Ordinanza sulla sicurezza delle informazioni in seno all'Amministrazione federale e all'esercito

(Ordinanza sulla sicurezza delle informazioni, OSIn)

avamprogetto del 24 agosto 2022

Il Consiglio federale svizzero,

visti gli articoli 2 capoversi 3 e 4, 12 capoverso 3, 83 capoverso 3, 84 capoverso 1, 85 capoversi 1 e 2 e 86 capoverso 4 della legge sulla sicurezza delle informazioni del 18 dicembre 2020[1] (LSIn),

ordina:

Sezione 1: Disposizioni generali

Art. 1 Oggetto
(art. 1 LSIn)

La presente ordinanza disciplina i compiti, le responsabilità e le competenze nonché le procedure per garantire la sicurezza delle informazioni in seno all'Amministrazione federale e all'esercito.

Art. 2 Campo d'applicazione
(art. 2–3 e 84 cpv. 3 LSIn)

[1] La presente ordinanza si applica:

a. al Consiglio federale;

b. alle unità amministrative dell'Amministrazione federale centrale secondo l'articolo 7 dell'ordinanza del 25 novembre 1998[2] sull'organizzazione del Governo e dell'Amministrazione (OLOGA);

c. all'esercito.

[2] La LSIn e la presente ordinanza si applicano alle unità amministrative dell'Amministrazione federale decentralizzata secondo l'articolo 7*a* OLOGA[3] come segue:

1 RS **128**
2 RS **172.010.1**
3 RS **172.010.1**

a. alle unità amministrative che accedono a mezzi informatici dei fornitori interni di prestazioni TIC secondo l'articolo 9 dell'ordinanza del 25 novembre 2020[4] sulla trasformazione digitale e l'informatica (OTDI), se questi sono assegnati al livello di sicurezza «protezione elevata» o «protezione molto elevata» secondo l'articolo 28: l'intera LSIn e la presente ordinanza;

b. alle unità amministrative che impiegano mezzi informatici assegnati al livello di sicurezza «protezione elevata» o «protezione molto elevata» secondo l'articolo 28: l'intera LSIn e la presente ordinanza;

c. alle unità amministrative che non rientrano tra quelle di cui alla lettera a o b, ma che trattano informazioni classificate della Confederazione: gli articoli 9–15 e 27–73 LSIn nonché le disposizioni della Sezione 4 della presente ordinanza.

3 La Cancelleria federale o i dipartimenti possono chiedere al Consiglio federale di assoggettare le unità amministrative dell'Amministrazione federale decentralizzata che non rientrano tra quelle di cui al capoverso 2 alla LSIn e alla presente ordinanza o a parti di essa.

4 Nell'allegato 1 sono riportate:

a. le unità amministrative di cui al capoverso 2;

b. le unità amministrative di cui al capoverso 3 e la relativa applicabilità della LSIn e della presente ordinanza.

5 Le organizzazioni di cui all'articolo 2 capoverso 4 della legge del 21 marzo 1997[5] sull'organizzazione del Governo e dell'Amministrazione (LOGA) sono escluse dal campo d'applicazione della LSIn e della presente ordinanza.

6 Fatto salvo l'articolo 3 capoverso 2 LSIn, per i Cantoni si applicano:

a. in caso di trattamento di informazioni classificate della Confederazione: le disposizioni della Sezione 4;

b. in caso di accesso a mezzi informatici della Confederazione: gli articoli 28–30 e 34.

Sezione 2: Principi

Art. 3 Obiettivi in materia di sicurezza

(art. 7 cpv. 2 lett. a LSIn)

1 Le organizzazioni di cui all'articolo 2 provvedono congiuntamente a una protezione delle loro informazioni e dei loro mezzi informatici basata sui rischi nonché a una resilienza adeguata riguardo ai rischi in materia di sicurezza delle informazioni.

2 Mediante la collaborazione e lo scambio di informazioni con altre autorità federali, i Cantoni, i Comuni, l'economia, la società, la scienza e partner internazionali contribuiscono a migliorare la sicurezza delle informazioni in Svizzera.

4 RS **172.010.58**
5 RS **172.010**

3 Si impegnano a favore di un'armonizzazione delle prescrizioni e dei livelli di sicurezza a livello nazionale e internazionale allo scopo di permettere l'interazione tra autorità federali e altre autorità della Confederazione nonché dei Cantoni e dei Comuni.

Art. 4 Responsabilità

1 Le unità amministrative sono responsabili della protezione delle informazioni di cui effettuano o commissionano il trattamento nonché della sicurezza dei mezzi informatici che gestiscono direttamente o che fanno gestire da terzi.

2 Nel loro settore di competenza le unità amministrative si occupano di tutti i compiti che la presente ordinanza o il diritto federale non attribuiscono a un'altra organizzazione o a un altro servizio.

3 I collaboratori dell'Amministrazione federale nonché i militari che trattano informazioni o utilizzano mezzi informatici della Confederazione sono responsabili del loro trattamento e del loro utilizzo conforme alle prescrizioni.

4 I superiori di tutti i livelli sono responsabili della formazione adeguata ai compiti dei loro collaboratori nel settore della sicurezza delle informazioni e sono tenuti a verificare che questi rispettino le prescrizioni.

Sezione 3: Gestione della sicurezza delle informazioni

Art. 5 Sistema di gestione della sicurezza delle informazioni
(art. 7 cpv. 1 LSIn)

1 Ogni unità amministrativa elabora un sistema di gestione della sicurezza delle informazioni (SGSI).

2 Definiscono gli obiettivi per il loro SGSI, verificano annualmente se gli obiettivi vengono raggiunti e rilevano gli indicatori necessari a tale scopo.

3 Fanno in modo che il loro SGSI venga verificato almeno ogni tre anni da un servizio indipendente o dal dipartimento e si occupano del miglioramento costante del sistema.

4 Si occupano del coordinamento del loro SGSI con la gestione ordinaria dei rischi, la gestione della continuità aziendale e la gestione delle crisi.

Art. 6 Cura delle basi legali e degli obblighi contrattuali
(art. 7 cpv. 1 LSIn)

1 Le unità amministrative, i dipartimenti e il servizio specializzato della Confederazione per la sicurezza delle informazioni tengono un registro ciascuno delle basi legali e degli obblighi contrattuali relativi alla sicurezza delle informazioni determinanti nel loro settore di competenza e lo tengono aggiornato.

2 Le unità amministrative e i dipartimenti consultano il servizio specializzato della Confederazione per la sicurezza delle informazioni riguardo a direttive e a progetti rilevanti sotto il profilo della sicurezza.

Art. 7 Inventariazione degli oggetti da proteggere
(art. 7 cpv. 1 LSIn)

1 Le unità amministrative compilano un inventario dei loro oggetti da proteggere e lo tengono aggiornato.

2 Sono considerati oggetti da proteggere:

a. le raccolte di informazioni trattate per adempiere un compito della Confederazione;

b. i mezzi informatici di cui all'articolo 5 lettera a LSIn.

3 L'inventario serve a comprovare:

a. la necessità di protezione degli oggetti da proteggere;

b. le responsabilità per gli oggetti da proteggere;

c. eventualmente l'utilizzo condiviso degli oggetti da proteggere;

d. la partecipazione di terzi;

e. il risultato della valutazione dei rischi;

f. l'attuazione delle misure di sicurezza e l'assunzione dei rischi residui;

g. i controlli e gli audit periodici.

Art. 8 Gestione dei rischi
(art. 7 cpv. 2 lett. b e 8 LSIn)

1 Le unità amministrative valutano costantemente i rischi per i loro oggetti da proteggere e a tale proposito svolgono in particolare i seguenti compiti:

a. analizzare periodicamente minacce e vulnerabilità e valutano le loro ripercussioni sugli oggetti da proteggere;

b. attuare le misure necessarie e controllare l'efficacia;

c. controllare il rispetto delle direttive;

d. comprovare l'accettazione dei rischi residui.

2 Il servizio specializzato della Confederazione per la sicurezza delle informazioni, le unità amministrative che forniscono prestazioni e gli organi di sicurezza della Confederazione informano le unità amministrative e i dipartimenti in merito alle minacce e alle vulnerabilità attuali nonché in merito ai rischi che li riguardano. In caso di necessità raccomandano misure volte a ridurre i rischi.

3 Le unità amministrative redigono un rapporto sui loro rischi relativi alla sicurezza delle informazioni nel quadro del processo ordinario di gestione dei rischi secondo le direttive dell'Amministrazione federale delle finanze.

Art. 9 Autorizzazione ed elenco delle deroghe
(art. 7 cpv. 1 LSIn)

1 Se un'unità amministrativa non è in grado di adempiere una direttiva per un oggetto da proteggere necessita di un'autorizzazione rilasciata dal servizio che ha deciso la direttiva.

2 Il servizio specializzato della Confederazione per la sicurezza delle informazioni e i dipartimenti possono delegare l'autorizzazione di deroghe.

3 Se una deroga che rientra nell'ambito di competenza del servizio specializzato della Confederazione per la sicurezza delle informazioni riguarda anche direttive della Cancelleria federale sulla trasformazione digitale e la governance delle TIC, il servizio specializzato della Confederazione per la sicurezza delle informazioni sente in via preliminare il delegato TDT di cui all'articolo 4 capoverso 1 OTDI[6].

4 Le unità amministrative, i dipartimenti e il servizio specializzato della Confederazione per la sicurezza delle informazioni tengono ciascuno un registro delle autorizzazioni eccezionali che:

a. hanno rilasciato essi stessi;

b. sono state rilasciate per i loro oggetti da proteggere.

Art. 10 Collaborazione con terzi
(art. 9 LSIn)

1 Secondo le direttive di cui all'articolo 10 le unità amministrative valutano i rischi per i loro oggetti da proteggere che derivano dalla collaborazione con terzi e la loro dipendenza da terzi.

2 I servizi d'acquisto di cui agli articoli 9 e 10 dell'ordinanza del 24 ottobre 2012[7] concernente l'organizzazione degli acquisti pubblici dell'Amministrazione federale (OOAPub) partecipano alla valutazione e mettono a disposizione le informazioni necessarie.

3 Previa consultazione della Conferenza degli acquisti della Confederazione di cui all'articolo 24 OOAPub, il servizio specializzato della Confederazione per la sicurezza delle informazioni raccomanda quali disposizioni in materia di sicurezza delle informazioni devono essere previste nei contratti di acquisto e per prestazioni di servizio della Confederazione.

Art. 11 Formazione e sensibilizzazione
(art. 7 cpv. 1 e 20 cpv. 1 lett. c LSIn)

1 Le unità amministrative formano i loro collaboratori quando assumono la loro funzione e poi periodicamente in maniera tale che siano in grado di far fronte alla loro responsabilità in materia di sicurezza delle informazioni. Tengono un registro in merito alle formazioni e alla relativa partecipazione.

2 I contenuti delle formazioni riguardano in particolare:

a. l'identificazione corretta della necessità di protezione delle informazioni;

b. la gestione sicura di informazioni e mezzi informatici;

c. la reazione corretta in caso di sospetto di un incidente legato alla sicurezza;

6 RS **172.010.58**
7 RS **172.056.15**

d. la conoscenza dell'organizzazione di sicurezza nonché delle persone di contatto in caso di domande relative alla sicurezza delle informazioni;

e. i compiti di controllo dei superiori;

f. l'attuazione della sicurezza delle informazioni nei progetti e nell'attività operativa.

3 Le unità amministrative, i dipartimenti e il servizio specializzato della Confederazione per la sicurezza delle informazioni provvedono a sensibilizzare periodicamente i collaboratori di tutti i livelli in merito ai rischi legati alla sicurezza delle informazioni.

4 Il servizio specializzato della Confederazione per la sicurezza delle informazioni assicura il coordinamento e realizza ausili per le attività di formazione e di sensibilizzazione.

Art. 12 Gestione degli incidenti
(art. 7 cpv. 1 e 10 cpv. 1 LSIn)

1 D'intesa con i loro fornitori di prestazioni, le unità amministrative stabiliscono come notificare e gestire gli incidenti legati alla sicurezza e le lacune in materia di sicurezza. Stabiliscono chi decide in merito a misure immediate.

2 I fornitori di prestazioni notificano senza indugio alle unità amministrative beneficiarie delle loro prestazioni gli incidenti legati alla sicurezza e le lacune in materia di sicurezza individuati che li riguardano e forniscono loro sostegno nella gestione.

3 Il servizio specializzato della Confederazione per la sicurezza delle informazioni può fornire sostegno alle unità amministrative e ai dipartimenti nella gestione di incidenti legati alla sicurezza e di lacune in materia di sicurezza.

4 Quando si tratta di gestire incidenti legati alla sicurezza le unità amministrative verificano se occorre effettuare una notifica all'Incaricato federale della protezione dei dati e della trasparenza secondo la legislazione sulla protezione dei dati.

5 Informano senza indugio il loro dipartimento e il servizio specializzato della Confederazione per la sicurezza delle informazioni in merito all'incidente legato alla sicurezza o alla lacuna in materia di sicurezza se è soddisfatta una delle condizioni seguenti:

a. potrebbe essere compromesso il funzionamento dell'Amministrazione federale o dell'esercito;

b. è interessato un mezzo informatico del livello di sicurezza «protezione elevata» o «protezione molto elevata»;

c. potrebbero essere interessati diversi dipartimenti;

d. potrebbe essere minacciata la protezione di informazioni classificate di uno Stato o di un'organizzazione internazionale con il quale o la quale il Consiglio federale ha concluso un trattato internazionale secondo l'articolo 87 LSIn;

e. l'incidente legato alla sicurezza o la lacuna in materia di sicurezza potrebbe avere un'importanza politica elevata;

f. l'incidente legato alla sicurezza o la lacuna in materia di sicurezza richiede misure che vanno oltre la procedura di cui al capoverso 1.

6 Il servizio specializzato della Confederazione per la sicurezza delle informazioni valuta il rischio e la necessità di sostegno insieme all'unità amministrativa interessata.

7 Nei casi di cui al capoverso 5, d'intesa con l'unità amministrativa interessata e il dipartimento interessato può assumere la direzione della gestione dell'incidente legato alla sicurezza o di una lacuna in materia di sicurezza. In tale contesto ha i compiti e le competenze seguenti:

a. può obbligare le unità amministrative, i fornitori di prestazioni e i terzi interessati a comunicare loro tutte le informazioni necessarie;

b. può disporre misure immediate;

c. può impiegare specialisti esterni a scopo di sostegno;

d. informa la direzione delle unità amministrative e dei dipartimenti interessati in merito all'andamento.

8 Se dopo un incidente legato alla sicurezza o una lacuna in materia di sicurezza la sicurezza delle informazioni è stata ripristinata e se i lavori successivi necessari nonché il loro finanziamento sono definiti, il servizio specializzato della Confederazione per la sicurezza delle informazioni ritrasferisce la direzione per l'ulteriore trattamento all'unità amministrativa interessata.

Art. 13 Pianificazione dei controlli e degli audit

(art. 7 cpv. 1, 81 cpv. 2 lett. c e 83 cpv. 1 lett. c LSIn)

1 All'interno di un piano annuale dei controlli e degli audit le unità amministrative e i dipartimenti stabiliscono le modalità con cui verificano in base ai rischi il rispetto delle prescrizioni secondo la presente ordinanza e l'efficacia delle misure volte a garantire la sicurezza delle informazioni nel loro settore di competenza nonché presso terzi incaricati.

2 Gli audit presso terzi che dispongono di una dichiarazione di sicurezza aziendale di cui all'articolo 61 LSIn devono essere coordinati con il servizio specializzato per la procedura di sicurezza relativa alle aziende di cui all'articolo 51 capoverso 2 LSIn.

3 Il servizio specializzato della Confederazione per la sicurezza delle informazioni rileva il fabbisogno di controlli e di audit per garantire la sicurezza delle informazioni di tutta l'Amministrazione federale e dell'esercito e lo comunica al Controllo federale delle finanze.

Art. 14 Rapporti

(art. 7 cpv. 1, 81 cpv. 2 lett. c e 83 cpv. 1 lett. h LSIn)

1 Ogni anno i dipartimenti e la Cancelleria federale redigono un rapporto destinato al servizio specializzato della Confederazione per la sicurezza delle informazioni in merito allo stato della sicurezza delle informazioni nel loro settore di competenza.

2 Rilevano le informazioni necessarie a tale scopo presso le unità amministrative e i loro fornitori di prestazioni.

3 Ogni anno il servizio specializzato della Confederazione per la sicurezza delle informazioni redige un rapporto destinato al Consiglio federale in merito allo stato della sicurezza delle informazioni in seno alla Confederazione.

4 Stabilisce le modalità per i rapporti dei fornitori interni di prestazioni di cui all'articolo 9 OTDI[8].

5 Coordina i rapporti con le autorità assoggettate di cui all'articolo 2 capoverso 1 LSIn.

Art. 15 Direttive concernenti la gestione della sicurezza delle informazioni

(art. 85 LSIn)

Il servizio specializzato della Confederazione per la sicurezza delle informazioni emana istruzioni generali e astratte valide per tutti i servizi di cui all'articolo 2 capoversi 1–3 concernenti i requisiti minimi per la gestione della sicurezza delle informazioni secondo gli articoli 5–14.

Sezione 4: Informazioni classificate

Art. 16 Principi

(art. 11 LSIn)

1 La comunicazione e il conferimento dell'accesso a informazioni classificate nonché la produzione di supporti di dati classificati devono essere limitati al minimo indispensabile.

2 Se le informazioni sono riunite in una collezione occorre verificare se quest'ultima deve essere classificata o assegnata a un livello di classificazione più elevato.

3 In presenza di domande di accesso a documenti ufficiali, il servizio competente verifica, indipendentemente da un'eventuale menzione di classificazione, se, conformemente alla legge sulla trasparenza del 17 dicembre 2004[9], l'accesso vada accordato, limitato, differito o negato.

Art. 17 Servizi incaricati della classificazione

(art. 12 LSIn)

1 Le persone e i servizi seguenti sono competenti per la classificazione e la declassificazione di informazioni:

a. i collaboratori della Confederazione nonché i militari: per supporti di informazioni che producono o che fanno produrre, e per informazioni che comunicano a voce;

b. i collaboratori di aziende che dispongono di una dichiarazione di sicurezza aziendale secondo l'articolo 61 LSIn: per supporti di informazioni che producono su incarico della Confederazione;

c. la persona responsabile del compito: per oggetti da proteggere di cui all'articolo 7 capoverso 2 lettera a.

8 RS **172.010.58**
9 RS **152.3**

2 All'interno di un catalogo di classificazione le unità amministrative, la Cancelleria federale e i dipartimenti stabiliscono in che modo classificare le informazioni che vengono trattate di frequente nel rispettivo settore di competenza.

3 Il servizio specializzato della Confederazione per la sicurezza delle informazioni verifica i cataloghi di classificazione di cui al capoverso 2 e in caso di necessità formula una raccomandazione.

4 Previa consultazione della Conferenza degli incaricati della sicurezza delle informazioni, stabilisce in che modo classificare le informazioni che vengono trattate di frequente nell'Amministrazione federale e nell'esercito.

Art. 18 Livello di classificazione «ad uso interno»
(art. 13 cpv. 1 LSIn)

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 LSIn come segue:

a. un importante processo operativo del Consiglio federale o dell'Amministrazione federale o un importante processo di condotta dell'esercito è più difficoltoso;

b. l'esecuzione di impieghi delle autorità di perseguimento penale, del Servizio delle attività informative della Confederazione (SIC), dell'esercito o di altri organi di sicurezza della Confederazione è più difficoltosa;

c. singole persone vengono ferite fisicamente;

d. la sicurezza nucleare o la sicurezza di impianti nucleari o di materiale nucleare è minacciata indirettamente;

e. la Svizzera subisce svantaggi a livello economico o di politica estera;

f. le relazioni tra la Confederazione e i Cantoni o tra i Cantoni sono intralciate per mesi.

Art. 19 Livello di classificazione «confidenziale»
(art. 13 cpv. 2 LSIn)

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 LSIn come segue:

a. la capacità decisionale o la capacità d'azione del Consiglio federale, del Parlamento, di diverse unità amministrative o di diversi corpi di truppa dell'esercito è più difficoltosa per più giorni;

b. l'esecuzione conforme agli obiettivi di operazioni delle autorità di perseguimento penale, del SIC, dell'esercito o di altri organi di sicurezza della Confederazione è minacciata;

c. i mezzi e i metodi operativi dei servizi informazioni e delle autorità di perseguimento penale della Confederazione nonché l'identità delle fonti e delle persone esposte sono resi noti;

d. la sicurezza della popolazione è minacciata per più giorni oppure singole persone o gruppi di persone muoiono;

e. la sicurezza nucleare o la sicurezza di impianti nucleari o di materiale nucleare è minacciata;

f. l'approvvigionamento economico del Paese o l'esercizio delle infrastrutture critiche sono più difficoltosi;

g. la Svizzera subisce svantaggi considerevoli a livello economico o di politica estera o le relazioni diplomatiche con uno Stato o un'organizzazione internazionale vengono interrotte;

h. la posizione negoziale della Svizzera in importanti affari di politica estera è temporaneamente indebolita considerevolmente.

Art. 20 Livello di classificazione «segreto»
(art. 13 cpv. 3 LSIn)

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 LSIn come segue:

a. il Consiglio federale, il Parlamento, diverse unità amministrative o diversi corpi di truppa dell'esercito per giorni sono incapaci di decidere o di agire oppure la loro capacità decisionale o la loro capacità d'azione è più difficoltosa per settimane;

b. l'esecuzione di operazioni importanti a livello strategico delle autorità di perseguimento penale, del SIC, dell'esercito o di altri organi di sicurezza della Confederazione è minacciata oppure più difficoltosa in misura particolarmente elevata per giorni;

c. le fonti strategiche, l'identità di persone particolarmente esposte oppure i mezzi e i metodi strategici dei servizi informazioni e delle autorità di perseguimento penale della Confederazione sono resi noti;

d. la sicurezza della popolazione è esposta a una minaccia particolarmente grave per settimane oppure un numero elevato di persone muore;

e. la sicurezza nucleare o la sicurezza di impianti nucleari o di materiale nucleare è minacciata in misura particolarmente elevata;

f. l'approvvigionamento economico del Paese o l'esercizio delle infrastrutture critiche non funzionano per giorni;

g. la Svizzera soffre per settimane di conseguenze particolarmente gravi a livello di politica estera o a livello economico come misure d'embargo o sanzioni;

h. la posizione negoziale della Svizzera in affari strategici di politica estera è indebolita per anni.

Art. 21 Direttive concernenti il trattamento
(art. 6 cpv. 2, 84 cpv. 1 e 85 LSIn)

1 Il servizio specializzato della Confederazione per la sicurezza delle informazioni emana istruzioni generali e astratte valide per tutti i servizi di cui all'articolo 2 capoversi 1–3 concernenti il trattamento di informazioni classificate e i requisiti organizzativi, tecnici, edili e riguardanti il personale per la loro protezione.

2 Consulta in via preliminare i seguenti servizi:

a. il servizio crittografico dell'esercito;

b. i servizi competenti per l'acquisto di beni nell'ambito della crittologia secondo l'articolo 10 capoverso 1 lettera d OOAPub[10]; e

c. i servizi competenti per la sicurezza degli oggetti dell'Amministrazione federale e dell'esercito.

3 Tiene conto degli standard internazionali in materia.

4 La Cancelleria federale disciplina il trattamento degli affari classificati del Consiglio federale.

5 Il trattamento di informazioni classificate provenienti dall'estero avviene secondo le prescrizioni che corrispondono al livello di classificazione estero. Sono fatte salve prescrizioni divergenti di un trattato internazionale secondo l'articolo 87 LSIn.

Art. 22 Misure di sicurezza specifiche all'impiego
(art. 6 cpv. 2 e 85 LSIn)

1 Se le informazioni classificate vengono trattate nel quadro di un impiego o di un'operazione e sono accessibili soltanto a una cerchia di utenti chiusa e determinabile in maniera inequivocabile, le seguenti persone possono decidere prescrizioni per operazioni o impieghi specifici dopo aver consultato il servizio specializzato della Confederazione per la sicurezza delle informazioni:

a. il direttore dell'Ufficio federale di polizia;

b. il direttore del SIC;

c. il capo dell'esercito;

d. il capo del Comando Operazioni;

e. il direttore dell'Ufficio federale della dogana e della sicurezza dei confini.

2 I servizi di cui al capoverso 1 fanno in modo che sia possibile individuare in modo equivocabile se si applicano le prescrizioni relative al trattamento semplificato.

3 Al di fuori della cerchia di utenti nonché per la conservazione in vista dell'archiviazione si applicano le direttive concernenti il trattamento secondo l'articolo 21.

10 RS **172.056.15**

Art. 23 Accreditamento in materia di sicurezza di mezzi informatici
(art. 83 cpv. 1 lett. e LSIn)

1 I mezzi informatici sono soggetti ad accreditamento in materia di sicurezza prima di essere messi in servizio se è soddisfatta una delle condizioni seguenti:

a. vengono impiegati per compiti che riguardano più uffici in cui vengono trattate informazioni classificate «segreto»;

b. vengono impiegati per compiti che riguardano più autorità o dipartimenti in cui vengono trattate informazioni classificate «confidenziale»;

c. l'accreditamento in materia di sicurezza è necessario per la collaborazione a livello internazionale.

2 L'accreditamento in materia di sicurezza dimostra che i mezzi informatici soddisfano i requisiti minimi di sicurezza per il relativo livello di classificazione e che i rischi residui sono sostenibili secondo lo stato della tecnica.

3 In caso di cambiamenti sostanziali riguardo ai rischi o di cambiamenti sostanziali del mezzo informatico l'accreditamento viene ripetuto.

4 Se non è possibile rilasciare l'accreditamento in materia di sicurezza poiché il mezzo informatico non soddisfa i requisiti minimi di sicurezza, è il Consiglio federale a decidere in merito ai rischi residui.

5 Il servizio specializzato della Confederazione per la sicurezza delle informazioni svolge i compiti seguenti:

a. rilascia l'accreditamento in materia di sicurezza dopo aver consultato il servizio crittografico dell'esercito nonché i servizi di cui all'articolo 10 capoverso 1 lettera d OOAPub[11];

b. esclusivamente per sistemi militari può delegare la competenza per l'accreditamento in materia di sicurezza all'Aggruppamento Difesa.

6 Il [dipartimento competente] definisce la procedura di accreditamento in materia di sicurezza e tiene conto degli standard internazionali in materia.

Art. 24 Protezione in caso di pericolo per le informazioni classificate
(art. 10 cpv. 1 e 11 cpv. 1 LSIn)

1 Chiunque constata che le informazioni classificate sono esposte a pericolo, sono andate perse o sono state usate in modo abusivo oppure che le informazioni sono state manifestamente classificate in modo errato o che, per errore, non sono state classificate, è tenuto ad adottare le necessarie misure di protezione.

2 Avvisa senza indugio il servizio incaricato della classificazione e gli organi di sicurezza competenti.

11 RS **172.056.15**

Art. 25 Verifica della necessità di protezione e cerchia delle persone autorizzate
(art. 11 cpv. 2 LSIn)

I servizi incaricati della classificazione verificano la necessità di protezione delle loro informazioni classificate e la cerchia delle persone autorizzate almeno ogni cinque anni nonché sempre nei casi in cui le informazioni vengono offerte all'Archivio federale per l'archiviazione.

Art. 26 Archiviazione
(art. 12 cpv. 3 LSIn)

1 L'archiviazione di informazioni classificate è retta dalle prescrizioni della legislazione in materia di archiviazione.

2 L'Archivio federale fa in modo che sia garantita la sicurezza delle informazioni secondo la presente ordinanza.

3 Dopo la scadenza del termine di protezione la classificazione degli archivi viene meno. Una proroga del termine di protezione si fonda sull'articolo 14 dell'ordinanza sull'archiviazione dell'8 settembre 1999[12].

Sezione 5: Sicurezza nell'impiego di mezzi informatici

Art. 27 Procedura di sicurezza
(art. 16 LSIn)

1 Le unità amministrative devono essere in grado di comprovare la necessità di protezione dei loro oggetti da proteggere e la rilevanza di questi ultimi per la gestione della continuità aziendale.

2 Attuano le direttive minime del relativo livello di sicurezza e verificano se sono necessarie misure di sicurezza supplementari.

3 Indicano i rischi che non possono essere adeguatamente ridotti (rischi residui).

4 I responsabili della sicurezza di cui all'articolo 36 decidono se i rischi residui vengono assunti. Possono delegare questa decisione ad altri membri della direzione.

5 La procedura di sicurezza viene ripetuta in caso di cambiamenti sostanziali della minaccia, della tecnologia, dei compiti o della situazione organizzativa.

6 Le unità amministrative verificano ogni anno se vi è stato un cambiamento sostanziale secondo il capoverso 5.

12 RS **152.11**

Art. 28 Assegnazione ai livelli di sicurezza «protezione elevata» e «protezione molto elevata»
(art. 17 LSIn)

1 Il livello di sicurezza «protezione elevata» viene assegnato a un mezzo informatico se una violazione della sicurezza delle informazioni può comportare un pregiudizio considerevole secondo l'articolo 19 o un danno tra 50 e 500 milioni di franchi.

2 Il livello di sicurezza «protezione molto elevata» viene assegnato a un mezzo informatico se una violazione della sicurezza delle informazioni può comportare un pregiudizio secondo l'articolo 20 o un danno di almeno 500 milioni di franchi.

Art. 29 Misure di sicurezza
(art. 6 cpv. 3, 18 e 85 LSIn)

1 Il servizio specializzato della Confederazione per la sicurezza delle informazioni emana istruzioni generali e astratte applicabili a tutti i servizi di cui all'articolo 2 capoversi 1–3 concernenti i requisiti minimi per i relativi livelli di sicurezza secondo l'articolo 17 LSIn.

2 Tiene conto dei requisiti per la sicurezza dei dati personali secondo la legislazione sulla protezione dei dati nonché di altre informazioni che la Confederazione è tenuta a proteggere in virtù di un obbligo legale o contrattuale.

3 Per i mezzi informatici seguenti, l'efficacia delle misure di sicurezza deve essere verificata prima della messa in servizio, in caso di cambiamenti sostanziali dei rischi durante l'esercizio, però almeno ogni cinque anni:

a. mezzi informatici assegnati al livello di sicurezza «protezione elevata» che vengono impiegati per adempiere compiti che riguardano più autorità o dipartimenti;

b. mezzi informatici assegnati al livello di sicurezza «protezione molto elevata».

4 I dipartimenti e la Cancelleria federale inseriscono i loro mezzi informatici assegnati al livello di sicurezza «protezione molto elevata» nella loro gestione della continuità.

Art. 30 Sicurezza durante l'esercizio
(art. 19 LSIn)

1 Le unità amministrative assicurano che le responsabilità per la sicurezza informatica a livello operativo siano definite negli accordi di progetto e di prestazione stipulati con i fornitori interni di prestazioni.

2 I fornitori interni di prestazioni mettono a disposizione delle unità amministrative, della Cancelleria federale, dei dipartimenti e del servizio specializzato della Confederazione per la sicurezza delle informazioni le informazioni di cui necessitano per garantire la sicurezza delle informazioni.

3 Garantiscono di disporre delle capacità necessarie in termini finanziari e di personale per l'individuazione tempestiva, l'analisi tecnica e la gestione di incidenti legati alla sicurezza e di lacune in materia di sicurezza che riguardano loro o, nel quadro degli accordi di cui al capoverso 2, i loro beneficiari di prestazioni.

4 Vigilano sull'utilizzo della loro infrastruttura informatica e la monitorano regolarmente alla ricerca di minacce e vulnerabilità tecniche. Possono incaricare terzi del monitoraggio.

6 Il trattamento di dati personali nel quadro della vigilanza e del monitoraggio secondo il capoverso 4 si fonda sull'ordinanza del 22 febbraio 2012[13] sul trattamento di dati personali derivanti dall'utilizzazione dell'infrastruttura elettronica della Confederazione.

Sezione 6: Misure relative alle persone e protezione fisica

Art. 31 Verifica dell'identità di persone e macchine

(art. 20 e 85 LSIn)

1 Dopo aver consultato il delegato TDT, il servizio specializzato della Confederazione per la sicurezza delle informazioni emana istruzioni generali e astratte applicabili a tutti i servizi di cui all'articolo 2 capoversi 1–3 concernenti i requisiti tecnici minimi per la verifica basata sui rischi dell'identità di persone e macchine che necessitano di avere accesso a informazioni, mezzi informatici, locali e altre infrastrutture della Confederazione.

2 Il trattamento di dati personali in sede di verifica dell'identità in sistemi di gestione delle identità secondo l'articolo 24 LSIn si fonda sulle disposizioni dell'ordinanza del 19 ottobre 2016[14] sui sistemi di gestione delle identità e sui servizi di elenchi della Confederazione.

Art. 32 Sicurezza delle persone

(art. 6 cpv. 2 e 3, 8 e 20 cpv. 1 lett. a e c LSIn)

1 Le unità amministrative assicurano che i collaboratori soggetti a un controllo di sicurezza relativo alle persone secondo l'ordinanza del …[15] sui controlli di sicurezza relativi alle persone (OCSP) vengano sensibilizzati ogni anno in merito all'attività determinante sensibile sotto il profilo della sicurezza e ai relativi rischi.

2 I collaboratori di cui al capoverso 1 sono tenuti a comunicare al loro datore di lavoro le circostanze nel loro contesto privato e professionale che compromettono l'esercizio conforme alle prescrizioni dell'attività sensibile sotto il profilo della sicurezza.

Art. 33 Sospetto di reato

(art. 7 cpv. 2 lett. c LSIn)

1 Se in presenza di una violazione delle prescrizioni relative alla sicurezza delle informazioni al contempo è ipotizzabile un reato, i dipartimenti inoltrano gli atti con i verbali d'interrogatorio al Ministero pubblico della Confederazione o all'uditore in capo dell'Esercito svizzero.

2 Mettono in sicurezza gli oggetti idonei a fungere da mezzi di prova in un procedimento.

13 RS **172.010.442**
14 RS **172.010.59**
15 RS **128.xxx**

Art. 34 Misure di protezione fisica
(art. 22 LSIn)

1 Previa consultazione dei servizi dell'Amministrazione federale e dell'esercito competenti per la sicurezza degli oggetti, il servizio specializzato della Confederazione per la sicurezza delle informazioni emana istruzioni generali e astratte applicabili a tutti i servizi di cui all'articolo 2 capoversi 1–3 concernenti le misure minime necessarie per la protezione fisica di informazioni e mezzi informatici.

2 In tale contesto tiene conto:

a. dell'intero ciclo di vita delle informazioni e dei mezzi informatici;

b. dei requisiti specifici per il posto di lavoro; e

c. delle strategie direttrici e dei schemi direttori dell'Amministrazione federale e dell'esercito.

Art. 35 Zone di sicurezza
(art. 23 e 85 LSIn)

1 Le unità amministrative possono istituire le seguenti zone di sicurezza:

a. zona di sicurezza 1: i locali e i settori in cui sono trattate frequentemente informazioni classificate «confidenziale» o sono impiegati mezzi informatici del livello di sicurezza «protezione elevata»;

b. zona di sicurezza 2: i locali e i settori in cui sono trattate frequentemente informazioni classificate «segreto» o sono impiegati mezzi informatici del livello di sicurezza «protezione molto elevata».

2 I locali e i settori secondo il capoverso 1 sono considerati come zona di sicurezza soltanto se il servizio competente per la sicurezza degli oggetti dell'Amministrazione federale o dell'esercito prima della messa in servizio e successivamente almeno ogni cinque anni conferma che i requisiti di sicurezza sono soddisfatti.

3 Dopo aver consultato i servizi competenti per la sicurezza degli oggetti dell'Amministrazione federale e dell'esercito, il servizio specializzato della Confederazione per la sicurezza delle informazioni emana istruzioni generali e astratte applicabili a tutti i servizi di cui all'articolo 2 capoversi 1–3 concernenti i requisiti di sicurezza per le zone di sicurezza e la loro istituzione.

Sezione 7: Organizzazione di sicurezza

Art. 36 Responsabili della sicurezza della Cancelleria federale e delle unità amministrative
(art. 7 cpv. 1 LSIn)

1 Il cancelliere della Confederazione, i segretari generali nonché i direttori delle unità amministrative dell'Amministrazione federale centrale e decentralizzata sono responsabili della sicurezza nel loro settore di competenza.

2 Possono delegare la responsabilità della sicurezza a un membro della direzione a condizione che questo disponga dei poteri necessari per predisporre, controllare e correggere misure.

3 I responsabili della sicurezza della Cancelleria federale e delle unità amministrative svolgono in particolare i seguenti compiti:

a. garantiscono lo sviluppo, l'esercizio, la verifica e il miglioramento continuo del SGSI nel loro settore di competenza ed emanano le direttive necessarie a tale scopo;

b. adottano tutte le decisioni che influiscono in misura determinante sulla sicurezza delle informazioni nel loro settore di competenza, in particolare per quanto concerne l'organizzazione, i processi, l'accettazione dei rischi e gli obiettivi di sicurezza;

c. decidono in merito alle misure necessarie, in particolare allo svolgimento di misure di formazione e di sensibilizzazione;

d. approvano il piano annuale di controllo e di audit e mettono a disposizione le risorse necessarie a tale scopo.

4 Il cancelliere della Confederazione, i segretari generali nonché i direttori delle unità amministrative dell'Amministrazione federale centrale e decentralizzata danno incarico ai loro incaricati della sicurezza delle informazioni secondo l'articolo 37 e provvedono affinché:

a. dispongano di competenze e di risorse adeguate; e

b. non vengano loro assegnati compiti che possono comportare un conflitto d'interessi con i compiti secondo l'articolo 37.

Art. 37 Incaricati della sicurezza delle informazioni delle unità amministrative
(art. 7 cpv. 1 LSIn)

1 Le unità amministrative designano un incaricato della sicurezza delle informazioni o diversi incaricati della sicurezza delle informazioni nonché il supplente o i supplenti.

2 Gli incaricati della sicurezza delle informazioni hanno in particolare i seguenti compiti:

a. su incarico del responsabile della sicurezza gestiscono il SGSI dell'unità amministrativa;

b. elaborano le necessarie basi decisionali a destinazione dei responsabili della sicurezza e propongono loro la decisione di misure;

c. fungono da organo centrale di contatto dell'unità amministrativa per questioni relative alla sicurezza delle informazioni e forniscono consulenza e sostegno alle persone e ai servizi competenti nell'adempimento dei loro compiti e doveri nel settore della sicurezza delle informazioni;

d. provvedono all'attuazione delle direttive in materia di sicurezza delle informazioni e all'applicazione della procedura di sicurezza di cui all'articolo 27;

e. vigilano sul registro delle basi legali, sull'inventario degli oggetti da proteggere e sul registro delle autorizzazioni eccezionali;

f. vigilano sulla pianificazione della formazione e della sensibilizzazione secondo l'articolo 11 e propongono al responsabile della sicurezza di svolgere misure supplementari di formazione e di sensibilizzazione;

g. fanno domanda per avviare la procedura di sicurezza relativa alle aziende di cui all'articolo 4 dell'ordinanza sulla procedura di sicurezza relativa alle aziende del …[16];

h. coordinano la notifica e la gestione di incidenti legati alla sicurezza e di lacune in materia di sicurezza nell'unità amministrativa nonché presso terzi incaricati;

i. redigono il piano annuale di controllo e di audit e lo presentano al responsabile della sicurezza per l'approvazione;

j. su incarico del responsabile della sicurezza possono controllare o far controllare la gestione delle informazioni in postazioni di lavoro aperte, condivise o non chiudibili a chiave e nei mezzi informatici dell'unità amministrativa;

k. informano il responsabile della sicurezza su base semestrale in merito allo stato della sicurezza delle informazioni.

Art. 38 Sicurezza delle informazioni nei servizi standard
(art. 7 cpv. 1 LSIn)

1 Il delegato TDT è competente per la garanzia della sicurezza delle informazioni nei servizi standard secondo l'articolo 17 capoverso 1 lettera e OTDI[17].

2 Designa un incaricato della sicurezza delle informazioni o diversi incaricati della sicurezza delle informazioni e il supplente o i supplenti.

3 L'incaricato della sicurezza delle informazioni si occupa dei compiti di cui all'articolo 37 capoverso 2 per i servizi standard e informa l'Amministrazione federale e l'esercito in merito ai rischi.

Art. 39 Responsabilità in materia di sicurezza dei dipartimenti
(art. 7 cpv. 1 e 81 LSIn)

1 I dipartimenti sono responsabili della gestione e della vigilanza sulla sicurezza delle informazioni nel loro settore di competenza.

2 In tale contesto si occupano in particolare dei compiti seguenti:

a. determinano la politica in materia di sicurezza delle informazioni e l'organizzazione in materia di sicurezza del dipartimento, compresa la direzione specialistica degli incaricati della sicurezza delle informazioni delle unità amministrative;

b. emanano le istruzioni necessarie e vigilano sull'attuazione;

c. vigilano sul SGSI delle unità amministrative e rilevano gli indicatori necessari a tale scopo;

16 RS **128.xxx**
17 RS **172.010.58**

d. stabiliscono ogni anno gli obiettivi in materia di sicurezza per le unità amministrative e verificano se sono stati raggiunti;

e. provvedono a una verifica basata sui rischi della sicurezza delle informazioni;

f. incaricano i loro incaricati della sicurezza delle informazioni secondo l'articolo 40 e provvedono affinché:

1. dispongano di competenze e di risorse adeguate,

2. non vengano loro assegnati compiti che possono comportare un conflitto d'interessi con i loro compiti di cui all'articolo 40.

3 Possono assumere compiti e competenze che la presente ordinanza attribuisce alle unità amministrative.

4 Possono stabilire requisiti di sicurezza per il loro settore di competenza che vanno oltre i requisiti minimi stabiliti dal servizio specializzato della Confederazione per la sicurezza delle informazioni o dall'unità amministrativa.

5 Se il capo del dipartimento non decide diversamente, è il segretario generale su suo incarico a essere responsabile della sicurezza nel dipartimento.

Art. 40 Incaricati della sicurezza delle informazioni dei dipartimenti
(art. 7 cpv. 1 e 81 LSIn)

In aggiunta ai compiti di cui all'articolo 81 capoverso 2 LSIn, gli incaricati della sicurezza delle informazioni dei dipartimenti hanno i seguenti compiti:

a. provvedono al coordinamento interdipartimentale della sicurezza delle informazioni;

b. elaborano le necessarie basi decisionali a destinazione dei responsabili della sicurezza e propongono loro la decisione di misure;

c. coordinano la notifica e la gestione di incidenti legati alla sicurezza e di lacune in materia di sicurezza che riguardano più unità amministrative;

d. rappresentano il dipartimento in organi specialistici;

e. vengono consultati in sede di nomina degli incaricati della sicurezza delle informazioni delle unità amministrative secondo l'articolo 37;

f. controllano periodicamente e in caso di cambiamento o di uscita di un membro del Consiglio federale o del cancelliere della Confederazione se i supporti di dati classificati «segreto» sono disponibili e completi;

g. autorizzano l'avvio di controlli di sicurezza relativi alle persone presso terzi (art. 8 cpv. 2 lett. b OCSP[18]);

h. informano ogni anno il responsabile della sicurezza del dipartimento in merito allo stato della sicurezza delle informazioni nel dipartimento.

18 RS **128.xxx**

Art. 41 Servizio specializzato della Confederazione per la sicurezza delle informazioni
(art. 7 cpv. 1 e 83 LSIn)

1 Il servizio specializzato della Confederazione per la sicurezza delle informazioni ha i seguenti compiti per l'Amministrazione federale e per l'esercito:

a. elabora strategie relative a temi rilevanti sotto il profilo della sicurezza;

b. può richiedere informazioni riguardo a progetti rilevanti sotto il profilo della sicurezza, prendere posizione al riguardo e richiedere modifiche;

c. partecipa alla formazione dell'organizzazione di sicurezza;

d. mette a disposizione modelli e strumenti ausiliari.

2 Per valutare e migliorare lo stato della sicurezza delle informazioni della Confederazione può cercare minacce tecniche o vulnerabilità nell'infrastruttura informatica dell'Amministrazione federale e dell'esercito o in Internet; può incaricare altri servizi dell'Amministrazione federale o dell'esercito nonché terzi di tale attività.

3 Per adempiere i compiti di cui al capoverso 1 nonché all'articolo 83 capoverso 1 LSIn consulta la Conferenza degli incaricati della sicurezza delle informazioni.

4 Nel contesto internazionale rappresenta la Svizzera in veste di autorità di sicurezza nazionale e svolge i seguenti compiti:

a. elabora i trattati internazionali di cui all'articolo 87 LSIn e vigila sulla loro attuazione;

b. assicura che gli incidenti legati alla sicurezza che riguardano informazioni classificate di Stati partner vengano chiariti in maniera adeguata;

c. può eseguire i controlli previsti dai trattati internazionali o commissionarli;

d. rappresenta la Svizzera in organi specializzati internazionali;

e. autorizza l'accoglienza di persone dall'estero che si recano in Svizzera per progetti classificati nonché l'invio di persone che si recano all'estero per progetti classificati;

f. rilascia le attestazioni nel contesto internazionale secondo l'articolo 30 OCSP[19].

5 Il servizio specializzato della Confederazione per la sicurezza delle informazioni è attribuito al *[dipartimento competente]*.

Sezione 8: Costi e valutazione

Art. 42 Costi

1 I costi per la sicurezza delle informazioni sostenuti a livello decentralizzato fanno parte dei costi dei progetti e di quelli di esercizio.

19 RS ...

2 Le unità amministrative assicurano che questi costi vengano considerati in maniera adeguata e riportati in sede di pianificazione.

3 Per il rilascio e il recapito delle attestazioni di sicurezza nel contesto internazionale secondo l'articolo 30 OCSP[20] a persone che non svolgono un'attività sensibile sotto il profilo della sicurezza il servizio specializzato della Confederazione per la sicurezza delle informazioni riscuote un emolumento pari a 100 franchi.

Art. 43 Valutazione
(art. 88 LSIn)

Sei anni dopo l'entrata in vigore della presente ordinanza e successivamente ogni dieci anni il servizio specializzato della Confederazione per la sicurezza delle informazioni richiede al Controllo federale delle finanze una valutazione della legislazione in materia di sicurezza delle informazioni in seno alla Confederazione.

Sezione 9: Trattamento di informazioni e di dati personali

Art. 44 In generale

1 Le organizzazioni di cui all'articolo 2 capoversi 1–3 nonché gli organi di sicurezza della Confederazione possono trattare le informazioni opportune per garantire la sicurezza delle informazioni, compresi i dati personali.

2 Possono scambiare tra loro informazioni, compresi dati personali, di cui al capoverso 1 nonché con organizzazioni nazionali, internazionali ed estere di diritto pubblico e privato se

a. non vengono violati gli obblighi del segreto legali o contrattuali; e

b. vengono rispettate le direttive della legislazione federale sulla protezione dei dati.

3 Se è necessario per gestire un incidente legato alla sicurezza o una lacuna in materia di sicurezza possono trattare o scambiare tra loro anche dati personali particolarmente degni di protezione concernenti l'identità o gli atti di persone che sono o potrebbero essere coinvolte nell'incidente o interessate dall'incidente.

Art. 45 Applicazione SGSI

1 Per la gestione della sicurezza delle informazioni le organizzazioni di cui all'articolo 2 capoversi 1–3 possono utilizzare un sistema d'informazione (applicazione SGSI).

2 Nell'applicazione SGSI possono trattare tutte le informazioni relative alla gestione della sicurezza delle informazioni secondo la presente ordinanza nonché i dati particolarmente degni di protezione di cui all'articolo 44 capoverso 3.

3 Possono collegare le loro applicazioni SGSI e scambiare tra loro informazioni rilevanti sotto il profilo della sicurezza delle informazioni tramite interfacce automatizzate.

20 RS **128.xxx**

Art. 46 Servizi di modulistica elettronica

[1] Il servizio specializzato della Confederazione per la sicurezza delle informazioni può gestire servizi di modulistica elettronica e collegarli con la sua applicazione SGSI per i seguenti scopi:

a. per la gestione dei viaggi secondo l'articolo 41 capoverso 4 lettera e;

b. per il rilascio e il recapito delle attestazioni di sicurezza nel contesto internazionale secondo l'art. 30 OCSP[21];

c. per il rilascio e il recapito delle attestazioni internazionali di sicurezza aziendale di cui all'articolo 66 LSIn.

[2] Con i servizi di modulistica di cui al capoverso 1 possono essere trattati dati personali secondo l'allegato 2. Questi dati possono essere conservati al massimo per 10 anni.

[3] Le organizzazioni di cui all'articolo 2 capoversi 1–3 possono gestire servizi di modulistica elettronica per notificare incidenti legati alla sicurezza e lacune in materia di sicurezza e collegarli con la loro applicazione SGSI.

[4] Con i servizi di modulistica di cui al capoverso 3 possono trattare dati personali, compresi dati personali particolarmente degni di protezione secondo l'articolo 44 capoverso 3 necessari per gestire incidenti legati alla sicurezza e lacune in materia di sicurezza.

[5] I dati di cui al capoverso 4 devono essere cancellati immediatamente dopo l'invio della notifica dal servizio di modulistica. Possono essere salvati temporaneamente per al massimo 24 ore prima dell'invio della notifica.

Sezione 10: Disposizioni finali

Art. 47 Abrogazione e modifica di altri atti normativi

[1] Sono abrogate le seguenti ordinanze:

a. l'ordinanza sui ciber-rischi del 27 maggio 2020[22];

b. l'ordinanza sulla protezione delle informazioni del 4 luglio 2007[23].

[2] La modifica di altri atti normativi è disciplinata nell'allegato 3.

Art. 48 Disposizioni transitorie

[1] Le direttive relative alla sicurezza informatica emanate dal Centro nazionale per la cibersicurezza e le deroghe da esso autorizzate prima dell'entrata in vigore della presente ordinanza rimangono applicabili per al massimo sei anni dopo l'entrata in vigore della presente ordinanza.

21 RS **128.xxx**
22 [RU **2020** 2107, **2020** 5871, **2021** 132]
23 [RU **2007** 3401, **2010** 3207, **2013** 1341, **2014** 3543, **2016** 1785, **2017** 7391, **2020** 6011]

2 Il servizio specializzato della Confederazione per la sicurezza delle informazioni decide in merito a modifiche di direttive e di deroghe autorizzate secondo il capoverso 1.

3 Le direttive relative alla protezione delle informazioni emanate dalla Conferenza dei segretari generali o dall'organo di coordinamento per la protezione delle informazioni in seno alla Confederazione prima dell'entrata in vigore della presente ordinanza rimangono applicabili per cinque anni al massimo dall'entrata in vigore della presente ordinanza.

4 Le unità amministrative e la Cancelleria federale devono creare il loro SGSI al massimo entro tre anni dall'entrata in vigore della presente ordinanza.

5 L'accreditamento in materia di sicurezza secondo l'articolo 23 non viene svolto per mezzi informatici che:

a. sono in uso prima dell'entrata in vigore della presente ordinanza;

b. sono in fase di sviluppo al momento dell'entrata in vigore della presente ordinanza, qualora comportasse un onere sproporzionato.

Art. 49 Entrata in vigore

La presente ordinanza entra in vigore il … 2023.

… In nome del Consiglio federale svizzero:

Il presidente della Confederazione, …
Il cancelliere della Confederazione, Walter Thurnherr

Allegato 1
(art. 2 cpv. 2 e 3)

Unità amministrative dell'Amministrazione federale decentralizzata alle quali si applicano l'ordinanza sulla sicurezza delle informazioni

1. Le unità amministrative che accedono a mezzi informatici dei fornitori interni di prestazioni TIC di cui all'articolo 9 OTDI[24], se questi sono assegnati al livello di sicurezza «protezione elevata» o «protezione molto elevata» secondo l'articolo 28:

a. …

b. …

c. …

2. Le unità amministrative che impiegano mezzi informatici assegnati al livello di sicurezza «protezione elevata» o «protezione molto elevata» secondo l'articolo 28:

a. …

b. …

c. …

3. Le unità amministrative che non rientrano tra quelle di cui all'articolo 2 capoverso 2 lettera a o b, ma che trattano informazioni classificate della Confederazione:

a. …

b. …

c. …

4. Altre unità amministrative (cfr. art. 2 cpv. 3):

a. …

b. …

c. …

24 RS **172.010.58**

Allegato 2
(art. 46 cpv. 2)

Trattamento dei dati in servizi di modulistica elettronica secondo l'articolo 46

Nei servizi di modulistica secondo l'articolo 46 possono essere trattati i seguenti dati personali:

1. Servizio di modulistica secondo l'articolo 46 capoverso 1 lettera a OSIn
   a. Dati personali:
      1. Cognome e nome*
      2. Numero AVS
      3. Appellativo, titolo e rango*
      4. Data di nascita*
      5. Luogo di origine e luogo di nascita*
      6. Cittadinanza/e*
      7. Numero della carta d'identità e del passaporto nonché luogo di rilascio e validità*
   b. Indicazioni relative alla funzione professionale o militare della persona:
      1. Funzione nell'organizzazione o nell'esercito*
      2. Indirizzo di lavoro, indirizzo e-mail, numero di telefono e ulteriori dati di contatto, in particolare elettronici
      3. Decisione positiva in merito al controllo di sicurezza relativo alle persone, livello di controllo e validità*
   c. Indicazioni relative all'organizzazione richiedente:
      1. Denominazione, indirizzo e dati di contatto dell'organizzazione*
      2. Cognome e nome della persona di riferimento
      3. Funzione della persona di riferimento nell'organizzazione o nell'esercito
      4. Indirizzo di lavoro, indirizzo e-mail, numero di telefono e dati di contatto elettronici della persona di riferimento
   d. Indicazioni relative alla visita:
      1. Nome, indirizzo, indirizzo e-mail e dati di contatto dell'organizzazione estera*
      2. Motivo della visita*
      3. Livello di sicurezza della visita*
      4. Durata della visita*
      5. Punti di attraversamento del confine*
      6. Mezzi di trasporto*
      7. Materiali trasportati, compresi armi, munizioni ed esplosivi, veicoli e altri equipaggiamenti*

Le indicazioni seguite da un (*) vengono comunicate all'autorità di sicurezza estera.

2. Servizio di modulistica secondo l'articolo 46 capoverso 1 lettera b OSIn
   a. Dati personali:
      1. Cognome e nome
      2. Numero AVS
      3. Appellativo, titolo e rango
      4. Data di nascita
      5. Luogo di origine e luogo di nascita
      6. Cittadinanza/e
      7. Numero della carta d'identità e del passaporto nonché luogo di rilascio e validità
   b. Indicazioni relative alla funzione professionale o militare della persona:
      1. Funzione nell'organizzazione o nell'esercito
      2. Indirizzo di lavoro, indirizzo e-mail, numero di telefono e ulteriori dati di contatto, in particolare elettronici
      3. Decisione positiva in merito al controllo di sicurezza relativo alle persone, livello di controllo e validità
   c. Indicazioni relative all'organizzazione richiedente:
      1. Denominazione, indirizzo, indirizzo e-mail e dati di contatto dell'organizzazione
      2. Cognome e nome della persona di riferimento
      3. Funzione della persona di riferimento nell'organizzazione o nell'esercito
      4. Indirizzo di lavoro, indirizzo e-mail e ulteriori dati di contatto, in particolare elettronici, della persona di riferimento
      5. Motivo dell'allestimento dell'attestazione.

3. Servizio di modulistica secondo l'articolo 46 capoverso 1 lettera c OSIn
   a. Indicazioni concernenti l'azienda:
      1. Denominazione completa*
      2. Forma giuridica*
      3. Numero d'identificazione delle imprese
      4. Indirizzo, indirizzo e-mail e ulteriori dati di contatto, in particolare elettronici*
      5. Sede*
      6. Cognome e nome della persona di riferimento*
      7. Funzione della persona di riferimento nell'azienda
      8. Indirizzo di lavoro, indirizzo e-mail e ulteriori dati di contatto, in particolare elettronici, della persona di riferimento
   b. Indicazioni relative alla dichiarazione di sicurezza aziendale:

1. Data del rilascio e validità*
2. Campo di applicazione e condizioni*
3. Livello di classificazione o di sicurezza più alto ammesso*

Le indicazioni seguite da un (*) vengono comunicate all'autorità di sicurezza estera.

4. Servizio di modulistica secondo l'articolo 46 capoversi 3–5 OSIn

a. Indicazioni relative alla persona che presenta la notifica:
   1. Cognome e nome
   2. Indirizzo, indirizzo e-mail, numero di telefono e ulteriori dati di contatto, in particolare elettronici
   3. Funzione nell'organizzazione o nell'esercito
b. Indicazioni relative all'evento dannoso e al calcolo del danno:
c. Registrazioni fotografiche, audio o video dell'incidente o della lacuna in materia di sicurezza
d. Documenti o file correlati all'incidente o alla lacuna in materia di sicurezza
e. Indicazioni relative a persone eventualmente coinvolte nell'incidente
f. Primi accertamenti effettuati da periti, comprese le misure già adottate

Allegato 3
(art. 47 cpv. 2)

Modifica di altri atti normativi

I seguenti atti normativi vengono modificati come segue:

1. Ordinanza del 25 novembre 2020[25] sul coordinamento della trasformazione digitale e la governance delle TIC in seno all'Amministrazione federale

Art. 2 cpv. 2, frase introduttiva

2 Fatte salve disposizioni di diverso tenore previste dal diritto federale in materia di organizzazione, possono impegnarsi mediante un accordo con il settore Trasformazione digitale e governance delle TIC della Cancelleria federale (settore TDT della CaF) a rispettare la presente ordinanza, l'ordinanza sulla sicurezza delle informazioni del […][26] e l'ordinanza GEVER del 3 aprile 2019[27] nonché le direttive fondate sulle stesse:

2. Ordinanza del 7 marzo 2003 sull'organizzazione del Dipartimento federale della difesa, della protezione della popolazione e dello sport[28]

Art. 3 cpv. 2

2 Il DDPS emana prescrizioni per garantire l'equipaggiamento dell'esercito.

Art. 6 lett. b

Abrogata

3. Ordinanza del 24 giugno 2009[29] sui contatti militari internazionali

Art. 4 lett. c

I servizi seguenti possono, nel loro settore di compiti, allacciare formalmente contatti militari internazionali senza l'autorizzazione del Protocollo militare:

c. il servizio specializzato della Confederazione per la sicurezza delle informazioni;

Art. 5 cpv. 1

25 RS **172.010.58**
26 RS …
27 RS **172.010.441**
28 RS **172.214.1**
29 RS **510.215**

[1] La consegna di informazioni classificate a persone e organi stranieri nonché l'accesso da parte di visitatori stranieri a informazioni militari classificate, a materiale classificato o a impianti militari in Svizzera si fondano sulle corrispondenti prescrizioni in materia di protezione delle informazioni, segnatamente:

a. il trattato internazionale secondo l'articolo 87 della legge sulla sicurezza delle informazioni del 20 dicembre 2020[30] applicabile nel caso concreto;

b. l'ordinanza del …[31] sui controlli di sicurezza relativi alle persone;

c. l'ordinanza del …[32] sulla sicurezza delle informazioni;

d. l'ordinanza del…[33] sulla procedura di sicurezza relativa alle aziende.

30 RS **128**
31 RS **...**
32 RS **...**
33 RS **...**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ordinanza sui sistemi di gestione delle identità e sui servizi di elenchi della Confederazione (OIAM)

Modifica del … Disegno del 25 luglio 2022

Il Consiglio federale svizzero
ordina:

I

L'ordinanza del 19 ottobre 2016[1] sui sistemi di gestione delle identità e sui servizi di elenchi della Confederazione è modificata come segue:

Ingresso

visti gli articoli 26 e 84 capoverso 1 della legge del 18 dicembre 2020[2] sulla sicurezza delle informazioni (LSIn);
visto l'articolo 27 capoversi 5 e 6 della legge del 24 marzo 2000[3] sul personale federale;
visto l'articolo 186 della legge federale del 3 ottobre 2008[4] sui sistemi d'informazione militari,

Art. 2 Campo d'applicazione

La presente ordinanza si applica:

a. alle unità amministrative dell'Amministrazione federale centrale di cui all'articolo 7 dell'ordinanza del 25 novembre 1998[5] sull'organizzazione del Governo e dell'Amministrazione (OLOGA);

b. alle unità amministrative dell'Amministrazione federale decentralizzata di cui all'articolo 7*a* OLOGA, sempre che abbiano accesso ai sistemi informatici dell'Amministrazione federale centrale.

1 RS **172.010.59**
2 RS **126**
3 RS **172.220.1**
4 RS **510.91**
5 RS **172.010.1**

Art. 3 cpv. 1

1 Lo scopo di un sistema IAM consiste nell'amministrare in modo raggruppato i dati sull'identità e sui diritti di persone, macchine e sistemi per metterli a disposizione di sistemi a valle e di altri sistemi IAM.

Art. 5 Sistemi IAM

1 Gli organi federali responsabili dei sistemi IAM sono:

a. il settore Trasformazione digitale e governance delle TIC della Cancelleria federale (settore TDT della CaF) per tutti i sistemi IAM offerti come servizi standard o esplicitamente attribuiti al settore TDT della CaF;

b. la Direzione delle risorse del Dipartimento federale degli affari esteri (DFAE) per il sistema IAM gestito dall'unità Informatica DFAE;

c. il settore TDT della Cancelleria federale per il sistema IAM dei processi di supporto, compresi i collegamenti cloud;

d. la Segreteria generale del Dipartimento federale della difesa, della protezione della popolazione e dello sport per il sistema IAM gestito dalla Base d'aiuto alla condotta (BAC) del DDPS;

e. la Segreteria generale del Dipartimento federale dell'economia, della formazione e della ricerca (DEFR) per il sistema IAM gestito presso il Centro servizi informatici DEFR (CSIeco);

f. l'Ufficio federale delle strade per il suo sistema IAM destinato all'esercizio degli equipaggiamenti di esercizio e sicurezza delle strade nazionali.

2Gli organi federali di cui al capoverso 1 provvedono affinché la liceità del trattamento dei dati personali nei sistemi IAM dei quali sono responsabili sia verificata almeno ogni quattro anni da un servizio esterno.

3 Nella misura in cui la presente ordinanza si applica alle organizzazioni assoggettate di cui all'articolo 2 capoverso 1 lettere a e c–e LSIn secondo l'articolo 84 capoverso 3 LSIn, tali organizzazioni stabiliscono esse stesse quali sono gli organi federali responsabili nel loro settore.

4 Il servizio tecnico competente rimane responsabile del sistema a valle, in particolare dell'accesso ad esso.

Art. 11 cpv. 2 e 3

2 In questo sistema non può essere eseguita alcuna profilazione.

3 In assenza di una base legale in questi sistemi non possono essere trattati dati personali degni di particolare protezione, eccettuati i dati biometrici secondo l'articolo 20 capoverso 2 LSIn.

Art. 13 cpv. 4

4 I dati possono essere messi a disposizione automaticamente di altri sistemi d'informazione interni alla Confederazione per essere ripresi e armonizzati a condizione che il sistema interessato:

a. sia dotato di una base legale che prevede il trattamento dei dati da mettere a disposizione e di un regolamento per il trattamento secondo l'articolo 21dell'ordinanza del 14 giugno 1993 relativa alla legge sulla protezione dei dati (OLPD); e

Art. 14 cpv. 2

2 Sono fatte salve le disposizioni sulla distruzione dei dati biometrici secondo l'articolo 20 capoverso 2 LSIn.

Titolo prima dell'art. 18

Sezione 6: Misure di protezione dei sistemi IAM e dei servizi di elenchi

Art. 18 cpv. 1 e 2

1 I gestori interni ed esterni di componenti di un sistema IAM e di un servizio di elenchi devono disporre di direttive scritte sulla sicurezza delle informazioni e sulla gestione dei rischi. In particolare, ogni organo responsabile di un sistema o di un servizio di elenchi secondo la presente ordinanza emana un regolamento per il trattamento secondo l'articolo 21 OLPD.

2 I sistemi IAM e i servizi di elenchi che non sono gestiti da servizi secondo l'articolo 2 o su loro mandato, possono essere collegati a sistemi IAM o servizi di elenchi interni alla Confederazione soltanto se soddisfano i requisiti minimi predefiniti in materia di sicurezza delle informazioni.

Art. 20 Sistema globale IAM

I sistemi IAM dell'Amministrazione federale possono essere collegati tra loro e con i sistemi IAM esterni di cui all'articolo 21 al fine di costituire un sistema globale.

Art. 21 Condizioni per il collegamento di sistemi IAM esterni

I seguenti sistemi esterni IAM possono essere collegati ai sistemi IAM della Confederazione per consentire l'accesso delle persone ivi registrate alle risorse della Confederazione, sempre che siano soddisfatte le condizioni e le procedure secondo gli articoli 22 e 23 e i loro gestori s'impegnino a rispettare la presente ordinanza e le direttive emanate in virtù della stessa:

a. sistemi IAM dei Servizi del Parlamento;

b. sistemi IAM dell'esercito;

c. sistemi IAM comprendenti collaboratori cantonali e comunali secondo l'articolo 9 lettera a;

d. sistemi IAM riconosciuti dal settore TDT della CaF previsti per la rete per le identificazioni nell'ambito del Governo elettronico;

e. sistemi IAM esteri o reti estere per le identificazioni il cui collegamento è previsto in un trattato internazionale; oppure

f. registri degli attributi che mettono a disposizione per l'utilizzo dati relativi alle funzioni professionali conformemente alla lettera b dell'allegato.

II

L'allegato è sostituito dalla versione qui annessa.

III

La presente ordinanza entra in vigore il … 2023.

In nome del Consiglio federale svizzero:

…

Il presidente della Confederazione, …
Il cancelliere della Confederazione, Walter Thurnherr

Allegato
(art. 11 e 13 cpv. 1 e 2)

Categorie di dati

Osservazione preliminare: per il significato degli asterischi (*) si veda l'articolo 11 capoverso 2.

	Servizi di elenchi e sistemi IAM con persone secondo gli art. 8 e 9 lett. a	Sistemi IAM con persone secondo l'art. 9 lett. b
a. Dati personali		
1. Cognome*	x	x
2. Nomi *	x	x
3. Data di nascita	x	x
4. Sesso	x	x
5. Appellativo*	x	x
6. Titolo*	x	x
7. Iniziali*	x	x
8. Identificativi personali locali	x	x
9. Denominazione della professione*	x	x
10. Lingua per la corrispondenza*	x	x
11. Particolari caratteristiche biometriche personali, segnatamente scansione dell'iride, retina, scansione delle vene, impronte digitali, impronta della mano, caratteristiche della forma del viso e profilo vocale	x	
12. Numero AVS	x	x
b. Dati relativi al rapporto con il datore di lavoro/mandante		
1. Rapporto di lavoro (interno / esterno)*	x	
2. Informazioni concernenti l'organizzazione e i posti in organico *	x	x
3. Futura attribuzione a un'unità organizzativa	x	
4. Categoria di personale	x	
5. Numero personale (anche cantonale)	x	
6. Funzione*	x	
7. Designazione del posto *	x	
8. Identificazione del sistema d'informazione concernente il personale (fonte)	x	

	Servizi di elenchi e sistemi IAM con persone secondo gli art. 8 e 9 lett. a	Sistemi IAM con persone secondo l'art. 9 lett. b
9. Data di entrata / data di partenza	x	
10. Numero del documento d'identità e/o del badge	x	x
c. Dati di contatto		
1. Luogo di lavoro e indirizzo postale professionale	x	x
2. Numero dell'ufficio*	x	
3. Elementi dell'indirizzo professionale* come indirizzo di posta elettronica*, numeri di telefono*, numero di fax*, indirizzo VOIP*	x	x
4. Elementi dell'indirizzo esterno* (per collaboratori e incaricati*) o elementi dell'indirizzo privato	x	x
d. Dati sulle funzioni professionali		
1. Iscrizioni registrate in albi professionali ufficiali (medico, pubblico ufficiale rogatore, avvocato ecc.)	x	x
2. Funzioni secondo il registro di commercio e altri registri di rappresentanza	x	x
e. Dati tecnici		
1. Dispositivi, collegamenti, sistemi, applicazioni ecc. attribuiti	x	x
2. Elementi dell'indirizzo, numeri d'identificazione ecc.	x	
3. Linguaggio di sistema dei dispositivi, dei collegamenti ecc.	x	x
4. Chiave pubblica dei certificati digitali*	x	x
5. Gruppi di autorizzazioni	x	x
6. Nomi per la registrazione nei sistemi IT	x	x
7. Password	x	x
8. Ultimo login	x	x
9. Tentativi di login falliti	x	x
10. Status (attivo/passivo)	x	x
f. Dati sui controlli di sicurezza relativi alle persone, se l'esito di quest'ultimi è una dichiarazione di sicurezza senza riserve o se l'autorità decisionale ha emanato una decisione positiva		
1. Livello di controllo	x	
2. Durata di validità della dichiarazione di sicurezza	x	

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ordinanza sui controlli di sicurezza relativi alle persone (OCSP)

del … Avamprogetto del 25 luglio 2022

Il Consiglio federale svizzero,

visti gli articoli 48, 83 capoverso 3, 84 capoverso 1 e 86 capoverso 4 della legge del 18 dicembre 2020[1] sulla sicurezza delle informazioni (LSIn);
visto l'articolo 41*b* capoverso 5 della legge federale del 16 dicembre 2005[2] sugli stranieri e la loro integrazione (LStrI);
visto l'articolo 119 della legge del 26 giugno 1998[3] sull'asilo (LAsi);
visto l'articolo 6*a* capoverso 5 della legge del 22 giugno 2001[4] sui documenti d'identità (LDI);
visto l'articolo 37 capoverso 1 della legge del 24 marzo 2000[5] sul personale federale (LPers);
visti gli articoli 14 capoverso 2 e 150 capoverso 1 della legge militare del 3 febbraio 1995[6] (LM);
visto l'articolo 24 capoverso 4 della legge federale del 21 marzo 2003[7] sull'energia nucleare (LENu);
visto l'articolo 20*a* capoverso 2 della legge del 23 marzo 2007[8] sull'approvvigionamento elettrico (LAEl),

ordina:

Sezione 1: Disposizioni generali

Art. 1 Oggetto

(art. 2 cpv. 3 e 4, 28, 30, 31 e 48 LSIn)

1 La presente ordinanza disciplina le seguenti procedure:

a. i controlli di sicurezza relativi alle persone (CSP) secondo la LSIn;

1 RS **128**
2 RS **142.20**
3 RS **142.31**
4 RS **143.1**
5 RS **172.220.1**
6 RS **510.10**
7 RS **732.1**
8 RS **734.7**

b. i controlli di sicurezza secondo gli articoli 41*b* capoverso 2 LStrI e 6*a* capoverso 2 LDI;

c. le verifiche dell'affidabilità secondo gli articoli 29*a* LAsi, 20*b* LPers, 14 LM e 20*a* LAEl;

d. i controlli di sicurezza relativi alle persone secondo gli articoli 23 capoverso 2 lettera d e 103 capoverso 3 lettera d LM;

e. le valutazioni del potenziale di pericolo o di abuso secondo l'articolo 113 capoverso 4 lettera d LM;

f. i controlli di affidabilità secondo l'articolo 24 LENu.

2 Disciplina inoltre:

a. l'organizzazione dei servizi specializzati (servizi specializzati CSP) competenti per l'esecuzione dei controlli di sicurezza relativi alle persone;

b. l'attestazione di sicurezza per persone che operano nel contesto internazionale;

c. la responsabilità in materia di protezione dei dati in relazione con il sistema d'informazione di cui all'articolo 45 LSIn nonché la sicurezza dei dati;

d. il controllo periodico del trattamento dei dati personali nel quadro dei controlli di sicurezza relativi alle persone da parte di un organo esterno.

3 Stabilisce nell'ambito di competenza del Consiglio federale:

a. le funzioni che richiedono l'esercizio di un'attività di cui al capoverso 1;

b. l'assegnazione di attività sensibili sotto il profilo della sicurezza ai livelli di controllo;

c. i servizi promotori e i servizi decisori competenti.

Art. 2 Campo d'applicazione

La presente ordinanza si applica alle autorità e organizzazioni assoggettate secondo l'articolo 2 LSIn, fatti salvi l'articolo 84 capoverso 3 LSIn e l'articolo 2 capoversi 2–5 dell'ordinanza del …[9] sulla sicurezza delle informazioni.

Sezione 2: Elenchi delle funzioni

Art. 3 Attribuzione
(art. 28 cpv. 1 LSIn e art. 24 cpv. 1 LENu)

1 Per l'Amministrazione federale valgono i seguenti elenchi delle funzioni:

a. per i controlli di sicurezza relativi alle persone secondo la LSIn: l'elenco delle funzioni di cui all'allegato 1;

9 RS **128.xxx**

b. per le verifiche dell'affidabilità secondo la LAsi: l'elenco delle funzioni di cui all'allegato 2;

c. per le verifiche dell'affidabilità secondo la LPers: l'elenco delle funzioni di cui all'allegato 3.

2 Per l'esercito valgono i seguenti elenchi delle funzioni:

a. per i controlli di sicurezza relativi alle persone secondo la LSIn: l'elenco delle funzioni di cui all'allegato 4;

b. per le verifiche dell'affidabilità secondo l'articolo 14 LM: l'elenco delle funzioni di cui all'allegato 5.

3 Per le funzioni secondo l'articolo 20*a* capoverso 1 LAEl vale l'elenco delle funzioni secondo l'allegato 6.

4 I titolari di una licenza di costruzione o d'esercizio e i destinatari di una decisione di disattivazione per impianti nucleari tengono un elenco delle funzioni che richiedono un controllo di affidabilità secondo l'articolo 24 LENu. L'Ispettorato federale della sicurezza nucleare (IFSN) fissa sotto forma di direttive i requisiti per questi elenchi e il loro aggiornamento.

Art. 4 Modifica

Su richiesta dei dipartimenti e della Cancelleria federale, il DDPS può completare o modificare gli elenchi delle funzioni di cui agli allegati 1–6. A tale scopo consulta preliminarmente il servizio specializzato della Confederazione per la sicurezza delle informazioni.

Art. 5 Pubblicazione, conservazione e comunicazione

1 Gli allegati 1, 4 e 6 non vengono pubblicati nella Raccolta ufficiale conformemente all'articolo 6 della legge del 18 giugno 2004[10] sulle pubblicazioni ufficiali.

2 Il DDPS conserva gli elenchi delle funzioni di cui agli allegati 1, 4 e 6 e li comunica ai servizi e alle persone che svolgono compiti secondo la presente ordinanza.

Art. 6 Verifica dell'aggiornamento
(art. 28 cpv. 2 LSIn)

1 I dipartimenti e la Cancelleria federale verificano l'aggiornamento degli elenchi delle funzioni nel loro ambito di competenza:

a. almeno ogni 4 anni;

b. in caso di riorganizzazioni oppure di assunzione o di trasferimento di compiti.

2 Redigono rapporti in tal merito per il DDPS e se necessario presentano proposte di modifica secondo l'articolo 4.

10 RS **170.512**

Sezione 3: Controlli senza elenchi delle funzioni

Art. 7 Controllo straordinario

Su domanda del dipartimento o della Cancelleria federale, il DDPS decide nel singolo caso se una persona tenuta a esercitare una funzione non ancora contenuta in un elenco delle funzioni di cui agli allegati 1–6 debba essere sottoposta al controllo. A tale scopo consulta preliminarmente il servizio specializzato della Confederazione per la sicurezza delle informazioni.

Art. 8 Controlli presso gli impiegati cantonali e terzi
(art. 29 cpv. 1 lett. b e c nonché cpv. 3 LSIn e art. 24 cpv. 1 LENu)

1 Il DDPS decide su domanda del Cantone, per quali funzioni degli impiegati cantonali viene eseguito un controllo di sicurezza relativo alle persone secondo l'articolo 29 capoverso 1 lettera b LSIn. A tale scopo consulta preliminarmente il servizio specializzato della Confederazione per la sicurezza delle informazioni.

2 Se nel caso di terzi che adempiono un mandato sensibile sotto il profilo della sicurezza per l'Amministrazione federale secondo l'articolo 49 LSIn occorre eseguire un controllo di sicurezza relativo alle persone, la decisione spetta:

a. nel quadro della procedura di sicurezza relativa alle aziende: al servizio specializzato per la sicurezza aziendale;

b. in tutti gli altri casi: all'incaricato della sicurezza delle informazioni del dipartimento o della Cancelleria federale.

Art. 9 Controllo di affidabilità straordinario da parte dell'IFSN

L'IFSN decide in merito all'affidabilità di persone che hanno accesso soltanto per un breve periodo a informazioni classificate in materia di sistemi rilevanti per la sicurezza esterna o interna di impianti nucleari o di materiale nucleare. A tale riguardo può rinunciare al controllo di affidabilità di cui all'articolo 24 capoverso 1 LENu e basarsi invece su informazioni ottenute in particolare dai seguenti organi:

a. un'azienda svizzera o estera per conto della quale la persona da controllare era o è attiva;

b. una camera di commercio svizzera o estera;

c. un'autorità estera del Paese da cui proviene la persona da controllare.

Sezione 4: Livelli di controllo

Art. 10 Controlli di sicurezza relativi alle persone secondo la LSIn
(art. 30 LSIn)

1 Sono attribuite al livello di controllo di sicurezza di base le seguenti attività sensibili sotto il profilo della sicurezza ai sensi della LSIn:

a. il trattamento di informazioni classificate «confidenziale»;

b. l'amministrazione, l'esercizio, la manutenzione e la verifica di mezzi informatici del livello di sicurezza «protezione elevata»;

c. 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;

d. le attività che devono essere sottoposte a un controllo di questo livello di controllo in virtù di un trattato internazionale.

2 Sono attribuite al livello di controllo di sicurezza ampliato le seguenti attività sensibili sotto il profilo della sicurezza ai sensi della LSIn:

a. il trattamento di informazioni classificate «segreto»;

b. l'amministrazione, l'esercizio, la manutenzione e la verifica di mezzi informatici del livello di sicurezza «protezione molto elevata»;

c. attività sensibili sotto il profilo della sicurezza esercitate da impiegati della Confederazione o da collaboratori esterni:
   1. presso il Servizio delle attività informative della Confederazione (SIC),
   2. presso il Servizio informazioni militare (SIM),
   3. presso il Centro operazioni elettroniche della Base d'aiuto alla condotta (COE),
   4. presso l'Autorità di vigilanza indipendente sulle attività informative (AVI-AIn);

d. attività sensibili sotto il profilo della sicurezza di collaboratori delle autorità d'esecuzione cantonali secondo l'articolo 9 della legge federale del 25 settembre 2015[11] sulle attività informative (LAIn);

e. attività che devono essere sottoposte a un controllo di questo livello di controllo in virtù di un trattato internazionale.

Art. 11 Verifica dell'affidabilità secondo la LPers

1 Sono attribuite a un controllo di sicurezza di base secondo l'articolo 20*b* LPers le seguenti attività:

a. attività di sovranità nazionale degli impiegati della Confederazione che sono in servizio all'estero e del personale del Dipartimento federale degli affari esteri (DFAE) soggetto al regime dell'obbligo di trasferimento;

b. attività secondo l'articolo 20*b* capoverso 1 lettera b LPers, dalla cui esecuzione infedele può derivare un danno da 50 a 500 milioni di franchi svizzeri;

c. attività nell'ambito di compiti di perseguimento penale o di polizia:
   1. in relazione ai mezzi e ai metodi operativi utilizzati per combattere i crimini o i delitti,
   2. in relazione all'identità di persone esposte,

11 RS **121**

3. del personale dell'Ufficio federale di polizia (fedpol) e dell'Ufficio federale di giustizia (UFG);

d. attività esercitate da persone direttamente subordinate a un capo di Dipartimento o al cancelliere della Confederazione oppure appartenenti al loro stato maggiore ristretto.

2 Sono attribuite a un controllo di sicurezza ampliato secondo l'articolo 20*b* LPers le seguenti attività:

a. attività di funzioni per le quali, secondo l'articolo 2 capoverso 1 dell'ordinanza del 3 luglio 2001[12] sul personale federale (OPers), il Consiglio federale è competente per costituire, modificare e risolvere il rapporto di lavoro;

b. attività nel quadro di rapporti di lavoro per le quali, secondo l'articolo 2 capoverso 1bis OPers, il capo di Dipartimento o il cancelliere della Confederazione è competente per costituire, modificare e risolvere il rapporto di lavoro;

c. attività dei responsabili di unità organizzative decentralizzate secondo l'articolo 2 capoverso 1 lettera e LPers;

d. attività secondo l'articolo 20*b* capoverso 1 lettera b LPers, dalla cui esecuzione infedele può derivare un danno di oltre 500 milioni di franchi svizzeri;

e. attività degli impiegati dei servizi specializzati CSP.

Art. 12 Controlli secondo la LM

1 Sono attribuiti a un controllo di sicurezza di base le seguenti attività e i seguenti controlli secondo la LM:

a. attività in uniforme all'estero secondo l'articolo 14 capoverso 1 lettera a LM, che vengono esercitate in rappresentanza sovrana della Svizzera oppure nell'ambito della diplomazia militare;

b. attività secondo l'articolo 14 capoverso 1 lettera b LM, dalla cui esecuzione infedele può derivare un danno finanziario da 50 a 500 milioni di franchi svizzeri;

c. controlli di cui all'articolo 23 capoverso 2 lettera d LM;

2 Un controllo di sicurezza relativo alle persone secondo l'articolo 103 LM per gli aspiranti è richiesto soltanto se:

1. sussiste un motivo di controllo secondo l'articolo 10 o il capoverso 1; oppure

2. è scaduto il termine minimo per la ripetizione secondo l'articolo 43 capoverso 1 LSIn.

12 RS **172.220.111.3**

Art. 13 Controlli di affidabilità secondo la LENu

1 Sono attribuiti a un controllo di sicurezza di base i controlli di affidabilità secondo l'articolo 24 capoverso 1 LENu delle seguenti persone:

a. persone impiegate presso il titolare di una licenza di costruzione o d'esercizio oppure presso il destinatario di una decisione di disattivazione per impianti nucleari e che hanno accesso a informazioni classificate «confidenziale» in materia di impianti nucleari e di materiale nucleare;

b. persone che hanno accesso per un lungo periodo a informazioni classificate in materia di sistemi rilevanti per la sicurezza esterna o interna di impianti nucleari e di materiale nucleare;

c. persone che operano nel settore della sicurezza esterna di impianti nucleari, segnatamente il personale di guardia.

2 Sono attribuiti a un controllo di sicurezza ampliato i controlli di affidabilità di persone impiegate presso il titolare di una licenza di costruzione o d'esercizio oppure presso il destinatario di una decisione di disattivazione per impianti nucleari e che hanno accesso a informazioni classificate «segreto» in materia di impianti nucleari e di materiale nucleare.

Art. 14 Verifiche dell'affidabilità secondo la LAEl

1 Sono attribuite a un controllo di sicurezza di base le attività per la società nazionale di rete secondo l'articolo 18 LAEl, per il cui adempimento è necessario l'accesso a informazioni critiche relative alla sicurezza d'approvvigionamento, ad applicazioni critiche o a infrastrutture critiche.

2 Sono attribuite a un controllo di sicurezza ampliato le attività per la società nazionale di rete per il cui adempimento è necessario l'accesso a informazioni estremamente critiche relative alla sicurezza dell'approvvigionamento, ad applicazioni estremamente critiche o a infrastrutture estremamente critiche.

Sezione 5: Esecuzione

Art. 15 Servizi promotori e servizi decisori
(art. 31 cpv. 1 LSIn)

1 I dipartimenti e la Cancelleria federale stabiliscono nel loro ambito di competenza i servizi promotori e i servizi decisori e li comunicano ai servizi specializzati CSP.

2 Se è responsabile della nomina o dell'attribuzione della carica o della funzione, il Consiglio federale è il servizio decisore.

3 Per i controlli di affidabilità secondo l'articolo 24 capoverso 1 LENu valgono le seguenti competenze:

a. servizi promotori: i titolari di licenze di costruzione o d'esercizio oppure i destinatari di decisioni di disattivazione per impianti nucleari;

b. servizio decisore: l'IFSN.

4 Per verifiche dell'affidabilità secondo l'articolo 20*a* LAEl la società nazionale di rete è il servizio promotore e decisore.

5 Le autorità assoggettate e i Cantoni comunicano ai servizi specializzati CSP quali servizi nel loro ambito di competenza sono i servizi promotori e decisori.

Art. 16 Servizi specializzati CSP
(art. 31 cpv. 2 LSIn)

1 I servizi specializzati CSP sono:

a. il servizio specializzato CSP della Cancelleria federale (servizio specializzato CSP CaF);

b. il servizio specializzato CSP del Dipartimento federale della difesa, della protezione della popolazione e dello sport (servizio specializzato CSP DDPS).

2 Il servizio specializzato CSP CaF è responsabile del controllo di persone che esercitano una delle seguenti funzioni:

a. funzioni per le quali, secondo l'articolo 2 capoverso 1 OPers[13], il Consiglio federale è competente per costituire, modificare e risolvere il rapporto di lavoro, ad eccezione di funzioni nella Cancelleria federale;

b. funzioni nel quadro di rapporti di lavoro per i quali, secondo l'articolo 2 capoverso 1bis OPers, il capo di Dipartimento o il cancelliere della Confederazione è competente per costituire, modificare e risolvere il relativo rapporto di lavoro;

c. funzioni all'interno del servizio specializzato CSP DDPS

d. funzioni all'interno del DDPS che comprendono compiti di condotta nei confronti del servizio specializzato CSP DDPS.

3 Il servizio specializzato CSP DDPS è responsabile di tutti gli altri controlli.

Art. 17 Verifica delle condizioni per il controllo
(art. 31 cpv. 2 LSIn)

1 Dopo l'avvio di un controllo, i servizi specializzati CSP verificano se:

a. la relativa funzione è contenuta nell'elenco delle funzioni;

b. il controllo è stato avviato dal rispettivo servizio competente;

c. la persona da controllare ha dato il proprio consenso all'esecuzione del controllo, nella misura in cui ciò sia necessario;

d. è eventualmente disponibile il consenso del servizio competente secondo gli articoli 7 o 8 (capoverso 2).

2 Nel caso della ripetizione straordinaria di un controllo verificano se tale ripetizione è sufficientemente motivata.

13 RS **172.220.111.3**

3 Se una delle condizioni di cui ai capoversi 1 e 2 non è soddisfatta, i servizi specializzati CSP non eseguono il controllo e lo comunicano immediatamente al servizio promotore.

Art. 18 Collaborazione
(art. 32 cpv. 3 LSIn)

1 La persona da controllare deve in particolare:

a. inoltrare i documenti e i dati utili al controllo;

b. fornire informazioni in modo veritiero.

2 Se la persona da controllare viene meno al suo obbligo di collaborazione nonostante il relativo ammonimento, i servizi specializzati CSP ne fanno menzione nel quadro della valutazione del rischio.

3 Se la persona da controllare si rifiuta di cooperare in modo tale da impedire una corretta valutazione, il servizio specializzato CSP emana una dichiarazione di constatazione secondo l'articolo 39 capoverso 1 lettera d LSIn.

Art. 19 Raccolta dei dati
(art. 34 LSIn)

1 I servizi specializzati CSP possono raccogliere e trattare i dati secondo l'allegato 7.

2 Viene effettuata un'audizione secondo l'articolo 34 capoverso 2 lettera d LSIn se:

a. secondo l'articolo 2 capoverso 1 OPers[14] il Consiglio federale è competente per costituire, modificare e risolvere il rapporto di lavoro;

b. secondo l'articolo 2 capoverso 1[bis] OPers il capo di Dipartimento o il cancelliere della Confederazione è competente per costituire, modificare e risolvere il rapporto di lavoro;

c. la persona da controllare esercita o è previsto che eserciti una funzione presso uno degli organi seguenti:
   1. SIC,
   2. autorità d'esecuzione cantonale secondo l'articolo 9 LAIn[15],
   3. SIM,
   4. COE,
   5. AVI-AIn,
   6. fedpol,
   7. servizi specializzati CSP;

d. la persona da controllare in quanto impiegata della Confederazione deve trattare informazioni classificate «segreto» e:

14 RS **172.220.111.3**
15 RS **121**

1. di conseguenza può avere una conoscenza in modo approfondito di affari importanti in materia di politica di sicurezza e un influsso significativo su di essi, oppure
2. svolge compiti di vigilanza e di coordinamento per funzioni secondo la lettera c;

e. in virtù di un trattato internazionale è prevista un'audizione.

3 Nel caso della ripetizione di controlli di sicurezza relativi alle persone è possibile rinunciare all'audizione.

4 Un'audizione secondo l'articolo 34 capoverso 3 LSIn come pure secondo l'articolo 113 capoverso 5 lettera e LM può essere effettuata presso i seguenti terzi:

a. specialisti medici e psicologici che assistono o che hanno assistito la persona da controllare;
b. istituti di formazione presso i quali la persona da controllare ha assolto delle formazioni;
c. precedenti o attuali superiori professionali o militari della persona da controllare;
d. altre persone dalle quali ci si possono attendere informazioni rilevanti sulla persona da controllare.

5 I servizi specializzati CSP possono svolgere le audizioni con l'ausilio di strumenti audiovisivi.

Art. 20 Assistenza amministrativa
(art. 35 LSIn)

1 Le autorità o le organizzazioni responsabili della raccolta di dati all'estero secondo l'articolo 34 LSIn trasmettono i dati raccolti ai servizi specializzati CSP:

a. indicando le fonti dei dati;
b. valutando l'affidabilità dei dati e delle fonti.

2 Tutti i dati che per se stessi o in relazione con altri dati possono fornire indicazioni concrete sui rischi per la sicurezza sono considerati rilevanti ai fini della sicurezza secondo l'articolo 35 capoverso 2 LSIn.

Art. 21 Raggruppamento di procedure di controllo

1 Se un'attività è soggetta a diversi controlli di cui all'articolo 1 capoverso 1, viene eseguita soltanto un'unica procedura di controllo.

2 Se l'attività è attribuita a diversi livelli di controllo secondo il capoverso 1, la procedura di controllo viene eseguita secondo i requisiti del livello di controllo più elevato, con riserva dell'articolo 27.

3 Se la responsabilità del controllo spetta sia al servizio specializzato CSP CaF che al servizio specializzato CSP DDPS, il controllo viene eseguito dal servizio specializzato CSP CaF. Sono fatte salve le valutazioni del potenziale di pericolo o di abuso secondo

l'articolo 113 capoverso 4 lettera d LM che vengono sempre eseguite dal servizio specializzato CSP DDPS.

4 Il competente servizio specializzato CSP indica nella dichiarazione di cui all'articolo 39 capoverso 1 LSIn il risultato della valutazione per ogni singolo controllo.

Art. 22 Condizioni
(art. 39 cpv. 1 lett. b LSIn)

I servizi specializzati CSP possono raccomandare ai servizi decisori di:

a. obbligare la persona sottoposta al controllo a rivelare dati personali al servizio decisore, in particolare:
   1. dati relativi a rapporti personali con terzi,
   2. dati finanziari, compresi i dati relativi a conti bancari e imposte,
   3. dati in merito ad accertamenti di cui alla lettera b,
   4. dati in merito a procedimenti pendenti al momento della dichiarazione;
b. far svolgere accertamenti medici o psicologici, in particolare accertamenti per quanto riguarda la capacità di giudizio e di decisione della persona da controllare come pure il consumo di droghe e di sostanze stupefacenti;
c. adottare misure secondo l'articolo 25 LPers;
d. applicare misure concernenti il possesso dell'arma personale, nella misura in cui la persona da controllare è un militare;
e. adottare altre misure che sembrano adeguate nei singoli casi specifici per ridurre il rischio per la sicurezza a un livello sostenibile.

Art. 23 Comunicazione
(art. 40 LSIn)

1 Se una persona è soggetta in modo consecutivo a diversi motivi di controllo e in occasione del controllo successivo un servizio specializzato CSP constata un rischio per la sicurezza, tale servizio comunica la propria dichiarazione ai servizi decisori dei controlli precedenti.

2 I servizi specializzati CSP comunicano le constatazioni provvisorie se sussistono segni di un rischio per la sicurezza che richiede un intervento urgente. Nel caso dei controlli di persone soggette all'obbligo di leva o di militari si può trattare in particolare di:

a. sentenze penali;
b. indagini di polizia, inchieste penali o procedimenti penali in corso a causa di un sospetto di un delitto o un crimine commesso; la comunicazione avviene soltanto se, in base alla valutazione del servizio che dirige l'indagine o il procedimento, non compromette la procedura in corso;
c. seri segni o indizi secondo l'articolo 113 capoverso 1 LM oppure un sospetto di tali segni o indizi;

d. segni o indizi per un'idoneità al servizio militare limitata, un'inidoneità al servizio militare oppure un'incapacità alla funzione;

e. seri segni o indizi che possano mettere in pericolo se stessi o terzi.

3 I servizi decisori comunicano ai servizi specializzati CSP a quale persona o servizio debbano essere inoltrate le comunicazioni secondo i capoversi 1 e 2.

Sezione 6: Conseguenze della dichiarazione

Art. 24 Esercizio dell'attività
(art. 41 LSIn)

1 Il servizio decisore permette alla persona sottoposta al controllo di esercitare l'attività soltanto se giudica sostenibili i rischi individuati o li può ridurre a un livello sostenibile con le condizioni di cui all'articolo 22.

2 Nel caso di dichiarazioni secondo l'articolo 39 capoverso 1 lettere b–d LSIn comunica la propria decisione alla persona sottoposta al controllo e al competente servizio specializzato CSP entro un mese. Nel caso di una dichiarazione di sicurezza secondo l'articolo 39 capoverso 1 lettera a LSIn si presume l'ammissione a esercitare l'attività.

Art. 25 Uso plurimo di una dichiarazione
(art. 42 LSIn)

1 Se a una persona è già stata rilasciata una dichiarazione valida in occasione di un controllo precedente, il servizio decisore può rinunciare a una nuova valutazione se:

a. alla base del controllo precedente vi erano gli stessi fattori di rischio del nuovo controllo; e

b. non esiste alcun motivo per una ripetizione straordinaria.

2 I rischi per la sicurezza constatati in occasione di una valutazione di un livello di controllo superiore devono essere considerati soltanto se:

a. questi rischi potrebbero essere individuati anche sulla base dei dati che vengono raccolti ad un livello di controllo inferiore; oppure

b. l'interesse pubblico di cui all'articolo 1 capoverso 2 LSIn è preponderante rispetto al diritto della personalità della persona sottoposta al controllo.

Art. 26 Ripetizione ordinaria
(art. 43 cpv. 1 e 2 LSIn)

1 Occorre avviare una ripetizione ordinaria del controllo:

a. entro tre mesi prima della scadenza del termine massimo di cui all'articolo 43 capoverso 1 LSIn: se in occasione del controllo precedente è stata rilasciata una dichiarazione di sicurezza secondo l'articolo 39 capoverso 1 lettera a LSIn;

b. entro tre mesi dopo la scadenza del termine minimo di cui all'articolo 43 capoverso 1 LSIn: se in occasione del controllo precedente è stata rilasciata una dichiarazione secondo l'articolo 39 capoverso 1 lettere b–d LSIn;

c. per funzioni dell'esercito e della protezione civile per il cui esercizio è necessario un controllo di sicurezza di base: se si prevede che la persona da controllare debba svolgere la funzione per almeno altri cinque anni.

2 Sono fatte salve altre scadenze in virtù di un trattato internazionale.

Art. 27 Ripetizione straordinaria
(art. 43 cpv. 3 LSIn)

1 Se ha motivo di presumere che dall'ultimo controllo siano emersi nuovi rischi rilevanti, che non possono essere valutati senza una ripetizione del controllo, il servizio decisore avvia immediatamente una ripetizione straordinaria del controllo.

2 Se ha motivo di presumere che determinati rischi constatati in occasione dell'ultimo controllo siano nel frattempo venuti meno, il servizio decisore può avviare una ripetizione straordinaria del controllo.

Art. 28 Effetto della ripetizione
(art. 43 LSIn)

1 Fino alla nuova decisione in virtù dell'articolo 24 capoverso 2 la persona sottoposta al controllo è considerata controllata secondo la decisione attuale.

2 Se prima della notifica della nuova decisione emergono segni di nuovi rischi per la sicurezza, il servizio decisore adotta le necessarie misure preventive.

Art. 29 Tutela giurisdizionale
(art. 44 cpv. 3 LSIn)

I servizi specializzati CSP sono autorizzati a interporre ricorso al Tribunale federale per quanto riguarda le decisioni del Tribunale amministrativo federale in merito alle loro dichiarazioni.

Art. 30 Attestazione di sicurezza nel contesto internazionale
(art. 48 lett. c LSIn)

1 La competenza per il rilascio di attestati di sicurezza nel contesto internazionale spetta al servizio specializzato della Confederazione per la sicurezza delle informazioni.

2 Un'attestazione di sicurezza viene rilasciata su richiesta se:

a. è stato effettuato un controllo del livello di controllo necessario;

b. la persona in questione è stata autorizzata a esercitare l'attività; e

c. la persona in questione è stata istruita in maniera comprovabile per esercitare l'attività.

3 Se non fa parte dell'Amministrazione federale e non necessita dell'attestazione di sicurezza per un mandato della Confederazione, il servizio richiedente si assume i costi della procedura.

Sezione 7: Trattamento di dati personali

Art. 31 Responsabilità della protezione dei dati e della sicurezza dei dati
(art. 48 lett. d LSIn)

1 Il servizio specializzato CSP DDPS è responsabile della protezione e della sicurezza del sistema d'informazione di cui all'articolo 45 LSIn come pure dei dati in esso contenuti.

2 La responsabilità della protezione e della sicurezza di dati che vengono trattati al di fuori del sistema d'informazione secondo l'articolo 45 capoverso 5 LSIn spetta al servizio che si occupa del trattamento dei dati.

Art. 32 Controllo periodico del trattamento dei dati personali
(art. 48 lett. e LSIn)

Il DDPS e la Cancelleria federale provvedono affinché un servizio indipendente verifichi almeno ogni cinque anni la liceità del trattamento dei dati personali nel sistema d'informazione da parte dei rispettivi servizi specializzati CSP.

Sezione 8: Disposizioni finali

Art. 33 Gestione elettronica degli affari
(art. 48 lett. a LSIn)

Il DDPS disciplina, previa consultazione della Cancelleria federale, la gestione elettronica degli affari.

Art. 34 Riscossione di emolumenti

1 Per l'esecuzione di controlli presso servizi al di fuori dell'Amministrazione federale centrale, i servizi specializzati CSP riscuotono emolumenti in funzione del tempo impiegato.

2 Viene applicata una tariffa oraria di 100–400 franchi. La tariffa dipende in particolare dall'urgenza dell'affare e dal livello di funzione del personale che esegue il lavoro.

3 Per il resto si applica l'ordinanza generale dell'8 settembre 2004[16] sugli emolumenti (OgeEm).

16 RS **172.041.1**

Art. 35 Prestazioni dei servizi specializzati CSP a favore dei Cantoni
(art. 86 cpv. 4 LSIn)

1 I Cantoni possono avvalersi delle prestazioni dei servizi specializzati CSP DDPS per la propria sicurezza delle informazioni se:

a. dispongono di una base legale sufficiente per i controlli ai sensi della presente ordinanza;

b. per garantire la sicurezza delle informazioni intendono procedere a valutazioni analoghe a quelle della Confederazione; e

c. hanno stipulato con il DDPS un accordo sulle prestazioni.

2 Negli accordi sulle prestazioni secondo l'articolo 1 lettera c il DDPS disciplina in particolare:

a. il numero di controlli da effettuare;

b. i servizi promotori e decisori presso i Cantoni;

c. il finanziamento delle prestazioni, comprese le modalità.

3 L'ammontare degli emolumenti è calcolato in funzione del tempo impiegato. Si applica una tariffa oraria di 100–400 franchi. La tariffa dipende in particolare dall'urgenza dell'affare e dal livello di funzione del personale che esegue il lavoro. Per il resto si applica l'OgeEm[17].

Art. 36 Abrogazione di altri atti normativi

Sono abrogati:

a. l'ordinanza del 4 marzo 2011[18] sui controlli di sicurezza relativi alle persone;

b. l'ordinanza della Cancelleria federale del 30 novembre 2011[19] sui controlli di sicurezza relativi alle persone;

c. l'ordinanza del DEFR del 2 novembre 2011[20] sui controlli di sicurezza relativi alle persone;

d. l'ordinanza del DDPS del 12 marzo 2012[21] sui controlli di sicurezza relativi alle persone;

e. l'ordinanza del DFAE del 14 agosto 2012[22] sui controlli di sicurezza relativi alle persone;

f. l'ordinanza del DATEC del 15 febbraio 2013[23] sui controlli di sicurezza relativi alle persone;

17 RS **172.041.1**
18 [RU **2011** 5903, **2012** 1153 3631 3765 5527 6669, **2013** 3041, **2014** 4567, **2016** 1785, **2017** 4151 4231, **2020** 5893]
19 [RU **2011** 6077, **2016** 1365]
20 [RU **2011** 4999, **2013** 1335]
21 [RU **2012 1161 1597**]
22 [RU **2012 4241**]
23 [RU **2013 765**]

g. l'ordinanza del DFGP del 26 giugno 2013[24] sui controlli di sicurezza relativi alle persone;

h. l'ordinanza del DFI del 12 agosto 2013[25] sui controlli di sicurezza relativi alle persone;

i. l'ordinanza del 9 giugno 2006[26] sui controlli di sicurezza relativi alle persone nell'ambito degli impianti nucleari.

Art. 37 Modifica di altri atti normativi

La modifica di altri atti normativi è disciplinata nell'allegato 8.

Art. 38 Diposizioni transitorie

1 Le valutazioni ancora pendenti al momento dell'entrata in vigore della presente ordinanza vengono portate avanti secondo la LSIn e la presente ordinanza oppure interrotte.

2 Durante il periodo transitorio secondo l'articolo 90 capoverso 3 LSIn i controlli di sicurezza relativi alle persone effettuati secondo il diritto anteriore corrispondono ai livelli di controllo secondo il nuovo diritto come indicato qui di seguito:

a. controllo di sicurezza di base secondo il diritto anteriore: controllo di sicurezza di base secondo il nuovo diritto;

b. controllo di sicurezza ampliato secondo il diritto anteriore: controllo di sicurezza ampliato secondo il nuovo diritto;

c. controllo di sicurezza ampliato con audizione secondo il diritto anteriore: controllo di sicurezza ampliato secondo il nuovo diritto.

3 Le persone in funzioni per le quali secondo il nuovo diritto deve essere effettuato un controllo oppure un controllo di un livello di controllo superiore, fino alla decisione secondo l'articolo 24 capoverso 2 sono considerate controllate se il nuovo controllo necessario viene avviato entro tre mesi dall'entrata in vigore della presente ordinanza. Se durante il controllo emergono segni di rischi per la sicurezza, il servizio decisore adotta le necessarie misure preventive.

4 I controlli di sicurezza ricevuti dalla società nazionale di rete su base privata prima dell'entrata in vigore della presente ordinanza e prima della scadenza del termine di cui al capoverso 5 restano utilizzabili nel quadro dei termini di ripetizione secondo gli articoli 26 e 27 come indicato qui di seguito:

a. controlli di sicurezza per funzioni critiche: come controllo di sicurezza di base secondo la presente ordinanza;

b. controlli di sicurezza per funzioni estremamente critiche: come controllo di sicurezza ampliato secondo la presente ordinanza.

24 [RU **2013 2633**]
25 [RU **2013 2675**]
26 [RU **2006 2481**, **2008 547**, **2011 1031**]

5 La società nazionale di rete è autorizzata a far svolgere verifiche dell'affidabilità secondo l'articolo 20*a* LAEl su base privata fino a un anno dopo l'entrata in vigore della presente ordinanza.

Art. 39 Entrata in vigore

La presente ordinanza entra in vigore il … 2023:

In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Ignazio Cassis
Il cancelliere della Confederazione, Walter Thurnherr

Allegato 1[27]
(art. 3 cpv. 1 lett. a)

Funzioni dell'Amministrazione federale soggette a un controllo di sicurezza relativo alle persone secondo la LSIn

1. Del livello di controllo di sicurezza di base:

Unità amministrativa	Funzione	Motivo del controllo secondo l'art. 10 cpv. 1		
		lett. a	lett. b	lett. c

2. Del livello di controllo di sicurezza ampliato:

Unità amministrativa	Funzione	Motivo del controllo secondo l'art. 10 cpv. 2			
		lett. a	lett. b	lett. c	lett. d

27 Non pubblicato nella RU secondo l'articolo 6 della legge del 18 giugno 2004 sulle pubblicazioni ufficiali (RS **170.512**).

Allegato 2
(art. 3 cpv. 1 lett. b)

Funzioni dell'Amministrazione federale soggette a una verifica dell'affidabilità secondo la LAsi

a. …,

b. …;

c. ….

Allegato 3
(art. 3 cpv. 1 lett. c)

Funzioni dell'Amministrazione federale soggette a una verifica dell'affidabilità secondo la LPers

1. Del livello di controllo di sicurezza di base:

Unità amministrativa	Funzione	Motivo del controllo secondo l'art. 11 cpv. 1				
		lett. a	lett. b	lett. c	lett. d	lett. e

2. Del livello di controllo di sicurezza ampliato:

Unità amministrativa	Funzione	Motivo del controllo secondo l'art. 11 cpv. 2		
		lett. a	lett. b	lett. c

Allegato 4[28]
(art. 3 cpv. 2 lett. a)

Funzioni dell'esercito soggette a un controllo di sicurezza relativo alle persone secondo la LSIn

1. Del livello di controllo di sicurezza di base:

Livello dell'articolazione e della struttura	Funzione	Motivo del controllo secondo l'art. 10 cpv. 1		
		lett. a	lett. b	lett. c

2. Del livello di controllo di sicurezza ampliato:

Livello dell'articolazione e della struttura	Funzione	Motivo del controllo secondo l'art. 10 cpv. 2	
		lett. a	lett. b

28 Non pubblicato nella RU secondo l'articolo 6 della legge del 18 giugno 2004 sulle pubblicazioni ufficiali (RS **170.512**).

Allegato 5
(art. 3 cpv. 2 lett. b)

Funzioni dell'esercito soggette a una verifica dell'affidabilità secondo l'articolo 14 LM

Del livello di controllo di sicurezza di base:

Livello dell'articolazione e della struttura	Funzione	Motivo del controllo secondo l'art. 12 cpv. 1 lett. a e b		
		lett. a	lett. b	

Allegato 6[29]
(art. 3 cpv. 3)

Funzioni secondo l'articolo 20*a* capoverso 1 LAEl

1. Del livello di controllo di sicurezza di base:

Funzione	Informazione / applicazione / infrastruttura critica

2. Del livello di controllo di sicurezza ampliato:

Funzione	Informazione / applicazione / infrastruttura estremamente critica

29 Non pubblicato nella RU secondo l'articolo 6 della legge del 18 giugno 2004 sulle pubblicazioni ufficiali (RS **170.512**).

Allegato 7
(art. 19 cpv. 1)

Raccolta e trattamento di dati

1. Dati che possono essere raccolti a tutti i livelli di controllo

a. Dati sull'identità della persona da controllare, in particolare:
   1. cognome, cognome da nubile/celibe e nomi
   2. soprannome, alias, pseudonimo e nome utente
   3. indirizzi
   4. data di nascita
   5. sesso o genere
   6. numeri di telefono (rete fissa e rete mobile)
   7. indirizzi e-mail (professionale e privato)
   8. numero AVS
   9. nazionalità
   10. in caso di nazionalità diversa da quella svizzera:
      – data della naturalizzazione
      – durata del soggiorno in Svizzera
   11. luogo d'origine
   12. luogo di nascita
   13. luoghi di domicilio precedenti

b. Dati sulla condotta di vita della persona da controllare, in particolare:
   1. carriera professionale
   2. carriera scolastica
   3. carriera nell'esercito, nella protezione civile o nel servizio civile
   4. formazioni
   5. hobby
   6. progetti
   7. appartenenza ad associazioni
   8. attività a titolo onorifico
   9. credenze o attività religiose
   10. opinioni filosofiche
   11. opinioni o attività politiche
   12. opinioni o attività sindacali

c. Dati sulle relazioni personali strette e sulla situazione familiare della persona da controllare, in particolare:
   1. stato civile
   2. sfera intima e sessualità

3. rapporto con la famiglia
4. identità dei genitori
5. cerchia di amici

d. Dati in merito alla relazione con l'estero della persona da controllare, in particolare:
1. vacanze
2. soggiorni linguistici
3. viaggi d'affari
4. relazioni personali all'estero e contatti internazionali
5. interessi finanziari all'estero

e. Dati sulla salute della persona da controllare, in particolare:
1. malattie fisiche e psichiche
2. menomazioni fisiche e psichiche
3. consumo di sostanze stupefacenti e di alcol
4. dipendenze

f. Dati finanziari della persona da controllare, in particolare:
1. estratti di conti bancari
2. attività finanziarie
3. salari
4. ipoteche
5. crediti
6. patrimoni
7. imposte
8. debiti
9. investimenti

g. Dati su procedimenti e sanzioni amministrativi o penali, in particolare:
1. esecuzioni e fallimenti
2. inchieste penali
3. inchieste amministrative
4. cause e procedimenti legali
5. mediazione
6. revoche di documenti

h. Dati su fattori di rischio riscontrati sinora nel quadro di un'attività sensibile sotto il profilo della sicurezza

i. Dati su terzi, in particolare:

1. dati secondo le lettere a–g sul coniuge o partner come pure sulla cerchia familiare e sulla cerchia di amici più intimi, nella misura in cui questi dati secondo l'articolo 34 capoverso 3 LSIn sono indispensabili ai fini della valutazione del rischio per la sicurezza
2. datore di lavoro e suo indirizzo
3. progetto

j. Dati ottenuti da sistemi e fonti pubblicamente accessibili, in particolare:
   1. dal casellario giudiziale: tutti i dati
   2. dalle autorità penali civili e militari: tutti i dati
   3. da organi della Confederazione secondo l'articolo 34 capoverso 1 lettera c LSIn:
      - dati del sistema d'informazione sulle armi ARMADA
      - dati del sistema d'informazione HOOGAN
      - dati del sistema d'informazione JANUS
      - dati del registro nazionale di polizia
      - dati del sistema di ricerca informatizzato di polizia RIPOL
      - dati dei sistemi d'informazione del SIC e del SIM
      - dati del registro SIAC
      - dati dello JORASYS
      - dati dei sistemi d'informazione dell'UDSC
      - dati del registro centrale degli assicurati delle assicurazioni sociali della Confederazione
      - dati del PISA
      - dati del reclutamento delle persone soggette all'obbligo di leva
      - dati sull'apprezzamento dell'idoneità al servizio e dell'idoneità a prestare servizio militare servizio delle persone soggette all'obbligo di leva, di prestare servizio militare e di prestare servizio di protezione civile come pure di civili che vengono chiamati a svolgere un impiego a tempo determinato nell'esercito
      - dati dell'esercito e dell'amministrazione militare in merito a persone soggette all'obbligo di leva e a militari

   4. dai registri e dagli atti degli organi di sicurezza dei Cantoni come pure della polizia: tutti i dati
   5. dai registri delle autorità di esecuzione e fallimento: tutti i dati

6. dagli atti dei controlli sinora effettuati: tutti i dati che risalgono a non più di dieci anni prima e che non sono ancora stati archiviati o distrutti secondo l'articolo 47 LSIn
7. da fonti pubblicamente accessibili:
   - su Internet: dati che sono accessibili a qualsiasi utente di Internet, dopo aver creato un account, pagato una quota d'iscrizione oppure dopo aver sottoscritto un abbonamento
   - sui social media: dati che sono accessibili a qualsiasi utente senza aver preso personalmente contatto con un altro utente.

2. Dati che possono essere raccolti soltanto nell'ambito del livello di controllo di sicurezza ampliato:

a. da autorità fiscali federali e cantonali: tutti i dati

b. dai registri dei controlli degli abitanti: tutti i dati

c. da istituti finanziari e banche secondo l'articolo 34 capoverso 2 lettera c LSIn: tutti i dati

d. mediante audizione della persona da controllare: tutti i dati che non risultano o che risultano soltanto in modo poco chiaro dalla restante raccolta dei dati

Allegato 8
(art. 37)

Modifica di altri atti normativi

Gli atti normativi qui appresso sono modificati come segue:

1. Ordinanza del 7 marzo 2003[30] sull'organizzazione del Dipartimento federale della difesa, della protezione della popolazione e dello sport

Art. 6 lett. c

Abrogato

2. Ordinanza del 3 luglio 2001[31] sul personale federale

Art. 94e Estratto del casellario giudiziale e del registro delle esecuzioni
(art. 20*a* LPers)

1 Se appropriato e necessario per motivi di prevenzione della corruzione o di sicurezza oppure se gli interessi economici o politici del datore di lavoro potrebbero essere messi in pericolo, 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.

2 L'estratto può essere richiesto ogni cinque anni oppure per motivi validi in qualsiasi momento.

3 I costi per gli estratti sono assunti dal datore di lavoro.

Art. 94f Verifica dell'affidabilità
(art. 20*b* LPers)

1 Una verifica dell'affidabilità di candidati a un impiego e di impiegati può essere eseguita alle condizioni menzionate nell'articolo 11 dell'ordinanza del …[32] sul controllo di sicurezza relativo alle persone (OCSP).

2 L'elenco delle funzioni, i livelli di controllo e la procedura di controllo sono disciplinati nell'OCSP.

30 RS **172.214.1**
31 RS **172.220.111.3**
32 RS …

3. Ordinanza del 24 giugno 2009[33] sui contatti militari internazionali

Art 5 cpv. 1 lett. b

1 La consegna di informazioni classificate a persone e organi stranieri nonché l'accesso da parte di visitatori stranieri a informazioni militari classificate, a materiale classificato o a impianti militari in Svizzera si fonda sulle corrispondenti prescrizioni in materia di protezione delle informazioni, segnatamente:

b. l'ordinanza del …[34] sui controlli di sicurezza relativi alle persone;

4. Ordinanza del 16 dicembre 2009[35] sui sistemi d'informazione militari

Art. 67 e allegato 30

Abrogati

Art. 70n lett. e

I dati del sistema FABIS sono raccolti:

e. dal sistema d'informazione per i controlli di sicurezza relativi alle persone di cui all'articolo 45 capoverso 1 della legge del 18 dicembre 2020[36] sulla sicurezza delle informazioni: i dati secondo l'allegato 33*c* numero 2.

Allegato 23a N. 36

36. Livello di controllo secondo l'articolo 5 o 6 dell'ordinanza del …[37] sui controlli di sicurezza relativi alle persone (OCSP), data del passaggio in giudicato della decisione conformemente all'articolo 24 OCSP come pure termine della successiva ripetizione ordinaria del controllo di sicurezza relativo alle persone secondo l'articolo 26 OCSP

Allegato 33c N. 2

2. Livello di controllo secondo gli articoli 10–14 OCSP[38], data del passaggio in giudicato della decisione conformemente all'articolo 24 OCSP come pure termine della successiva ripetizione ordinaria del controllo di sicurezza relativo alle persone secondo l'articolo 26 OCSP concernente una persona autorizzata ad accedere.

33 RS **510.215**
34 RS **…**
35 RS **510.911**
36 RS **128**
37 RS **…**
38 RS **…**

Allegato 33d N. 2

2. Livello di controllo secondo gli articoli 10–14 OCSP[39], data del passaggio in giudicato della decisione secondo l'articolo 24 OCSP come pure termine della successiva ripetizione ordinaria del controllo di sicurezza relativo alle persone secondo l'articolo 26 OCSP concernente una persona autorizzata ad accedere.

5. Ordinanza del 22 novembre 2017[40] concernente l'obbligo di prestare servizio militare

Art. 11 cpv. 3 lett. g

4 Alla manifestazione informativa i partecipanti vengono in particolare informati su:

g. i controlli di sicurezza relativi alle persone secondo l'ordinanza del …[41] sui controlli di sicurezza relativi alle persone (OCSP) e le conseguenze in presenza di circostanze personali particolari secondo l'articolo 33 capoverso 2.

Art. 16 cpv. 3 lett. b

3 Una persona idonea al servizio militare è attribuita provvisoriamente a una funzione di reclutamento dell'esercito, se:

b. è necessario un controllo di sicurezza relativo alle persone, ma non vi è ancora alcuna decisione secondo l'articolo 24 OCSP[42] o alcuna informazione secondo l'articolo 23 capoverso 2 OCSP.

Art. 21 cpv. 1 lett. b n. 3

1 Su domanda congiunta della persona interessata e del comando competente, gli specialisti, i sottufficiali superiori e gli ufficiali superiori possono essere autorizzati a prorogare l'obbligo di prestare servizio militare, se:

b. la persona interessata soddisfa le condizioni seguenti:
   3. il servizio decisore secondo l'articolo 24 OCSP[43] consente alla persona interessata di esercitare la funzione.

Art. 72 cpv. 2 lett. c

2 Per l'incorporazione in una determinata funzione o la promozione a un grado superiore devono essere soddisfatte le condizioni seguenti:

39 RS **…**
40 RS **512.21**
41 RS **…**
42 RS **…**
43 RS **…**

c. il servizio decisore secondo l'articolo 24 OCSP [44] consente alla persona interessata di esercitare la funzione.

Art. 80 cpv. 2 lett. c

2 Soldati, appuntati, sottufficiali e sottufficiali superiori possono essere nominati ufficiali specialisti se:

c. il servizio decisore secondo l'articolo 24 OCSP [45] consente alla persona interessata di esercitare la funzione.

6. Ordinanza del 10 dicembre 2004[46] sull'energia nucleare

Art. 33a Controlli di affidabilità

1 I controlli periodici di affidabilità di persone impiegate in funzioni essenziali per la sicurezza nucleare e la sicurezza esterna degli impianti nucleari sono disciplinati nell'ordinanza del …[47] sul controllo di sicurezza relativo alle persone.

2 I costi per il controllo vengono assunti dal titolare della licenza della centrale nucleare.

44 RS **…**
45 RS **…**
46 RS **732.11**
47 RS …

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ordinanza sulla procedura di sicurezza relativa alle aziende
(OPSAz)

del … Avamprogetto del 25 luglio 2022

Il Consiglio federale svizzero,

visti gli articoli 73 e 84 capoverso 1 della legge del 18 dicembre 2020[1] sulla sicurezza delle informazioni (LSIn),

ordina:

Sezione 1: Disposizioni generali

Art. 1 Oggetto e campo d'applicazione
(art. 2, 49 e 73 LSIn)

[1] La presente ordinanza disciplina:

a. la procedura di sicurezza relativa alle aziende di cui agli articoli 49–73 LSIn;

b. l'applicazione della procedura di sicurezza relativa alle aziende a imprese subappaltatrici;

c. l'organizzazione del servizio specializzato competente per l'esecuzione della procedura di sicurezza relativa alle aziende (servizio specializzato PSA);

d. la sicurezza dei dati nel sistema d'informazione secondo l'articolo 70 LSIn;

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

[2] Fatti salvi l'articolo 84 capoverso 3 LSIn e l'articolo 2 capoversi 2−5 dell'ordinanza del …[2] sulla sicurezza delle informazioni (OSIn), si applica alle autorità e alle organizzazioni assoggettate di cui all'articolo 2 LSIn.

Art. 2 Aziende interessate
(art. 50 LSIn)

[1] La presente ordinanza si applica alle aziende con sede in Svizzera.

RS .....
1 RS **128**
2 RS ...

2 Per le aziende con sede all'estero la procedura è disciplinata dal corrispondente trattato internazionale secondo l'articolo 87 LSIn.

Art. 3 Autorità competente
(art. 51 cpv. 2 LSIn)

1 Il [Dipartimento competente] gestisce il servizio specializzato PSA.

2 Il servizio specializzato coordina le attività internazionali con il servizio specializzato della Confederazione per la sicurezza delle informazioni secondo l'articolo 83 LSIn.

Sezione 2: Avvio della procedura di sicurezza relativa alle aziende

Art. 4 Domanda di avvio della procedura
(art. 52 LSIn)

1 I seguenti organi nella sfera di competenze del Consiglio federale sono competenti per presentare la domanda d'avvio della procedura al servizio specializzato PSA:

a. gli incaricati della sicurezza delle informazioni delle unità amministrative secondo l'articolo 37 OSIn;

b. gli incaricati della sicurezza aziendale in applicazione dell'articolo 12 lettera c.

2 Le autorità assoggettate secondo l'articolo 2 capoverso 1 LSIn comunicano al servizio specializzato PSA chi è competente per la domanda di avvio della procedura nel rispettivo ambito di competenza:

3 La domanda comprende in particolare:

a. una descrizione della prestazione edile, della fornitura o della prestazione di servizio;

b. commenti sulla sensibilità del mandato sotto il profilo della sicurezza;

c. informazioni sulla procedura di aggiudicazione prevista.

Art. 5 Esame della domanda
(art. 53 LSIn)

1 Prima di avviare la procedura il servizio specializzato PSA consulta il mandante o l'autorità estera o l'organizzazione internazionale competente in materia.

2 Avvia la procedura in ogni caso se è soddisfatta una delle condizioni seguenti:

a. il mandato sensibile comprende il trattamento di informazioni classificate «segreto» o l'amministrazione, l'esercizio, la manutenzione o la verifica di mezzi informatici del livello di sicurezza «protezione molto elevata»;

b. il mandato sensibile comprende il trattamento di informazioni classificate «confidenziale» che concernono più autorità o dipartimenti;

c. il mandato sensibile comprende l'amministrazione, l'esercizio, la manutenzione o la verifica di mezzi informatici del livello di sicurezza «protezione elevata» impiegati per l'adempimento di compiti che coinvolgono più autorità o di compiti interdipartimentali;

d. l'azienda si candida per un mandato per il quale necessita di un'attestazione internazionale di sicurezza aziendale secondo l'articolo 66 LSIn.

3 Se è prevedibile che l'esame della domanda duri più di 30 giorni, il servizio specializzato PSA informa il mandante.

Art. 6 Esame della domanda con autorità di sicurezza estere
(art. 52 cpv. 3 LSIn)

1 Se per l'adempimento del mandato sensibile entrano in linea di conto aziende estere, il servizio specializzato PSA trasmette la domanda al servizio specializzato della Confederazione per la sicurezza delle informazioni.

2 Il servizio specializzato della Confederazione per la sicurezza delle informazioni esamina unitamente all'autorità di sicurezza estera competente, se le aziende interessate dispongono di un'attestazione di sicurezza aziendale valida. In caso contrario, domandano l'avvio della procedura di sicurezza relativa alle aziende.

Art. 7 Definizione dei requisiti di sicurezza
(art. 54 LSIn)

1 I requisiti in materia di sicurezza delle informazioni durante la procedura di aggiudicazione e l'adempimento del mandato si basano sulle disposizioni dell'OSIn[3] e dell'ordinanza del …[4] sui controlli di sicurezza relativi alle persone.

2 Se la procedura è avviata su richiesta di un'autorità estera o di un'organizzazione internazionale, i requisiti in materia di sicurezza delle informazioni sono disciplinati dal rispettivo trattato internazionale.

3 RS …
4 RS …

3 Il servizio specializzato PSA definisce, d'intesa con il mandante, quali compiti sensibili sotto il profilo della sicurezza devono essere eseguiti dal mandante durante la procedura di aggiudicazione e l'adempimento del mandato.

4 Il mandante rimane responsabile del coordinamento degli iter procedurali nell'ambito della procedura di aggiudicazione.

Sezione 3: Valutazione delle aziende

Art. 8 Notifica delle aziende idonee
(art. 55 LSIn)

1 Il mandante può comunicare al servizio specializzato PSA fino a cinque aziende che entrano in considerazione. In casi eccezionali motivati, il servizio specializzato PSA può autorizzare un numero maggiore di aziende su richiesta del mandante.

2 Il servizio specializzato PSA verifica se le aziende che entrano in considerazione hanno dato il loro consenso allo svolgimento della procedura.

3 Informa il mandante se è prevedibile che la valutazione dell'idoneità duri più di 30 giorni.

Art. 9 Raccolta dei dati
(art. 56 LSIn)

1 Il servizio specializzato PSA raccoglie tutti i dati rilevanti per la sicurezza necessari alla valutazione dell'idoneità dell'azienda, in particolare:

a. dati sui rapporti di proprietà e sulle modifiche previste, quali fusioni, partecipazioni o acquisizioni;

b. dati sulla composizione della direzione aziendale;

c. dati sulle relazioni d'interesse dei membri della direzione aziendale;

d. dati sulla solvibilità e su eventuali procedure di pignoramento e fallimento;

e. dati sul pagamento di imposte e contributi sociali;

f. referenze da precedenti procedure d'aggiudicazione;

g. dati sulle relazioni dell'azienda con Stati o organizzazioni esteri e altre dipendenze.

2 Raccoglie presso il Servizio delle attività informative della Confederazione i dati concernenti i compiti secondo l'articolo 6 capoverso 1 lettera a della legge del 25 settembre 2015[5] sulle attività informative.

3 Al servizio specializzato PSA le aziende devono:

a. presentare documentazioni e dati utili per l'esame delle fattispecie di cui al capoverso 1;

5 RS **121**

b. fornire informazioni veritiere.

Art. 10 Esclusione dalla procedura
(art. 57 e 58 LSIn)

1 Il mandante e il servizio specializzato PSA si informano reciprocamente senza indugio se sussistono indizi secondo cui una delle aziende che entrano in considerazione potrebbe essere esclusa dalla procedura di aggiudicazione.

2 Il servizio specializzato PSA continua la procedura finché il mandante non esclude l'azienda interessata dalla procedura di aggiudicazione.

3 Se il mandante esclude l'azienda, la procedura di sicurezza relativa alle aziende concernente tale azienda viene abbandonata.

Art. 11 Scambio di informazioni
(art. 57 e 58 LSIn)

Fatti salvi gli articoli 70 capoverso 3 e 71 capoverso 1 lettera a LSin, nell'ambito dello scambio di informazioni secondo l'articolo 10 capoverso 1, il mandante e il servizio specializzato PSA mettono reciprocamente a disposizione tutte le informazioni e i dati utili per la valutazione dell'idoneità o delle fattispecie secondo l'articolo 44 della legge federale del 21 giugno 2019[6] sugli appalti pubblici (LAPub).

Sezione 4: Piano in materia di sicurezza

Art. 12 Incaricati della sicurezza aziendale

1 Le aziende che entrano in linea di conto per l'esecuzione del mandato comunicano al servizio specializzato PSA un incaricato della sicurezza aziendale e un'adeguata supplenza. L'incaricato è membro della direzione o opera direttamente per essa.

2 L'incaricato della sicurezza aziendale assume i compiti seguenti:

a. è la persona di contatto del servizio specializzato PSA per tutte le questioni relative alla sicurezza delle informazioni;

b. si occupa dell'applicazione del piano in materia di sicurezza;

c. chiede l'avvio della procedura di sicurezza relativa alle aziende per le imprese subappaltatrici nella misura in cui l'azienda è stata autorizzata dal mandante ad aggiudicare un mandato sensibile a tali imprese.

Art. 13 Comunicazione dell'aggiudicazione
(art. 59 cpv. 1 LSIn)

1 La comunicazione dell'aggiudicazione avviene separatamente per ogni singolo rapporto di mandato connesso a un contratto quadro.

6 RS **172.056.1**

2 Unitamente alla comunicazione dell'aggiudicazione, il mandante trasmette al servizio specializzato PSA le informazioni necessarie per l'allestimento del piano in materia di sicurezza.

Art. 14 Contenuto ed esame del piano in materia di sicurezza
(art. 59 cpv. 2 e 3 LSIn)

1 Il servizio specializzato PSA stabilisce le direttive per il piano in materia di sicurezza dopo un esame presso l'azienda.

2 Il piano in materia di sicurezza definisce le misure organizzative, di personale, tecniche e fisiche per garantire un'esecuzione adeguata in funzione dei rischi del mandato rilevante in materia di sicurezza.

3 Se il piano in materia di sicurezza non è conforme alle direttive del servizio specializzato PSA, quest'ultimo accorda all'azienda un termine adeguato per migliorarlo.

4 Se è prevedibile che l'esame del piano in materia di sicurezza duri più di 30 giorni, il servizio specializzato PSA informa il mandante.

Art. 15 Controlli di sicurezza relativi alle persone
(art. 60 LSIn)

1 Il servizio specializzato PSA stabilisce quali persone dell'azienda sottostanno ai controlli di sicurezza relativi alle persone.

2 Può autorizzare l'azienda ad avviare autonomamente il controllo di sicurezza relativo alle persone.

Sezione 5: Dichiarazione di sicurezza aziendale e ripetizione della procedura

Art. 16 Rilascio della dichiarazione di sicurezza aziendale
(art. 61 e 62 LSIn)

La dichiarazione di sicurezza aziendale stabilisce per quale attività sensibile sotto il profilo della sicurezza l'azienda è autorizzata.

Art. 17 Annunci dell'azienda
(art. 63 cpv. 2 LSIn)

1 Sono considerati cambiamenti rilevanti sotto il profilo della sicurezza in particolare:

a. il cambiamento dei rapporti di proprietà o delle strutture dell'azienda;
b. il cambiamento della sede aziendale;
c. il cambiamento della composizione della direzione aziendale;
d. il cambiamento delle relazioni d'interesse dei membri della direzione aziendale;

e. il cambiamento a livello di solvibilità e di eventuali procedure di pignoramento e fallimento;

f. le controversie giuridiche di diritto pubblico e privato nonché i procedimenti penali;

g. i cambiamenti nell'impiego di mezzi informatici;

h. l'assunzione di collaboratori che dovranno essere coinvolti nelle attività sensibili sotto il profilo della sicurezza;

i. i cambiamenti nelle relazioni dell'azienda con Stati o organizzazioni esteri e altre dipendenze;

j. l'esecuzione di mandati che generano un conflitto di interessi con un mandante o una dipendenza da esso.

2 Sono considerati incidenti rilevanti sotto il profilo della sicurezza in particolare:

a. l'accesso illecito nell'azienda;

b. l'impiego indebito dei mezzi informatici dell'azienda;

c. un attacco tentato o riuscito contro i mezzi informatici dell'azienda;

d. la scoperta di punti deboli e di falle nella sicurezza;

e. l'apertura di procedure di esecuzione per debiti e di procedimenti penali contro persone dell'azienda coinvolte nell'esecuzione del mandato sensibile;

f. perquisizioni domiciliari e sequestri.

3 Se vi sono indizi concreti che un incidente di cui al capoverso 2 possa essersi verificato occorre parimenti procedere a un annuncio.

4 L'azienda deve anche annunciare i cambiamenti e gli incidenti di cui ai capoversi 2 e 3 che riguardano i fornitori, nella misura in cui tali cambiamenti e incidenti possono essere rilevanti per l'esecuzione del mandato sensibile.

5 L'azienda informa senza indugio il servizio specializzato PSA se è prevedibile che al momento della scadenza della validità della dichiarazione di sicurezza aziendale è in corso l'esecuzione di un mandato sensibile.

Art. 18 Obblighi del mandante

1 Se il mandante constata un cambiamento o un incidente rilevante sotto il profilo della sicurezza secondo l'articolo 17 nel corso della sua collaborazione con l'azienda, adotta le misure immediate necessarie e informa senza indugio il servizio specializzato PSA.

2 Il mandante deve inoltre informare il servizio specializzato PSA, se:

a. nell'ambito dell'esecuzione del mandato sensibile, dispone di indizi che lasciano supporre una revoca dell'aggiudicazione secondo l'articolo 44 LAPub.

b. intende apportare un cambiamento al mandato rilevante sotto il profilo della sicurezza;

c. intende assegnare un ulteriore mandato all'azienda.

Art. 19 Attestazione internazionale di sicurezza aziendale
(art. 66 LSIn)

1 Per il rilascio di un'attestazione internazionale di sicurezza aziendale il servizio specializzato PSA riscuote un emolumento di 100 franchi.

2 Se per il rilascio dell'attestazione internazionale di sicurezza aziendale è necessario eseguire dapprima una procedura di sicurezza relativa alle aziende, viene riscosso un emolumento supplementare in funzione del tempo impiegato. Si applica una tariffa oraria tra 100 e 400 franchi calcolata in base all'urgenza dell'affare e al livello di funzione del personale che esegue la procedura. Per il resto si applica l'ordinanza generale dell'8 settembre 2004[7] sugli emolumenti.

3 Su richiesta, il servizio specializzato della Confederazione per la sicurezza delle informazioni e il servizio specializzato PSA possono trasmettere all'autorità estera o all'organizzazione internazionale una copia dell'attestazione internazionale di sicurezza aziendale.

Art. 20 Revoca della dichiarazione di sicurezza aziendale e ritiro del mandato
(art. 67 LSIn)

1 Se il servizio specializzato PSA dispone di indizi secondo cui vi è motivo per revocare la dichiarazione di sicurezza aziendale, esso accorda all'azienda, d'intesa con il mandante, un termine adeguato per eliminare la lacuna.

2 Se il mandato viene ritirato in seguito alla revoca della dichiarazione di sicurezza aziendale, il mandante provvede senza indugio a:

a. interrompere immediatamente tutte le attività sensibili sotto il profilo della sicurezza e a revocare i diritti d'accesso corrispondenti;

b. proteggere tutte le informazioni classificate, i mezzi informatici e i materiali.

3 Il mandante conferma al servizio specializzato PSA l'esecuzione delle misure di cui al capoverso 2 entro dieci giorni dalla presa di conoscenza della revoca.

Art. 21 Ripetizione della procedura
(art. 68 LSIn)

1 Il servizio specializzato PSA è competente per l'avvio della ripetizione della procedura di sicurezza relativa alle aziende.

2 Se, al momento della scadenza della validità della dichiarazione di sicurezza aziendale, è in corso la procedura di ripetizione, la validità è prorogata fino al rilascio di una nuova dichiarazione di sicurezza aziendale o fino all'interruzione della procedura di sicurezza relativa alle aziende.

7 RS **172.041.1**

3 Se una dichiarazione di sicurezza aziendale non è rinnovata o se la procedura di sicurezza relativa alle aziende è interrotta, l'articolo 20 è applicabile per analogia. È fatto salvo l'articolo 58 capoverso 3 LSIn.

Sezione 6: Trattamento dei dati personali

Art. 22 Sistema d'informazione sulla procedura di sicurezza relativa alle aziende
(art. 70 LSIn)

I dati personali e aziendali contenuti nel sistema d'informazione sulla procedura di sicurezza relativa alle aziende sono elencati nell'allegato.

Art. 23 Controllo periodico del trattamento di dati personali
(art. 73 lett. e LSIn)

Il [Dipartimento competente] provvede affinché un organo indipendente dal servizio specializzato PSA verifichi almeno ogni cinque anni la liceità del trattamento dei dati personali da parte degli organi coinvolti.

Sezione 7: Disposizioni finali

Art. 24 Abrogazione e modifica del diritto previgente

1 L'ordinanza del 29 agosto 1990[8] sulla tutela del segreto in occasione di mandati con contenuto classificato è abrogata.

2 L'ordinanza del 24 giugno 2009[9] sui contatti militari internazionali è modificata come segue:

Art. 5 cpv. 1 lett. d

1 La consegna di informazioni classificate a persone e organi stranieri nonché l'accesso da parte di visitatori stranieri a informazioni militari classificate, a materiale classificato o a impianti militari in Svizzera si fondano sulle corrispondenti prescrizioni in materia di protezione delle informazioni, segnatamente:

d. l'ordinanza del …[10] sulla procedura di sicurezza relativa alle aziende;

3 L'ordinanza del 16 agosto 2017[11] sulle attività informative è completata come segue:

Allegato 3 numeri 10.5 e 10.6

8 RU **1999** 1774
9 RS **510.215**
10 RS …
11 RS **121.1**

Il SIC può comunicare dati personali alle autorità e ai servizi svizzeri seguenti alle condizioni menzionate all'articolo 60 LAIn e per gli scopi menzionati qui appresso:

10. Dipartimento federale della difesa, della protezione della popolazione e dello sport:

10.5 servizio specializzato per i controlli di sicurezza relativi alle persone: per l'esecuzione di controlli di sicurezza relativi alle persone,

10.6. servizio specializzato per l'esecuzione della procedura di sicurezza relativa alle aziende: per l'esecuzione di procedure di sicurezza relative alle aziende;

4 L'ordinanza del 21 novembre 2018[12] sulla sicurezza militare è modificata come segue:

Art. 3 lett. b

Abrogato

Art. 6 cpv. 2 lett. e f

2 La SIO adempie i compiti seguenti:

e. esegue in seno al DDPS e all'esercito una supervisione tecnica specifica in tali ambiti e disciplina gli obblighi d'annuncio necessari;

f. dispone di diritti di controllo nel DDPS e nell'esercito;

5 L'ordinanza del 16 dicembre 2009[13] sui sistemi d'informazione militari è modificata come segue:

art. 68 e allegato 31

Abrogati

Art. 25 Disposizioni transitorie

Per i mandati aggiudicati prima dell'entrata in vigore della presente ordinanza e le procedure di tutela del segreto pendenti al momento dell'entrata in vigore si applica il diritto anteriore.

Art. 26 Entrata in vigore

La presente ordinanza entra in vigore il … 2023.

12 RS **513.61**
13 RS **510.911**

…

In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Ignazio Cassis
Il cancelliere della Confederazione, Walter Thurnherr

Allegato
(art. 22)

Dati del sistema d'informazione sulla procedura di sicurezza relativa alle aziende

Dati personali

1. Cognome
2. Nome
3. Indirizzo
4. Numero d'assicurato
5. Nazionalità
6. Luogo d'origine
7. Datore di lavoro e indirizzo del datore di lavoro
8. Stato civile
9. Luogo di nascita
10. Data di nascita
11. Data della naturalizzazione
12. Data di inizio del soggiorno in Svizzera
13. Cognome e nome del coniuge o del partner
14. Funzione
15. Mandante e indirizzo del mandante
16. Progetto

Dati concernenti l'azienda

Azienda

17. Numero di dossier
18. Denominazione
19. Indirizzo
20. Numero telefonico
21. Fax
22. Indirizzo e-mail
23. Indirizzo Internet

Incaricato della sicurezza aziendale

24. Appellativo/titolo
25. Cognome

26. Nome
27. Sesso
28. Indirizzo e-mail

Dati concernenti i controlli

29. Data della valutazione dell'idoneità
30. Codice del ramo d'attività economica dell'azienda (codice NOGA)
31. Visita (data, ordine cronologico e osservazioni)
32. Controllo (data, ordine cronologico e osservazioni)
33. Dichiarazione di sicurezza aziendale (data, rilascio, revoca, restituzione)
34. Piano in materia di sicurezza (data, ordine cronologico)

Atti

35. Numero di esemplare
36. Mittente
37. Data dell'atto
38. Data di spedizione
39. Data del controllo
40. Data di restituzione
41. Denominazione

Mandati

42. Denominazione (mandato principale)
43. Mandante
44. Denominazione (mandati)
45. Classificazione
46. Data di notifica
47. Data d'inizio della validità
48. Data di scadenza della validità
49. Denominazione abbreviata (ramo)
50. Codice del ramo d'attività economica dell'azienda (codice NOGA)