro i ciberincidenti;

c. strumenti tecnici e istruzioni per l'individuazione di ciberincidenti che rispondono alle elevate esigenze di protezione delle infrastrutture critiche.

3 Il UFCS può fornire loro consulenza e sostegno nel far fronte a ciberincidenti ed eliminare vulnerabilità se il funzionamento dell'infrastruttura critica interessata rischia di essere compromesso e, nel caso si tratti di gestori privati, se non è possibile procurarsi per tempo un sostegno equivalente sul mercato.

4 Previo consenso del gestore interessato, il UFCS può accedere alle informazioni e ai mezzi informatici di quest'ultimo per analizzare un ciberincidente.

Sezione 2:[54] Obbligo di segnalare ciberattacchi

Art. 74*a* Principi

1 Le autorità e le organizzazioni di cui all'articolo 74*b* provvedono affinché i ciberattacchi verso i loro mezzi informatici siano segnalati all'UFCS.

2 Il UFCS informa le autorità e organizzazioni interessate sul loro eventuale assoggettamento all'obbligo di segnalazione; su richiesta, pronuncia una decisione sull'assoggettamento a tale obbligo.

3 La segnalazione di un ciberattacco conferisce alle autorità e organizzazioni assoggettate all'obbligo di segnalazione il diritto a ottenere sostegno dall'UFCS nel far fronte all'incidente secondo l'articolo 74 capoverso 3.

4 L'obbligo di segnalazione è finalizzato soltanto a consentire all'UFCS di individuare tempestivamente il modo operativo utilizzato negli attacchi contro infrastrutture critiche, così da avvisare possibili interessati e raccomandare loro misure di prevenzione e di difesa adeguate.

Art. 74*b* Autorità e organizzazioni assoggettate all'obbligo di segnalazione

1 L'obbligo di segnalazione si applica:

a. alle scuole universitarie secondo l'articolo 2 capoverso 2 della legge federale del 30 settembre 2011[55] sulla promozione e sul coordinamento del settore universitario svizzero;

b. alle autorità federali, cantonali e comunali nonché alle organizzazioni intercantonali, cantonali e intercomunali; è eccettuato l'Aggruppamento Difesa,

54 Introdotta dalla cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

55 RS **414.20**

laddove l'esercito presti servizio d'appoggio secondo articolo 67 o servizio attivo secondo l'articolo 76 della legge militare del 3 febbraio 1995[56];

c. alle organizzazioni cui sono affidati compiti di diritto pubblico nei settori della sicurezza e del salvataggio, dell'approvvigionamento di acqua potabile, del trattamento delle acque di scarico e dello smaltimento dei rifiuti;

d. alle imprese attive nel settore dell'approvvigionamento energetico secondo l'articolo 6 capoverso 1 della legge federale del 30 settembre 2016[57] sull'energia, nonché nel commercio, nella misurazione e nella gestione dell'energia; sono esentati i titolari di licenze conformemente alla legge federale del 21 marzo 2003[58] sull'energia nucleare, per quanto riguarda i ciberattacchi effettuati contro un impianto nucleare;

e. alle imprese che sottostanno alla legge dell'8 novembre 1934[59] sulle banche, alla legge del 17 dicembre 2004[60] sulla sorveglianza degli assicuratori o alla legge del 19 giugno 2015[61] sull'infrastruttura finanziaria;

f. agli stabilimenti che figurano nell'elenco cantonale di cui all'articolo 39 capoverso 1 lettera e della legge federale del 18 marzo 1994[62] sull'assicurazione malattie;

g. ai laboratori medici che dispongono di un'autorizzazione secondo l'articolo 16 capoverso 1 della legge del 28 settembre 2012[63] sulle epidemie;

h. alle imprese che dispongono di un'omologazione secondo la legge del 15 dicembre 2000[64] sugli agenti terapeutici per la fabbricazione, l'immissione in commercio e l'importazione di medicamenti;

i. alle organizzazioni che forniscono prestazioni volte a coprire le conseguenze di malattie, infortuni, incapacità al lavoro e al guadagno, vecchiaia, invalidità e grande invalidità;

j. alla Società svizzera di radiotelevisione;

k. alle agenzie di stampa d'importanza nazionale;

l. ai fornitori di servizi postali registrati presso la Commissione delle poste secondo l'articolo 4 capoverso 1 della legge del 17 dicembre 2010[65] sulle poste;

m. alle imprese ferroviarie secondo gli articoli 5 o 8*c* della legge federale del 20 dicembre 1957[66] sulle ferrovie e alle imprese che gestiscono impianti di trasporto a fune, linee filoviarie, autobus e battelli e sono titolari di una

56 RS **510.10**
57 RS **730.0**
58 RS **732.1**
59 RS **952.0**
60 RS **961.01**
61 RS **958.1**
62 RS **832.10**
63 RS **818.101**
64 RS **812.21**
65 RS **783.0**
66 RS **742.101**

concessione secondo l'articolo 6 della legge del 20 marzo 2009[67] sul trasporto di viaggiatori;

n. alle imprese dell'aviazione civile che dispongono di un'autorizzazione dell'Ufficio federale dell'aviazione civile e agli aeroporti nazionali conformemente al Piano settoriale dei trasporti, Parte Infrastruttura aeronautica;

o. alle imprese che trasportano merci sul Reno secondo la legge federale del 23 settembre 1953[68] sulla navigazione marittima sotto bandiera svizzera e alle imprese che gestiscono l'iscrizione, il carico o lo scarico nei porti di Basilea;

p. alle imprese che riforniscono la popolazione di beni indispensabili di uso quotidiano e il cui dissesto totale o parziale comporterebbe considerevoli difficoltà di approvvigionamento;

q. ai fornitori di servizi di telecomunicazione registrati presso l'Ufficio federale delle comunicazioni secondo l'articolo 4 capoverso 1 LTC[69];

r. ai gestori di registri e ai centri di registrazione di domini Internet secondo l'articolo 28*b* LTC;

s. ai fornitori e ai gestori di servizi e infrastrutture che servono all'esercizio dei diritti politici;

t. ai fornitori e ai gestori di servizi di nuvole informatiche, motori di ricerca o servizi di sicurezza e fiduciari digitali nonché ai centri di calcolo, sempre che abbiano una sede in Svizzera;

u. ai produttori di hardware o software i cui prodotti sono utilizzati da infrastrutture critiche, sempre che tali hardware o software abbiano un accesso remoto per la manutenzione o siano impiegati per uno dei seguenti scopi:
   1. la gestione e il monitoraggio di sistemi e processi tecnici,
   2. la garanzia della sicurezza pubblica.

2 Le autorità e organizzazioni che esercitano anche attività non rientranti nel campo di applicazione del capoverso 1 non hanno l'obbligo di segnalare i ciberattacchi che hanno ripercussioni unicamente su queste attività.

3 L'obbligo di segnalazione di cui al capoverso 1 si applica a ciberattacchi che hanno ripercussioni in Svizzera anche se i mezzi informatici interessati si trovano all'estero.

Art. 74*c* Eccezioni all'obbligo di segnalazione

Il Consiglio federale esenta le autorità e organizzazioni dall'obbligo di segnalazione di cui all'articolo 74*b* per quanto riguarda i ciberattacchi che causano guasti funzionali con ripercussioni minime sul funzionamento dell'economia o sul benessere della popolazione.

67 RS **745.1**
68 RS **747.30**
69 RS **784.10**

Art. 74*d* Ciberattacchi da segnalare

Un ciberattacco deve essere segnalato se:

a. compromette il funzionamento dell'infrastruttura critica interessata;

b. ha comportato una manipolazione o una fuga di informazioni;

c. non è stato identificato per un periodo prolungato, in particolare se vi sono indizi secondo cui potrebbe essere stato effettuato per preparare altri ciberattacchi; o

d. è connesso al reato di estorsione, minaccia o coazione.

Art. 74*e* Termine e contenuto della segnalazione

1 La segnalazione deve avvenire entro le 24 ore successive all'individuazione del ciberattacco.

2 Contiene informazioni sull'autorità o sull'organizzazione assoggettata all'obbligo di segnalazione, sul tipo di ciberattacco e sulla sua esecuzione, sulle sue ripercussioni, sulle misure adottate e, se note, sulle misure previste.

3 Se al momento della segnalazione non sono ancora note tutte le informazioni necessarie, l'autorità o l'organizzazione assoggettata all'obbligo di segnalazione completa la stessa non appena dispone di nuove informazioni.

4 Chi deve adempiere l'obbligo di segnalazione per conto di un'autorità o di un'organizzazione non è tenuto, nel quadro della segnalazione, a fornire indicazioni che lo rendono penalmente perseguibile.

5 Il UFCS informa l'autorità o l'organizzazione assoggettata all'obbligo di segnalazione non appena ha ricevuto tutte le informazioni che consentono di adempiere tale obbligo.

Art. 74*f* Trasmissione della segnalazione

1 L'UFCS mette a disposizione un sistema sicuro con cui trasmettergli per via elettronica le segnalazioni di ciberattacchi.

2 Il sistema deve permettere alle autorità e organizzazioni assoggettate all'obbligo di segnalazione di trasmettere anche ad altre autorità la segnalazione del ciberattacco o delle sue ripercussioni, sia nella sua totalità sia in parte.

3 Se per adempiere un obbligo di segnalazione nei confronti di altre autorità sono necessarie informazioni che vanno oltre quelle menzionate all'articolo 74*e*, il sistema deve permettere alle autorità e organizzazioni assoggettate a tale obbligo di trasmettere queste informazioni direttamente alle autorità interessate, senza che il UFCS vi acceda.

Sezione 3: Protezione dei dati e scambio di informazioni[70]

Art. 75[71] Trattamento di dati personali

1 Per l'adempimento dei propri compiti, il UFCS può trattare dati personali, compresi elementi di indirizzo di cui all'articolo 3 lettera f LTC[72] e i relativi dati personali degni di particolare protezione, che contengono informazioni su:

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 cibersicurezza;

b. perseguimenti o sanzioni di carattere amministrativo o penale.

2 In caso di trattamento di dati personali o di indizi concreti di usurpazione d'identità o di utilizzazione non autorizzata di elementi di indirizzo, il UFCS informa le persone interessate, sempre che ciò non comporti un onere sproporzionato e nessun interesse pubblico preponderante vi si opponga.

Art. 76[73] Cooperazione a livello nazionale

1 Il UFCS e i gestori di infrastrutture critiche possono comunicarsi reciprocamente dati personali, sempre che ciò sia necessario alla protezione contro le ciberminacce.

2 Il UFCS e i fornitori di servizi di telecomunicazione possono comunicarsi reciprocamente elementi di indirizzo e i relativi dati personali, sempre che ciò sia necessario alla protezione contro le ciberminacce.

Art. 76*a*[74] Sostegno alle autorità

1 Il UFCS sostiene il SIC con valutazioni periodiche sul numero, sul tipo e sulla portata dei ciberattacchi e, su richiesta, con analisi tecniche delle ciberminacce.

2 Concede al SIC l'accesso a informazioni che riguardano l'identità e il modo di operare degli autori di ciberattacchi al fine di individuare tempestivamente e sventare minacce alla sicurezza interna o esterna, valutare la situazione di minaccia e assicurare un servizio di preallerta informativa per la protezione di infrastrutture critiche secondo l'articolo 6 capoversi 1 lettera a, 2 e 5 LAIn[75].

70 Introdotta dalla cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

71 Nuovo testo giusta la cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

72 RS **784.10**

73 Nuovo testo giusta la cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

74 Introdotto dalla cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

75 RS **121**

3 Il UFCS concede alle autorità di perseguimento penale l'accesso a informazioni che riguardano l'identità e il modo di operare degli autori di ciberattacchi.

4 Concede ai servizi cantonali competenti per la cibersicurezza l'accesso alle informazioni necessarie alla protezione contro le ciberminacce.

Art. 77 Cooperazione a livello internazionale

1 Il UFCS può scambiare con servizi esteri e internazionali competenti per la cibersicurezza informazioni che permettono di stabilire l'identità e il modo di operare degli autori di ciberattacchi, se detti servizi necessitano di tali informazioni per l'adempimento di compiti che corrispondono a quelli del UFCS. Se lo scambio di informazioni concerne anche dati personali, vanno osservati gli articoli 16 e 17 LPD[76].

2 Lo scambio di informazioni di cui al capoverso 1 è ammesso soltanto se i servizi esteri e internazionali garantiscono che i dati sono trattati per i fini previsti.

Art. 78[77]

Art. 79 Conservazione e archiviazione dei dati

1 Il UFCS conserva i dati personali soltanto fino a che sono utili per individuare ciberminacce o far fronte a ciberincidenti, ma al massimo per cinque anni dall'ultimo utilizzo a tale scopo. Per i dati personali degni di particolare protezione il termine è di due anni.[78]

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

Art. 80[79]

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:

76 RS **235.1**
77 Abrogato dalla cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), con effetto dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).
78 Nuovo testo giusta la cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), in vigore dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).
79 Abrogato dalla cifra I della LF del 29 set. 2023 (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), con effetto dal 1° apr. 2025 (RU **2024** 257; **2025** 173; FF **2023** 84).

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.

Data dell'entrata in vigore:
Art. 87: 1° maggio 2022[80]
Rimanenti disposizioni: 1° gennaio 2024[81]

80 DCF del 6 apr. 2022.
81 O dell' 8 nov. 2023 (RU **2023** 650).

Allegato 1
(art. 89)

Modifica di altri atti normativi

Le leggi federali qui appresso sono modificate come segue:

...[82]

82 Le mod. possono essere consultate alla RU **2022** 232.

Allegato 2
(art. 91)

Coordinamento con altri atti normativi

...[83]

83 Le disp. di coordinamento possono essere consultate alla RU **2022** 232.