Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa, della protezione, della popolazione e dello sport DDPS

Segreteria generale DDPS SG-DDPS
Digitalizzazione e cibersicurezza DDPS

8 novembre 2023

Diritto d'esecuzione relativo alla legge sulla sicurezza delle informazioni

Spiegazioni

Dossier: SG-DDPS-251.2-35/1/6/8

Indice

Spiegazioni

1 Situazione iniziale

Il 18 dicembre 2020 l'Assemblea federale ha approvato la legge sulla sicurezza delle informazioni (LSIn)[1]. Il termine per il referendum è scaduto inutilizzato a metà aprile 2021. La nuova legge crea un quadro legale formale uniforme per la sicurezza delle informazioni in seno alla Confederazione.

L'espressione «sicurezza delle informazioni» comprende la totalità dei requisiti e delle misure con cui vengono protette la confidenzialità, l'integrità, la disponibilità e la tracciabilità di informazioni e di dati di ogni tipo nonché la disponibilità e l'integrità di mezzi informatici. Dato che oggi le informazioni vengono perlopiù trattate elettronicamente, si pone l'accento sulla «cibersicurezza». L'espressione «sicurezza delle informazioni» comprende però anche tutti i processi di elaborazione, dunque anche documenti cartacei e affermazioni orali, e non soltanto il trattamento elettronico. Nell'uso colloquiale, tuttavia, spesso «cibersicurezza» e «sicurezza delle informazioni» sono utilizzati come sinonimi.

Le ordinanze d'esecuzione della LSIn sono state elaborate in collaborazione con rappresentanti delle altre autorità federali assoggettate e dei Cantoni. Nel messaggio del 22 febbraio 2017[2] concernente la legge sulla sicurezza delle informazioni (messaggio LSIn) il Consiglio federale ha annunciato la sua intenzione di invitare le altre autorità federali assoggettate e i Cantoni a esprimere il proprio parere in merito a tutti i disciplinamenti importanti (cfr. n. 1.5, pag. 2621). Lo scopo è conseguire, da un lato, un livello di sicurezza il più uniforme possibile e, dall'altro, tenere debitamente conto delle esigenze di tutte le autorità federali e dei Cantoni. Si è svolta pertanto una procedura di consultazione, i cui risultati sono stati integrati negli atti normativi qui appresso.

2 Punti essenziali degli atti normativi

2.1 Entità del diritto d'esecuzione relativo alla LSIn

Il diritto d'esecuzione relativo alla LSIn comprende quattro ordinanze:

- una nuova ordinanza sulla sicurezza delle informazioni (OSIn; v. n. 3.1);
- una modifica dell'ordinanza del 19 ottobre 2016[3] sui sistemi di gestione delle identità e sui servizi di elenchi della Confederazione (v. n. 3.2);
- una nuova ordinanza sui controlli di sicurezza relativi alle persone (OCSP, v. n. 3.3);
- una nuova ordinanza sulla procedura di sicurezza relativa alle aziende (OPSAz; v. n. 3.4).

Il 29 settembre 2023 le Camere federali hanno adottato una modifica della LSIn che introduce un obbligo di segnalare ciberattacchi a infrastrutture critiche. Il capitolo 5 della LSIn viene così completamente rimaneggiato. La relativa ordinanza è attualmente in fase di elaborazione presso il Dipartimento federale della difesa, della protezione, della popolazione e dello sport (DDPS).

2.2 Condizioni generali e principi

Il Consiglio federale ha motivato la necessità formale e materiale della LSIn nel corrispondente messaggio. Questa situazione iniziale e i relativi obiettivi e approcci di soluzione del Consiglio federale rimangono assolutamente attuali. Fungono da base concettuale per il diritto d'esecuzione relativo alla LSIn. Lo stesso vale per la valutazione della minaccia, l'orientamento strategico della Svizzera e i principi operativi stabiliti dal Consiglio federale e dai Cantoni nell'aprile 2023 nella Ciberstrategia nazionale (CSN). Per l'attuazione della sicurezza delle informazioni nell'Amministrazione federale e nell'esercito occorre inoltre tenere conto di ulteriori strategie, in particolare le strategie informatiche nazionali e interne alla Confederazione

Per l'elaborazione del diritto d'esecuzione relativo alla LSIn sono stati definiti quali indicatori strategici i cinque principi seguenti:

[1] FF **2020** 8755
[2] FF **2017** 2563
[3] RS **172.010.59**

a. Responsabilità in materia di sicurezza interconnessa

Conformemente all'articolo 45 della legge del 21 marzo 1997[4] sull'organizzazione del Governo e dell'Amministrazione (LOGA), i direttori dei gruppi e degli uffici sono responsabili dell'esecuzione dei compiti loro assegnati, compresa la protezione delle proprie informazioni e dei propri mezzi informatici. In un contesto interconnesso e digitalizzato questa responsabilità considerata isolata non è tuttavia sufficiente. Le informazioni vengono scambiate, i sistemi interconnessi e le raccolte di dati rese disponibili per un uso condiviso secondo il cosiddetto principio *«once only»*. In tal modo, minacce e attacchi contro un'organizzazione o i suoi fornitori possono estendersi anche all'ambito di competenza di altre organizzazioni. La sicurezza delle informazioni è quindi necessariamente un compito interconnesso con responsabilità interconnessa che richiede obiettivi comuni, una procedura coordinata e standard minimi.

b. Approccio basato sul rischio

È risaputo che non è possibile raggiungere la sicurezza assoluta e che i rischi sono quindi inevitabili. Le direttive sulla protezione IT di base nell'Amministrazione federale offrono una protezione in funzione dei rischi contro un'ampia gamma di minacce. Servono alla sicurezza delle informazioni interconnessa della Confederazione e devono essere rispettate. Inoltre, nell'ambito della sicurezza delle informazioni i responsabili sono tenuti a esercitare una gestione del rischio attiva, nel contesto della quale i punti deboli, le minacce e le loro potenziali ripercussioni sull'adempimento dei compiti vengono consapevolmente considerati e priorizzati. Con un simile approccio basato sul rischio è possibile concentrarsi, oltre che sui rischi, su possibilità e opportunità, nuove idee, applicazioni o tecnologie.

c. Armonizzazione e standardizzazione

Un'adeguata sicurezza delle informazioni è un presupposto per la fiducia nel Governo elettronico. Ciò vale non soltanto per l'ambito nazionale, ma anche per la crescente interconnessione delle autorità su scala internazionale. Occorre perciò perseguire un'armonizzazione nazionale e internazionale delle prescrizioni e una standardizzazione delle misure di sicurezza. La standardizzazione comporta ulteriori importanti vantaggi: da un lato, le autorità responsabili dello sviluppo e i servizi incaricati degli acquisti avranno a disposizione chiari requisiti di sicurezza, sui quali potranno fondarsi per implementare la sicurezza nei mezzi informatici; dall'altro, consente di prevedere e pianificare in modo più semplice i costi della sicurezza nell'ambito dei progetti.

d. Neutralità tecnologica

Con l'avanzare della digitalizzazione emergono tecnologie, concetti o forme di lavoro sempre nuovi rilevanti per la sicurezza. Le ordinanze dovranno essere in grado di tenere conto di sviluppi quali «cloud computing», «Internet of Things», «intelligenza artificiale» o «quantum computing» senza dovere essere continuamente adeguate. A livello di ordinanza occorre quindi stabilire innanzitutto principi, compiti, competenze e responsabilità. Le direttive imposte dalla tecnologia dovranno essere definite a livello di istruzioni e standard tecnici.

e. Consentire la digitalizzazione

Nei progetti legislativi si dovrà tenere conto fin dall'inizio delle esigenze della digitalizzazione. In occasione della verifica da un punto di vista giuridico o di una ridefinizione di compiti, processi e procedure, occorrerà garantire che le nuove prescrizioni permettano la digitalizzazione.

2.3 Ordinanza sulla sicurezza delle informazioni (OSIn)

a. Oggetto

La nuova ordinanza sulla sicurezza delle informazioni (OSIn) sostituisce l'ordinanza sui ciber-rischi del 27 maggio 2020[5] (OCiber) e l'ordinanza sulla protezione delle informazioni del 4 luglio 2007[6] (OPrI). L'OSIn disciplina la gestione della sicurezza delle informazioni, la protezione delle informazioni classificate, la sicurezza informatica e le misure per la sicurezza personale e fisica. Definisce i compiti, le competenze e le responsabilità nell'Amministrazione federale e nell'esercito in questo ambito.

[4] RS **172.010**
[5] RS **120.73**
[6] RS **510.411**

b. Campo d'applicazione

L'OSIn si applica al Consiglio federale, all'Amministrazione federale e all'esercito. Le unità amministrative dell'Amministrazione federale decentralizzata di cui all'articolo 7*a* dell'ordinanza del 25 novembre 1998[7] sull'organizzazione del Governo e dell'Amministrazione (OLOGA) sono assoggettate alla LSIn e all'OSIn solamente se trattano informazioni classificate della Confederazione, se accedono a mezzi informatici dell'Amministrazione federale centrale o se fanno gestire i propri mezzi informatici dai fornitori di prestazioni della Confederazione. In questi casi esse non devono applicare la LSIn e l'OSIn nella loro integralità, bensì soltanto le disposizioni che garantiscono il trattamento di informazioni classificate o la sicurezza dei mezzi informatici. Lo stesso vale per le organizzazioni di cui all'articolo 2 capoverso 4 LOGA alle quali vengono attribuiti compiti amministrativi ma che sono al di fuori dell'Amministrazione federale. La Cancelleria federale (CaF) e i dipartimenti possono nondimeno assoggettare all'intera LSIn unità amministrative decentralizzate che svolgono costantemente attività sensibili sotto il profilo della sicurezza.

L'OSIn si applica, per analogia, all'Assemblea federale, ai tribunali della Confederazione, al Ministero pubblico della Confederazione e alla sua Autorità di vigilanza nonché alla Banca nazionale svizzera qualora non emanino proprie prescrizioni.

c. Collaborazione con i Cantoni

Nella misura in cui i Cantoni trattano informazioni classificate della Confederazione o accedono ai mezzi informatici della Confederazione, si applicano le relative prescrizioni della LSIn e dell'OSIn. Tra queste ultime rientrano anche i relativi requisiti minimi del servizio specializzato della Confederazione per la sicurezza delle informazioni, in particolare le prescrizioni e i requisiti tecnici minimi per la protezione di base IT nell'Amministrazione federale nonché per la protezione delle informazioni classificate. Come sinora, i Cantoni dovranno soddisfare i requisiti di sicurezza che l'ufficio federale responsabile del mezzo informatico ha stabilito in applicazione delle direttive della LSIn e dell'OSIn. Essi possono tuttavia esentarsi dalle direttive del diritto federale se garantiscono di propria iniziativa una sicurezza delle informazioni equivalente. Ciò presuppone che essi emanino proprie prescrizioni di sicurezza, allineate agli standard federali, che applicano nel proprio ambito di competenza. I Cantoni non sono tenuti ad attuare un sistema di gestione della sicurezza delle informazioni (SGSI).

d. Gestione della sicurezza delle informazioni

Tutte gli uffici, le segreterie generali, i gruppi e la CaF sono tenuti ad attuare la propria sicurezza delle informazioni tramite un SGSI. Un SGSI non è un sistema informatico, bensì uno strumento di gestione che serve alla pianificazione, all'attuazione, alla verifica e al miglioramento sistematici della sicurezza delle informazioni. Esso comprende le prescrizioni, le procedure, le misure e i controlli necessari a tal fine e permette di vedere chi, all'interno dell'organizzazione, svolge quali compiti, e detiene quali competenze e responsabilità. Con «SGSI» si rinvia implicitamente alla norma ISO/IEC 27001, che vale quale standard sia nel settore privato sia, sempre più, nelle amministrazioni pubbliche. Diversi uffici e dipartimenti hanno già deciso di attuare la propria sicurezza delle informazioni sistematicamente secondo la norma ISO. Alcuni di essi sono certificati ufficialmente. Agli uffici, segreterie generali, gruppi e CaF l'OSIn chiede unicamente un SGSI *light*: ciò significa che non devono attuare la norma ISO completa, ma solamente i processi di gestione più importanti, che figurano nell'OSIn. Non è richiesta una certificazione esterna. Le unità amministrative e i dipartimenti possono tuttavia fissare un livello di ambizione più elevato.

e. Protezione di informazioni classificate e sicurezza informatica

I criteri per la classificazione delle informazioni e per l'attribuzione dei mezzi informatici ai vari livelli di sicurezza vengono allineati ai parametri della gestione dei rischi della Confederazione, motivo per cui in futuro quest'ultima eseguirà un numero minore di classificazioni. Per loro stessa natura, i criteri sono formulati in modo aperto e dovranno essere interpretati. Per l'attuazione si realizzeranno strumenti ausiliari.

Per quanto riguarda le misure concrete adottate per la protezione delle informazioni classificate e per la garanzia della sicurezza informatica, l'OSIn riprende in gran parte le normative esistenti dell'OPrI e dell'OCiber. Le direttive dettagliate, compresi i requisiti tecnici attualmente mancanti, per

[7] RS **172.010.1**

il trattamento elettronico delle informazioni classificate, verranno elaborate adeguandole agli standard dell'Unione europea e della NATO.

f. Certificazione in materia di sicurezza di strumenti informatici

L'OSIn introduce la possibilità di far certificare la sicurezza dei sistemi d'informazione. Una certificazione in materia di sicurezza è richiesta all'estero e nella collaborazione internazionale quando bisogna trattare informazioni protette di un'autorità (o di uno Stato) in un sistema di un'altra autorità (o di un altro Stato). La certificazione conferma che il sistema ricevente soddisfa i requisiti di sicurezza prestabiliti e che i rischi residui sono sostenibili secondo lo stato della tecnica. L'OSIn colma così una lacuna che rendeva difficile la cooperazione internazionale nel settore della sicurezza. Contrariamente alla maggior parte dei Paesi, che per il trattamento elettronico delle informazioni classificate esigono la certificazione, nell'OSIn la certificazione è richiesta solamente se è necessaria per la cooperazione nazionale o internazionale.

g. Sicurezza delle persone

L'assunzione della responsabilità dei rischi per la sicurezza relativi a persone è un compito di condotta permanente. Il nuovo articolo 20*a* della legge del 24 marzo 2000[8] sul personale federale (LPers) introdotto con la LSIn autorizza il datore di lavoro, se necessario per tutelare i suoi interessi, a esigere dai candidati a un impiego e dagli impiegati che presentino un estratto del casellario giudiziale e del registro delle esecuzioni. La prassi ha mostrato che, dopo avere superato un controllo di sicurezza relativo alle persone (CSP), è piuttosto raro che si affronti di nuovo la questione dei rischi per la sicurezza riferiti a persone. Ai sensi di una gestione a posteriori (cosiddetta *«after-care»*) usuale a livello internazionale, i collaboratori che sono stati sottoposti a CSP devono pertanto notificare al proprio datore di lavoro circostanze derivanti dal proprio contesto privato e professionale che possono minacciare la sicurezza (p. es. indebitamento nel casinò, contesti relazionali problematici o viaggi in particolari Paesi). Per i collaboratori queste situazioni possono risultare molto pesanti sotto il profilo psicologico. È parte dell'obbligo di tutela del datore di lavoro ai sensi dell'articolo 4 capoverso 2 lettera g LPers che esso ascolti i propri dipendenti e cerchi assieme a loro di ridurre l'esposizione al rischio. La gestione di un rischio eventualmente accresciuto rimane in definitiva compito del datore di lavoro. Questi può esigere dai collaboratori anche prima che sia trascorso il termine previsto per la ripetizione del CSP estratti ai sensi dell'articolo 20*a* LPers. A seconda del singolo caso una simile notifica può anche portare a una ripetizione straordinaria del CSP.

h. Responsabili della sicurezza delle informazioni e incaricati della sicurezza delle informazioni

Una novità importante nell'OSIn riguarda le direzioni degli uffici. L'ordinanza trasferisce a loro compiti, competenze e responsabilità concreti nell'ambito della sicurezza delle informazioni che, in caso di bisogno, potranno delegare a un membro della loro direzione (responsabile della sicurezza delle informazioni). I responsabili della sicurezza delle informazioni vigilano sul SGSI dell'ufficio e prendono tutte le decisioni importanti nell'ambito della sicurezza delle informazioni. Le attività di vigilanza operativa sono compito degli incaricati della sicurezza delle informazioni secondo l'articolo 37 OSIn. Con l'OSIn gli attuali ruoli degli «incaricati della sicurezza informatica» e degli «incaricati della protezione delle informazioni» vengono riuniti nel nuovo ruolo degli «incaricati della sicurezza delle informazioni». I loro compiti vengono precisati di conseguenza e completati con l'esercizio del SGSI.

Secondo articoli 37, 38, 41 e 42 LOGA, i dipartimenti sono responsabili della gestione, del coordinamento e della vigilanza della sicurezza delle informazioni nel dipartimento. Essi definiscono in particolare la politica in materia di sicurezza delle informazioni e l'organizzazione della sicurezza del dipartimento. La responsabilità operativa per la sicurezza va assunta dal segretario generale, sempreché il capo di dipartimento non decida altrimenti. Come è avvenuto finora, gli incaricati della sicurezza delle informazioni svolgeranno i compiti di coordinamento e di vigilanza operativi (cfr. art. 81 LSIn).

i. Servizio specializzato della Confederazione per la sicurezza delle informazioni

La LSIn crea un servizio specializzato della Confederazione per la sicurezza delle informazioni. L'articolo 83 LSIn ne definisce i compiti, prevalentemente di supporto e di coordinamento, in vista della collaborazione con le autorità assoggettate indipendenti dal Consiglio federale. L'OSIn definisce i compiti per l'ambito di competenza del Consiglio federale. Il servizio specializzato deciderà

[8] RS **172.220.1**

per l'Amministrazione federale e l'esercito le necessarie direttive organizzative, tecniche, edili e riguardanti il personale per garantire la sicurezza delle informazioni secondo lo stato della tecnica. Supporterà inoltre la CaF e i dipartimenti nella gestione della sicurezza. Nell'ambito delle relazioni internazionali assolverà il ruolo di autorità di sicurezza nazionale della Svizzera (cfr. in merito il messaggio LSIn, n. 5.2. e l'art. 42 cpv. 3 OSIn). Il servizio specializzato della Confederazione per la sicurezza delle informazioni farà parte della Segreteria di Stato della politica di sicurezza (SEPOS) in seno al DDPS. Assumerà i compiti dell'Ufficio federale per la cibersicurezza (UFCS) in merito all'autoprotezione della Confederazione (direttive e consulenza).

L'UFCS si concentrerà sulla protezione della Svizzera dai ciber-rischi. Con l'introduzione di un obbligo di segnalare ciberincidenti nella LSIn, l'UFCS potenzierà le proprie prestazioni a favore delle infrastrutture critiche, dell'economia e della popolazione. Continuerà tuttavia a fornire consulenza e a sostenere la CaF, i dipartimenti e gli uffici nelle questioni di cibersicurezza, compreso quando emanano direttive tecniche. Con la modifica della LSIn, anche le autorità federali sono tenute a segnalare ciberincidenti all'UFCS. Nella misura in cui i dipartimenti e gli uffici non sono in grado di gestire un incidente, l'UFCS li assisterà o, d'intesa con il servizio specializzato della Confederazione per la sicurezza delle informazioni, assumerà persino la direzione.

Poiché con l'entrata in vigore della LSIn il servizio specializzato della Confederazione per la sicurezza delle informazioni non sarà ancora operativo, fino alla metà del 2025 l'UFCS continuerà ad assumere i compiti sinora svolti nell'ambito dell'autoprotezione della Confederazione (sicurezza informatica della Confederazione).

2.4 Modifica dell'ordinanza sui sistemi di gestione delle identità e sui servizi di elenchi della Confederazione (OIAM)

Finora l'OIAM si è fondata principalmente sulla LOGA. Con gli articoli 24–26 LSIn si crea ora una base legale formale specifica sulla quale l'OIAM si baserà da qui in avanti. In base all'articolo 20 capoverso 2 LSIn sarà inoltre ammesso, a determinate condizioni, utilizzare ora in generale dati biometrici nei sistemi IAM. Di conseguenza, occorre procedere ai necessari adeguamenti nell'OIAM.

In quanto parte del servizio standard eIAM, l'Amministrazione federale ha sviluppato un servizio di autenticazione per l'accesso alle sue applicazioni tecniche e alle prestazioni di servizio di e-government. Questo servizio si è dimostrato valido e, fondandosi sulla legge federale concernente l'impiego di mezzi elettronici per l'adempimento dei compiti delle autorità (LMeCA), sarà messo a disposizione anche dei Cantoni interessati (e dei loro Comuni) per l'integrazione con le loro applicazioni. Di conseguenza, nell'OIAM occorre procedere alle modifiche necessarie.

Nell'ambito di questo atto normativo, all'OIAM vengono apportate soltanto le modifiche necessarie in virtù della LSIn e della LMeCA. L'ulteriore fabbisogno di adeguamenti dell'OIAM individuato non è invece parte di questo atto normativo, ma è oggetto di una revisione totale di cui la CaF si sta occupando.

2.5 Ordinanza sui controlli di sicurezza relativi alle persone (OCSP)

a. In generale

Con l'adozione della LSIn il legislatore ha ripreso in questa legge il disciplinamento dei CSP dalla legge federale del 21 marzo 1997[9] sulle misure per la salvaguardia della sicurezza interna (LMSI). Nel contempo le disposizioni legali sono state adeguate alle odierne esigenze della sicurezza delle informazioni. Per motivi inerenti ai controlli al di fuori della sicurezza delle informazioni (p. es. la lotta alla corruzione) sono state create basi in altre leggi. Questo ammodernamento del diritto dei CSP deve anche servire a rafforzare l'efficacia dei CSP, ampliando la gamma di dati a cui possono accedere i servizi specializzati CSP per la valutazione del rischio per la sicurezza. Il Consiglio federale vuole per contro che con il diritto il CSP venga riservato a funzioni che possono effettivamente rappresentare un rischio notevole per la Confederazione. In futuro si svolgerà quindi un numero nettamente inferiore di CSP. I CSP dovranno essere gestiti tempestivamente in modo professionale utile con le risorse esistenti. Le principali modifiche al quadro giuridico dei CSP sono contenute nella stessa LSIn.

[9] RS **120**

b. Oggetto

La nuova ordinanza sui controlli di sicurezza relativi alle persone (OCSP) riassume in un unico atto normativo le disposizioni esecutive concernenti i vari controlli riferiti a persone. Sostituisce l'ordinanza del 4 marzo 2011[10] sui controlli di sicurezza relativi alle persone (OCSP), l'ordinanza del 9 giugno 2006[11] sui controlli di sicurezza relativi alle persone nell'ambito degli impianti nucleari (OCSPN) e tutte le altre ordinanze dipartimentali sui controlli di sicurezza relativi alle persone[12].

Sotto il profilo materiale l'ordinanza disciplina sia i CSP secondo la LSIn sia tutti gli altri controlli nonché tutte le altre valutazioni e verifiche che, pur non essendo previsti nella LSIn, vengono però effettuati in base alla procedura dei CSP secondo la LSIn. Tuttavia, a prescindere dalla loro denominazione o dal motivo del controllo, in tutti i controlli si valuterà sempre se la persona interessata è affidabile nell'esercizio dell'attività determinante. All'interno degli stessi livelli di controllo verranno raccolti gli stessi dati e si applicherà lo stesso metodo di valutazione.

c. Campo d'applicazione

L'OCSP si applica, in linea di principio, a tutte le autorità e organizzazioni sottoposte alla LSIn. Per le unità amministrative decentralizzate e le organizzazioni con compiti amministrativi ai sensi dell'articolo 2 capoverso 4 LOGA il campo d'applicazione è limitato: soltanto quelle che rientrano nel campo d'applicazione dell'OSIn rientreranno, per quanto riguarda i CSP ai sensi della LSIn, anche in quello dell'OCSP. Le unità amministrative decentralizzate contemplate dal campo d'applicazione della LPers potranno parimenti essere interessate dalle verifiche dell'affidabilità di cui al suo articolo 20*b* e, in tale contesto, rientrare nel campo d'applicazione dell'OCSP.

L'OCSP si applica anche alle autorità federali assoggettate ai sensi dell'articolo 2 capoverso 1 LAIn indipendenti dal Consiglio federale. Nell'articolo 48 LAIn il legislatore ha infatti conferito al Consiglio federale la competenza esclusiva di disciplinare le modalità della procedura di esame e dell'organizzazione dei servizi specializzati CSP. Le autorità assoggettate rimarranno invece competenti per l'allestimento dei propri elenchi delle funzioni o per la designazione dei servizi promotori e decisori.

d. Snellimento dei motivi del controllo

La nuova normativa limita i motivi per l'esecuzione di CSP. Le funzioni attribuite al massimo livello di controllo, ossia il controllo di sicurezza ampliato, dovranno rimanere l'eccezione. Vi è tuttavia il rischio che, in pratica, la soglia giuridica per i controlli venga abbassata se gli uffici non dispongono di alcun altro strumento per verificare l'affidabilità dei loro dipendenti. Il nuovo articolo 20*a* LPers offre a tal fine ai datori di lavoro i mezzi appropriati.

e. Elenchi delle funzioni

Per tenere il numero dei controlli entro il limite auspicato nell'allestire e nell'aggiornare gli elenchi delle funzioni in cui figurano le funzioni da controllare in futuro occorrerà controllare meglio la legalità delle iscrizioni. Il DDPS gestirà quindi a livello centrale gli elenchi delle funzioni e li aggiornerà costantemente su richiesta dei dipartimenti e della CaF.

Gli elenchi delle funzioni per i quali sarà necessario un CSP secondo la LSIn sono sensibili dal punto di vista della sicurezza delle informazioni. Sono intesi a fornire una panoramica dell'insieme delle funzioni svolte dall'Amministrazione e dall'esercito che hanno accesso a informazioni classificate o che gestiscono o amministrano sistemi critici della Confederazione. Sebbene gli elenchi non conterranno alcun nome dei titolari delle funzioni, nell'era dei media sociali è semplice per un potenziale aggressore collegare una funzione a un nome ottenendo così un obiettivo di spionaggio o di sabotaggio. Nell'ambito dell'esercito gli elenchi delle funzioni dettagliati possono inoltre consentire di trarre conclusioni sull'organizzazione di dettaglio dell'esercito, non pubblicata. Pertanto, fondandosi sull'articolo 6 della legge sulle pubblicazioni ufficiali del 18 giugno 2004[13] (LPub), non verranno pubblicati gli elenchi delle funzioni che contengono le funzioni da controllare secondo la LSIn. Per gli stessi motivi, anche gli elenchi delle funzioni secondo la legge del 23 marzo 2007[14] sull'approvvigionamento elettrico (LAEl) non saranno pubblicati. Per contro gli elenchi delle funzioni sottoposte a controllo principalmente a titolo di protezione dalla corruzione o per evitare danni di reputazione, continueranno a essere pubblicati.

[10] RS **120.4**
[11] RS **732.143.3**
[12] RS **120.421**–**120.427**
[13] RS **170.512**
[14] RS **734.7**

2.6 Ordinanza sulla procedura di sicurezza relativa alle aziende (OPSAz)

a. In generale

La LSIn (cfr. art. 49–72) introduce la cosiddetta procedura di sicurezza relativa alle aziende (PSA). La PSA ha lo scopo di garantire la sicurezza delle informazioni nell'ambito dell'assegnazione di mandati sensibili sotto il profilo della sicurezza da parte delle autorità federali a imprese (aziende) che non sottostanno direttamente alla loro vigilanza. La PSA serve a verificare l'affidabilità dell'impresa alla quale si intende affidare un mandato. Le aziende che sono sotto l'influenza di servizi informazioni esteri non devono ottenere l'accesso a informazioni sensibili sotto il profilo della sicurezza o a mezzi informatici critici della Confederazione. La PSA consente inoltre di controllare e imporre l'attuazione della sicurezza delle informazioni durante l'esecuzione del mandato.

b. Oggetto e campo d'applicazione

Il nuovo diritto disciplina i dettagli della procedura e sostituisce l'attuale ordinanza del 29 agosto 1990[15] sulla tutela del segreto, limitata a mandati con contenuto classificato dal punto di vista militare. L'OPSAz si applicherà all'insieme delle autorità e delle organizzazioni che rientrano nell'ambito di applicazione della LSIn. Per le unità amministrative dell'Amministrazione federale decentralizzata si applicherà soltanto se esse rientrano anche nel campo d'applicazione dell'OSIn (cfr. n. 2.3 lett. b).

c. Acquisti assoggettati

L'ordinanza definisce gli acquisti per i quali la procedura dovrà essere eseguita in ogni caso. Sono interessati i mandati in cui dovranno essere rese accessibili informazioni classificate SEGRETO nonché gli acquisti di sistemi sensibili nei quali si tratteranno informazioni classificate CONFIDENZIALE di più organizzazioni o che saranno impiegati in più uffici e dipartimenti. Per tutti gli altri acquisti, il servizio specializzato competente per l'esecuzione della procedura di sicurezza relativa alle aziende (servizio specializzato PSA) valuterà con il servizio che assegna il mandato (mandante) se l'esecuzione della procedura è opportuna.

d. Armonizzazione con il diritto in materia di acquisti pubblici

Come la stessa LSIn, la nuova ordinanza presenta numerose interfacce con la legislazione della Confederazione in materia di acquisti pubblici. Durante l'elaborazione dell'avamprogetto esse sono state esaminate e rettificate dettagliatamente in collaborazione con rappresentanti degli uffici specializzati. La corretta esecuzione della PSA presuppone inoltre una stretta collaborazione tra il mandante, il servizio incaricato degli acquisti (servizio d'acquisto) e il competente servizio specializzato PSA. Tale collaborazione deve avere luogo già al momento di scegliere la procedura di aggiudicazione da applicare. In tal modo sarà possibile individuare e ridurre precocemente i rischi legati agli acquisti.

2.7 Termini transitori

Sia la LSIn sia le sue ordinanze d'esecuzione prevedono termini transitori idonei a un passaggio riuscito al nuovo diritto. I seguenti termini transitori si applicano agli uffici, alle segreterie generali, ai gruppi e alla CaF a decorrere dall'entrata in vigore della LSIn:

- 1 anno per definire in un catalogo di classificazione come si devono classificare secondo il nuovo diritto le informazioni nel proprio ambito competenza (cfr. art. 51 cpv. 5 OSIn);
- 2 anni per svolgere un'analisi delle necessità di protezione e classificare i propri mezzi informatici secondo il nuovo diritto (cfr. art. 90 cpv. 2 OSIn);
- 3 anni per:
  - sviluppare il proprio SGSI (cfr. art. 51 cpv. 4 OSIn),
  - verificare il proprio elenco delle funzioni concernente i CSP (cfr. art. 6 cpv. 1 OCSP);
- 6 anni (un ciclo di vita) per attuare le nuove prescrizioni di sicurezza tecniche per tutti i mezzi informatici (cfr. art. 90 cpv. 2 LSIn).

[15] RS **510.413**

3 Commento a singoli articoli

3.1 Ordinanza sulla sicurezza delle informazioni (OSIn)

Ingresso

L'ingresso rimanda a tutte le norme di legge che conferiscono al Consiglio federale una competenza normativa nell'ambito dell'OSIn.

Sezione 1: Disposizioni generali

Art. 1 Oggetto

L'espressione «sicurezza delle informazioni» comprende la sicurezza di tutte le informazioni, inclusi i dati personali secondo la legislazione sulla protezione dei dati, della quale sono responsabili l'Amministrazione federale e l'esercito. L'OSIn disciplina i compiti, le responsabilità, le competenze e le procedure per garantire la sicurezza delle informazioni in seno all'Amministrazione federale e all'esercito che, nell'ambito della gestione della sicurezza delle informazioni, sono necessari alla protezione di informazioni classificate, alla sicurezza informatica e alle misure per la sicurezza personale e fisica. Analogamente alla LSIn (cfr. messaggio LSIn, commento ad art. 1), nemmeno nell'OSIn viene definito il termine «informazione». Quest'ultimo sottintende anche i dati. Quando si intendono dati personali ai sensi della legislazione sulla protezione dei dati, si utilizza ogni volta l'espressione «dati personali».

Il rapporto tra la LSIn e l'abrogata LPD del 19 giugno 1992 (vLPD) è illustrato dettagliatamente nel messaggio concernente la LSIn (cfr. messaggio LSIn, n. 1.2.3 pag. 2589). Gli organi di sicurezza secondo gli articoli 36 segg. OSIn assicureranno il coordinamento con i competenti consulenti per la protezione dei dati nell'ambito del SGSI.

Art. 2 Campo d'applicazione

Capoversi 1–3: l'OSIn si applica al Consiglio federale, all'Amministrazione federale centrale e all'esercito.

In linea di principio, tutte le unità amministrative dell'Amministrazione federale decentralizzata di cui all'articolo 7*a* dell'ordinanza del 25 novembre 1998[16] sull'organizzazione del Governo e dell'Amministrazione (OLOGA) nonché le organizzazioni di cui all'articolo 2 capoverso 4 LOGA, alle quali vengono attribuiti compiti amministrativi ma che sono al di fuori dell'Amministrazione federale, rientrano nel campo d'applicazione della LSIn (cfr. l'art. 2 cpv. 2 [LSIn]). L'articolo 2 capoversi 3 e 4 LSIn conferisce tuttavia al Consiglio federale la competenza di limitare il campo d'applicazione della legge a determinate organizzazioni o di limitarlo ad alcune parti della legge. La legge gli concede un margine di discrezionalità per tenere conto dell'autonomia esecutiva delle unità organizzative interessate. Con il disciplinamento di cui all'articolo 2 capoversi 2 e 3 OSIn il Consiglio federale sfrutta il proprio margine di discrezionalità escludendo dal campo d'applicazione della LAIn le organizzazioni in questione per l'impiego di mezzi informatici propri, indipendentemente dal loro livello di protezione, mentre in altri due settori parziali rimangono assoggettati alla LAIn. Con la limitazione delle disposizioni sulla base dell'articolo 2 capoverso 4 LAIn nell'ambito di competenza del Consiglio federale, per garantire l'autonomia esecutiva e per ragioni di costi ci si concentra sulla sicurezza delle informazioni dell'Amministrazione federale centrale e dell'esercito.

Le unità amministrative dell'Amministrazione federale decentralizzata saranno di conseguenza assoggettate alla LSIn e all'OSIn solamente se trattano informazioni classificate della Confederazione, se accedono a mezzi informatici dell'Amministrazione federale centrale o se fanno gestire i propri mezzi informatici dai fornitori di prestazioni della Confederazione. In questi casi esse non dovranno applicare la LSIn e l'OSIn nella loro integralità, bensì soltanto le disposizioni che garantiscono il trattamento di informazioni classificate o la sicurezza dei mezzi informatici. Lo stesso vale per organizzazioni di cui all'articolo 2 capoverso 4 LOGA alle quali vengono attribuiti compiti amministrativi ma che sono al di fuori dell'Amministrazione federale. Con questa soluzione pragmatica le unità amministrative decentralizzate saranno assoggettate solamente se le loro attività sono suscettibili di rappresentare una minaccia per l'Amministrazione federale centrale.

La CaF e i dipartimenti potranno tuttavia decidere che le unità amministrative decentralizzate loro subordinate debbano essere assoggettate alla LSIn nel suo complesso. Ciò presuppone che tali unità amministrative od organizzazioni svolgano costantemente attività sensibili sotto il profilo

[16] RS **172.010.1**

della sicurezza ai sensi dell'articolo 5 lettera b LSIn. Nel DDPS ciò è il caso, ad esempio, dell'Autorità di vigilanza indipendente sulle attività informative (AVI-AIn), che quotidianamente tratta informazioni classificate «SEGRETO» dei servizi di informazione. L'assoggettamento comporta gli stessi compiti e le stesse responsabilità che gli uffici federali dell'Amministrazione federale centrale ricevono dalla LSIn e dall'OSIn. In particolare, devono anche dotarsi die un SGSI.

Questa ordinanza si applica, per analogia, alle altre autorità assoggettate di cui all'articolo 2 capoverso 1 lettere a nonché c–e LSIn (Assemblea federale, tribunali della Confederazione, Ministero pubblico della Confederazione e la sua Autorità di vigilanza nonché la Banca nazionale svizzera), sempreché suddette autorità non emanino proprie disposizioni esecutive. Se esse si avvalgono di tale possibilità, sono esentate dall'OSIn – ma non dalla LSIn – (cfr. invece l'applicabilità dell'OCSP e dell'OPSAz).

Capoverso 4: quando i Cantoni trattano informazioni classificate della Confederazione, si applicano le disposizioni della sezione 4 di questa ordinanza. Se essi accedono ai mezzi informatici della Confederazione, si applicano loro le disposizioni riguardanti l'attribuzione ai livelli di sicurezza (art. 28), le misure di sicurezza (art. 29), la sicurezza durante l'esercizio (art. 30) e le misure per la protezione fisica (art. 34). Essi possono tuttavia esentarsi dalle direttive del diritto federale se garantiscono di propria iniziativa una sicurezza delle informazioni equivalente. Ciò presuppone che essi emanino proprie prescrizioni di sicurezza, allineate agli standard federali, che applicano nel proprio ambito di competenza. Gli standard federali determinanti sono le norme e i requisiti tecnici per la protezione IT di base (Si001) nonché per la protezione delle informazioni classificate. I Cantoni non sono tenuti ad attuare un SGSI secondo gli articoli 5 segg.

Vi è una «sicurezza delle informazioni equivalente» se misure di sicurezza diverse da quelle previste nell'OSIn secondo lo stato della tecnica conformemente all'articolo 85 capoverso 1 LSIn producono un effetto comparabile e per lo meno altrettanto elevato o forte. I Cantoni valutano in primo luogo a propria discrezione se vi è una sicurezza delle informazioni equivalente.

Nel termine «Cantoni», oltre alle amministrazioni cantonali, sono compresi enti, istituti o fondazioni di diritto pubblico assoggettati al diritto amministrativo del rispettivo Cantone. Da parte loro, i Cantoni devono valutare caso per caso se un'organizzazione o un istituto (p. es. un ospedale, una centrale elettrica o anche un istituto finanziario) è da considerarsi un «Cantone» ai sensi della LSIn o dell'OSIn. Se un'organizzazione cantonale non rientra nel campo d'applicazione della LSIn viene trattata come «terzo» ai sensi dell'articolo 9 LSIn (v. commento ad art 10).

Capoverso 4 lettera b: con «accesso a mezzi informatici» si intendono tutti i tipi di accessi tecnici da parte dei Cantoni ai mezzi informatici della Confederazione. La questione dell'accesso deve essere chiarita in ogni singolo caso. In ultima analisi, è la Confederazione a decidere se vi è un accesso.

Capoverso 5: l'OSIn si applica anche all'esercito. I compiti, le competenze e le responsabilità vengono sono assunti, come sinora, dall'amministrazione militare, cosa che rimarrà invariata con la nuova legislazione.

Sezione 2: Principi

Art. 3 Obiettivi in materia di sicurezza

I mezzi informatici dell'Amministrazione centrale e dell'esercito presentano sempre più interfacce tecniche comuni. Per questa ragione i rischi o le minacce per la singola organizzazione o i rispettivi fornitori non possono essere considerati separatamente. La sicurezza delle informazioni è necessariamente un compito interconnesso che richiede un obiettivo comune e una procedura coordinata.

Il Consiglio federale si adopera affinché la protezione di informazioni e mezzi informatici sia garantita secondo un approccio basato sul rischio. Oggi non basta più attuare la sicurezza semplicemente in base a una lista di controllo. I responsabili devono esercitare una gestione del rischio attiva, conoscere le minacce alla sicurezza delle informazioni e le loro potenziali ripercussioni sulle attività, adeguare il dispendio per minimizzare i rischi alle loro dimensioni ovvero concentrarsi sui rischi maggiori e applicare le misure più efficaci per minimizzare i rischi. Con l'approccio basato sul rischio occorre focalizzarsi non soltanto sui rischi (effetti negativi), ma anche sulle possibilità e opportunità (effetti positivi) di nuove idee, applicazioni o tecnologie. Con «resilienza» si intende la resistenza di un'organizzazione e la rapida ripresa del normale esercizio dopo un incidente legato alla sicurezza.

Art. 4 Responsabilità

Capoversi 1–2: conformemente all'articolo 45 LOGA i direttori dei gruppi e degli uffici sono responsabili di fronte ai loro superiori della direzione delle unità amministrative loro subordinate e dell'esecuzione dei compiti loro affidati. Ciò include la responsabilità per la sicurezza delle informazioni. Finora l'UFCS definiva direttive minime in materia di sicurezza delle informazioni, in particolare la protezione IT di base nell'Amministrazione federale, intese a proteggere l'intera Amministrazione federale e che gli uffici, le segreterie generali e la CAF devono attuare con un margine di manovra limitato. Queste direttive non le esentano tuttavia dalla loro responsabilità di valutare costantemente i rischi e, se necessario, di adottare misure più estese. Per poter garantire questa protezione in tutta l'Amministrazione federale, anche i Cantoni che trattano informazioni classificate della Confederazione o accedono ai suoi mezzi informatici dovranno attenersi a questi requisiti (v. commento ad art. 49).

Capoverso 3: nel trattamento di informazioni o nell'utilizzo di mezzi informatici della Confederazione i collaboratori dovranno rispettare le pertinenti prescrizioni di comportamento. L'assunzione di questa responsabilità presuppone che essi siano istruiti e formati di conseguenza e che dispongano dei mezzi necessari (v. commento ad art. 4 cpv. 4 e ad art. 11 OSIn).

Con «collaboratori dell'Amministrazione federale» si intendono i collaboratori interni ed esterni assoggettati alla facoltà di emanare istruzioni della Confederazione: i collaboratori «interni» sono impiegati della Confederazione ai sensi della LPers; i collaboratori «esterni» sono invece persone impiegate mediante un contratto di fornitura di personale a prestito. Non sono per contro collaboratori della Confederazione persone esercitanti un'attività autonoma o collaboratori di imprese che, ad esempio, in base a un rapporto contrattuale operano a livello di consulenza per la Confederazione o le forniscono prestazioni di servizio o in natura (quali sviluppo di software, potenziamento della rete, costruzione di un locale dei server, assunzione della direzione di progetti ecc.). Queste persone sono considerate «terzi» (v. commento ad art. 10 OSIn). Nel caso di «terzi», la corretta manipolazione degli oggetti da proteggere deve essere assicurata e verificata, se del caso, mediante relativi contratti secondo l'articolo 9 LSIn.

Capoverso 4: anche nell'ambito della sicurezza delle informazioni i superiori di tutti i livelli saranno responsabili dell'istruzione e della formazione conformi alla funzione e improntate alla prassi dei propri collaboratori o dei militari subordinati nonché della verifica del rispetto delle prescrizioni. Spetta così ai superiori spiegare ai propri collaboratori in modo pratico come dovranno gestire le informazioni protette, renderli attenti all'impiego coerente e conforme alle direttive di software di crittografia o assicurarsi che frequentino le formazioni proposte. Riguardo alla responsabilità degli uffici, delle segreterie generali, dei gruppi e della CaF si rimanda al commento ad articolo 11.

Sezione 3: Gestione della sicurezza delle informazioni

Gli articoli 5–15 OSIn definiscono i requisiti minimi per la gestione della sicurezza delle informazioni nell'Amministrazione federale e nell'esercito. Per i compiti fondamentali della sicurezza delle informazioni definisco le rispettive competenze degli uffici, della CaF, dei dipartimenti e del servizio specializzato della Confederazione per la sicurezza delle informazioni. Quest'ultimo emanerà direttive in tal senso e metterà a disposizione gli strumenti ausiliari necessari. L'UFCS fornisce importanti prestazioni a favore della gestione della sicurezza dell'Amministrazione federale, in particolare nella gestione di ciberincidenti (cfr. art. 12).

Art. 5 Sistema di gestione della sicurezza delle informazioni

Capoverso 1: un «SGSI» comprende procedure e norme che illustrano com'è organizzata la sicurezza delle informazioni in un sistema e rende visibile quali compiti, competenze e responsabilità sono riconducibili alle relative persone (v. n. 2.3 lett. d).

Mentre i responsabili della sicurezza delle informazioni delle unità amministrative (cfr. art. 36) garantiscono lo sviluppo, l'esercizio, la verifica e il miglioramento continuo del SGSI, l'esercizio vero e proprio del SGSI spetta agli incaricati della sicurezza delle informazioni delle unità amministrative (cfr. art. 37 cpv. 2 lett. a) su incarico dei responsabili della sicurezza delle informazioni. Secondo l'articolo 51 capoverso 4, un SGSI deve essere realizzato al massimo entro tre anni dall'entrata in vigore dell'OSIn.

Capoverso 2: lo scopo di un SGSI è gestire e migliorare la sicurezza delle informazioni nell'organizzazione. A tal fine occorrono obiettivi concreti in base ai quali la direzione dell'ufficio può valutare

se il SGSI produce gli effetti desiderati Questa definizione e misurazione di obiettivi annuale è un compito direttivo della direzione dell'ufficio.

Capoverso 3: per garantire una certa obiettività e comparabilità nella valutazione dell'attuazione e dell'efficacia del SGSI, è richiesta una verifica periodica eseguita da un servizio indipendente dall'ufficio o dalla CaF oppure eseguita dal dipartimento. Questa verifica indipendente del SGSI garantisce il miglioramento costante della sicurezza nell'ufficio e, al contempo, crea fiducia per i partner dell'ufficio. L'ufficio o la CaF deciderà come gestire i risultati della verifica e quali misure attuare. Il costante processo di miglioramento è fondamentale per garantire la sicurezza delle informazioni. Queste verifiche ne tengono conto.

Anche se la periodicità di tre anni si basa sul ciclo di certificazione ufficiale delle norme ISO (ISO/IEC 27001), l'entità della verifica obbligatoria è tuttavia nettamente meno ambiziosa di quella prevista dallo Standard ISO: non si richiede necessariamente un audit formale ai sensi della norma ISO, sebbene tale audit andrebbe accolto favorevolmente. A seconda del mandato sarà inoltre possibile verificare l'intero SGSI o soltanto determinate sue parti. L'unità amministrativa interessata avrà il potere decisionale sulla scelta di un servizio di controllo indipendente. Queste verifiche potranno essere effettuate dalle strutture di vigilanza interne dei dipartimenti o da un'impresa esterna (cfr. spiegazioni nel messaggio LSIn, pag. 2631).

Capoverso 4: evidenzia lo stretto legame tra il SGSI e la gestione dei rischi della Confederazione, la gestione della continuità operativa e la gestione delle crisi. Si tratta di compiti di gestione che esulano dal campo d'applicazione dell'OSIn, ma che le unità amministrative dovranno allineare e coordinare strettamente tra loro.

Art. 6 Cura delle basi legali e degli obblighi contrattuali

Un registro delle basi legali e degli obblighi contrattuali determinanti nel proprio settore di competenza nell'ambito della sicurezza delle informazioni serve a dimostrare il rispetto delle basi giuridiche rilevanti che, ad esempio, viene controllato nel contesto della misurazione dell'annuale raggiungimento degli obiettivi del SGSI (cfr. art. 5 cpv. 2 o la verifica SGSI secondo l'art. 5 cpv. 3 OSIn). A causa delle crescenti catene di approvvigionamento nell'ambito della sicurezza delle informazioni, è imprescindibile disporre di un riepilogo degli obblighi da assolvere e dei diritti da rivendicare e, non da ultimo, favorire lo sfruttamento delle sinergie di altri contratti esistenti.

Il servizio specializzato offre consulenza alle unità amministrative nelle questioni inerenti alla sicurezza, fra l'altro anche nella cura delle direttive rilevanti per la sicurezza (p. es. istruzioni e linee guida) o dei progetti (p. es. progetti IT rilevanti sotto il profilo della sicurezza) delle unità amministrative o dei dipartimenti.

Art. 7 Inventariazione degli oggetti da proteggere

Capoverso 1: un inventario contiene un elenco di tutti gli oggetti da proteggere di cui all'articolo 7 capoverso 2 in un dato momento (cosiddetta lista dell'inventario).

Capoverso 2: nell'OCiber si trovavano solamente gli «oggetti informatici da proteggere» (cfr. art. 3 lett. h OCiber), che sono coperti dalla lettera b. Tuttavia, le informazioni non vengono sempre elaborate in un unico sistema d'informazione dedicato. Questo è il caso, ad esempio, quando un compito viene svolto nell'ambiente informatico generale della Confederazione o quando le informazioni vengono elaborate in un cloud esterno. Con l'oggetto da proteggere «informazioni» ai sensi della lettera a si esclude pertanto la dipendenza da un determinato mezzo informatico e si valuta soltanto la protezione delle informazioni elaborate per l'adempimento del compito. In linea di principio, però, vengono utilizzati gli stessi criteri e metodi per valutare la necessità di protezione degli oggetti informatici da proteggere. Più oggetti da proteggere identici o connessi tra loro possono anche essere raggruppati in un singolo oggetto da proteggere. Le direttive del servizio specializzato della Confederazione per la sicurezza dell'informazione (cfr. art. 15) preciseranno questo aspetto.

Capoverso 3: soltanto una lista d'inventario aggiornata può fornire la prova costante relativa a tutti gli oggetti da proteggere riguardo alle informazioni secondo le lettere a–g.

Capoverso 3 lettera c: da un lato, il riepilogo dei vincoli contrattuali con terzi (v. commento ad art. 10 cpv. 1 OSIn), ad esempio con fornitori di tecnologie dell'informazione, serve a una gestione dei fornitori funzionante e permette di individuare precocemente le eventuali dipendenze della Confederazione dai fornitori (incl. valutazione del pericolo di grandi rischi). Dall'altro, permette di identificare rischi che per il tramite di questi fornitori possono avere ripercussioni sulla Confederazione.

Capoverso 3 lettera e: l'attuazione delle misure di sicurezza non deve obbligatoriamente essere documentata nell'inventario. Quest'ultimo dovrà però indicare chiaramente almeno dove è visibile questa documentazione e chi è la persona competente.

Capoverso 3 lettera f: v. commento ad articolo 13 in combinato disposto con l'articolo 5 capoversi 2 e 3.

Capoverso 3 lettera g: la possibilità dell'utilizzo condiviso dei relativi oggetti da proteggere fa riferimento al principio *«once only»*. Le unità amministrative decidono a propria discrezione quali oggetti da proteggere verranno condivisi con altre unità amministrative. Se l'oggetto da proteggere contiene dati personali, ovviamente tutte le unità amministrative coinvolte dovranno disporre delle basi legali necessarie per accedere a tali dati e trattarli.

Art. 8 Gestione dei rischi

Capoverso 1: la valutazione dei rischi è una delle basi per una gestione efficace dei rischi e, di conseguenza, per una sicurezza delle informazioni funzionale ed economica (cfr. messaggio LSIn, pag. 2631 seg.). Le direttive sulla protezione IT di base nell'Amministrazione federale offrono una protezione in funzione dei rischi contro un gran numero di minacce. Servono alla sicurezza delle informazioni in rete della Confederazione e devono essere rispettate. Consentono una manutenzione poco onerosa a livello di sicurezza di mezzi informatici che non sono particolarmente sensibili sotto il profilo della sicurezza. In tal caso le unità amministrative non devono neanche eseguire valutazioni dei rischi complesse.

Capoverso 1 lettera a: in tale contesto, la valutazione dei rischi quanto alle loro ripercussioni sugli oggetti da proteggere (cfr. art. 7 cpv. 2) è anche molto tecnico-operativa e dipende dall'esigenza di confidenzialità, disponibilità, integrità e tracciabilità delle informazioni e del sistema informatico.

Capoverso 1 lettera b: il controllo dell'efficacia può ad esempio avvenire mediante test di penetrazione o la raccolta di indicatori rilevanti.

Capoverso 1 lettera c: v. commento ad articolo 6.

Capoverso 1 lettera d: è richiesta una decisione consapevole da parte del responsabile della sicurezza delle informazioni, vale a dire l'accettazione comprovabile di rischi residui sulla base di un accurato processo di analisi e di decisione. La comprovabilità non è legata a una forma determinata. In un contesto digitalizzato sarà così possibile impiegare metodi di comprovabilità tecnologicamente neutri.

Capoverso 3: sono determinanti le istruzioni sulla politica della Confederazione in materia di gestione dei rischi nonché le direttive e i manuali correlati. Gli uffici riferiscono al proprio dipartimento, che successivamente redige un rapporto destinato al Consiglio federale. Il consolidamento avviene tramite l'organo di coordinamento della gestione dei rischi della Confederazione e la Conferenza dei segretari generali (CSG).

Art. 9 Autorizzazione ed elenco delle deroghe

Come avveniva già in passato con l'UFCS, con la messa in vigore dell'OSIn il servizio specializzato della Confederazione per la sicurezza delle informazioni stabilirà in base all'articolo 85 LSIn quali requisiti minimi dovranno essere soddisfatti nel settore della sicurezza delle informazioni. In queste direttive stabilirà anche chi decide in merito alle deroghe al rispetto di direttive minime. In linea di principio verrà ripresa l'attuale procedura dell'OCiber relativa alle autorizzazioni eccezionali.

Art. 10 Collaborazione con terzi

Capoverso 1: sono considerati «terzi» ai sensi della LSIn tutte le autorità, organizzazioni e persone di diritto pubblico o privato che non sono né un'autorità né un'organizzazione assoggettata e che perciò, in linea di principio, agiscono indipendentemente da queste autorità o organizzazioni. Sono considerati terzi anche le unità amministrative decentralizzate, sempreché non siano assoggettate alla LSIn (cfr. messaggio LSIn pag. 2625 seg. e 2632), o determinate organizzazioni che gestiscono infrastrutture critiche (art. 2 cpv. 5 LSIn). La valutazione dei rischi per la sicurezza si rifà alle direttive dell'articolo 8 OSIn.

Capoverso 3: diversi incidenti verificatisi presso partner esterni della Confederazione hanno mostrato che, quando trattano informazioni della Confederazione o le forniscono prestazioni di servizi informatici, questi partner devono rispettare lo stesso standard di sicurezza delle autorità federali. I

contratti con terzi dovranno pertanto stabilire chiari requisiti in materia di sicurezza delle informazioni e di verifica delle prescrizioni. Dovranno, tra l'altro, comprendere l'obbligo di garantire la protezione delle informazioni e dei dati della Confederazione secondo gli standard federali (incl. requisiti in materia di protezione dei dati, cfr. messaggio LSIn ad art. 9) e di segnalare eventi rilevanti per la sicurezza. Nei contratti dovranno figurare anche le modalità della prova dell'attuazione delle direttive di sicurezza e in particolare un diritto di audit della Confederazione.

Art. 11 Formazione e sensibilizzazione

Se l'Amministrazione federale e l'esercito vogliono migliorare in modo duraturo la propria sicurezza, è importante sensibilizzare e formare i propri collaboratori e militari (tra i quali anche i superiori) affinché non soltanto attuino le misure di sicurezza preventive in modo conforme alle prescrizioni, ma siano anche in grado di riconoscere autonomamente pericoli e minacce, di reagire correttamente e di presentare le pertinenti segnalazioni di sicurezza.

In aggiunta agli sforzi dei superiori diretti, che sono principalmente responsabili della formazione adeguata alla funzione dei propri collaboratori (v. commento ad art. 4 cpv. 4), le unità amministrative garantiscono la formazione generale (p. es. campagne di sensibilizzazione e di consapevolezza o corsi di formazione introduttivi a intervalli regolari) per tutto il personale e mettono a disposizione budget, tempo e risorse necessari.

Art. 12 Gestione degli incidenti

Capoverso 1: le unità amministrative sono responsabili della gestione di incidenti legati alla sicurezza e di lacune in materia di sicurezza. Nell'ambito del proprio SGSI dovranno perciò definire nell'ufficio e con i fornitori di prestazioni come notificare e trattare gli incidenti legati alla sicurezza. Con «incidenti legati alla sicurezza» si intendono eventi in cui la sicurezza delle informazioni o le pertinenti direttive di sicurezza vengono violate o sono state violate. È considerata una «lacuna in materia sicurezza» un difetto in un mezzo informatico il cui sfruttamento può violare la sicurezza delle informazioni. È importante stabilire in anticipo chi, in caso di emergenza, decide in merito a misure immediate e chi deve essere consultato o informato nel caso si adottino queste decisioni. Chi detiene la competenza decisionale riguardo a misure immediate deve essere in grado di capire quali sono le ripercussioni sulle attività della misura adottata.

Capoverso 2: questa disposizione è in linea con il diritto attuale (cfr. art. 14 cpv. 4 lett. c OCiber).

Capoverso 3: in relazione allo sviluppo e al funzionamento del SGSI, gli uffici e i loro dipartimenti nonché la CaF sono abilitati a gestire gli incidenti in modo professionale secondo un approccio sistematico. Sia il servizio specializzato della Confederazione sia l'UFCS possono fornire consulenza alle unità amministrative e ai dipartimenti o assisterli in tale compito. L'UFCS continuerà a concentrarsi sulla consulenza nel settore della cibersicurezza e il servizio specializzato, da parte sua, offrirà un'ampia consulenza generale nel settore della gestione della sicurezza e sarà inoltre in grado di rispondere a questioni specialistiche nei settori diritto della sicurezza, sicurezza aziendale o sicurezza delle persone. Con la disposizione potestativa si sottolinea che il servizio specializzato della Confederazione per la sicurezza delle informazioni e l'UFCS possono fornire sostegno ma, appunto, non sono tenuti a farlo. Il sostegno ai suddetti servizi viene fornito, in linea di massima, su richiesta delle unità amministrative o dei dipartimenti. Ovviamente il sostegno verrà fornito in funzione della criticità e dell'importanza dell'incidente e delle risorse disponibili.

Capoversi 5–7: se un incidente raggiunge o potrebbe raggiungere una dimensione superiore, gli uffici e i dipartimenti dovranno informare il servizio specializzato. I criteri di cui al capoverso 5 riguardano incidenti che possono pregiudicare non soltanto gli interessi e i compiti dell'ufficio o del dipartimento, ma dell'intera Amministrazione federale. L'importanza politica elevata dell'incidente dipende sia dalle informazioni, dai sistemi informatici o dalle organizzazioni coinvolti, sia dalle circostanze dell'incidente. L'importanza politica di un incidente tende a modificarsi dinamicamente e sarà oggetto di verifica assieme alla persona responsabile della sicurezza delle informazioni del rispettivo ufficio o dipartimento.

Quando un incidente è «critico» in base ai criteri del capoverso 5, il servizio specializzato verifica con l'unità amministrativa interessata, e anche con l'UFCS qualora l'incidente riguardi la cibersicurezza, se sia necessario fornire supporto o addirittura assumerne la direzione. Se indugiare può essere rischioso, la decisione verrà presa molto rapidamente. A seconda della natura dell'incidente o della vulnerabilità scoperta, potrà essere il servizio specializzato o l'UFCS ad assumere la dire-

zione. Con «direzione» si intende la competenza decisionale operativa. Tuttavia, l'unità amministrativa o il dipartimento interessato rimarrà responsabile della sicurezza delle informazioni (v. commento ad art. 4). Se il servizio specializzato o l'UFCS assume la direzione, potrà per esempio disporre misure immediate o ricorrere all'impiego di specialisti a scopo di sostegno. I relativi costi saranno a carico dell'unità amministrativa responsabile o del dipartimento e assunti d'intesa con essi.

Con l'introduzione dell'obbligo di segnalare in caso di ciberincidenti (v. n. 2.1), come tutte le altre infrastrutture critiche le autorità federali devono presentare una notifica all'UFCS se sono vittime di un ciberattacco. Il DDPS farà sì che la notifica all'UFCS e al servizio specializzato venga coordinata e che i processi nella gestione degli incidenti legati alla sicurezza siano chiari, efficienti ed efficaci. In merito al trattamento dei dati nell'ambito della gestione degli incidenti cfr. gli articoli 44–46 OSIn.

Art. 13 Pianificazione dei controlli e degli audit

La mancanza di controlli e di audit è una lacuna significativa nella gestione della sicurezza delle informazioni dell'Amministrazione federale e dell'esercito. Solo con audit adeguati, le organizzazioni potranno conoscere lo stato della sicurezza delle proprie informazioni, quali sono i rischi e quali sono le eventuali misure correttive necessarie (cfr. messaggio LSIn, pag. 2590). Questo articolo prevede pertanto che le unità amministrative e i dipartimenti stabiliscano annualmente quali controlli e audit basati sul rischio effettueranno l'anno successivo e per quale motivo. Se si pianifica una verifica del SGSI ai sensi dell'articolo 5 capoverso 3 OSIn, occorrerà inserire tale verifica nel piano dei controlli e degli audit. Quest'ultimo e le relative risorse devono essere approvati dai responsabili della sicurezza delle informazioni dell'unità amministrativa (cfr. art. 36 cpv. 3 lett. d). L'articolo 13 non specifica quanti controlli e audit dovranno essere effettuati; la decisione spetta unicamente all'unità amministrativa. Con il piano dei controlli e degli audit obbligatorio la direzione dell'ufficio dovrà prendere una decisione positiva e comprensibile.

Con «controlli», in questa sede si intendono verifiche precise con un campo d'applicazione limitato che si possono svolgere in modo informale con un dispendio contenuto e spesso sono più economici rispetto agli audit. Per esempio, un ufficio o la CaF può pianificare il controllo dell'attualità della documentazione di sicurezza o il controllo del rispetto della *«Clean Desk Policy»*. Gli «audit» seguono invece una procedura formalizzata e sono svolti spesso da un organismo indipendente. Durante un audit si esamina se i sistemi, i processi o i sistemi di gestione rispettano le direttive vigenti o gli standard e le norme richiesti.

Capoverso 2: i controlli e gli audit riguardano anche il rispetto delle prescrizioni da parte di terzi, per esempio di fornitori. Tutti i contratti con terzi dovranno prevedere un diritto di audit per la Confederazione (cfr. anche art. 10 cpv. 3). Se è previsto un controllo di questo tipo e se il terzo dispone di una dichiarazione di sicurezza aziendale (cfr. art. 61 segg. LSIn), un coordinamento con il servizio specializzato PSA responsabile della procedura di sicurezza relativa alle aziende provvederà affinché la Confederazione impieghi le proprie risorse in modo sensato e non controlli più volte gli stessi elementi presso un partner.

Capoverso 3: su richiesta delle autorità federali, il servizio specializzato della Confederazione per la sicurezza delle informazioni potrà eseguire verifiche (cfr. art. 83 cpv. 1 lett. c LSIn). Il livello di ambizione viene consapevolmente mantenuto basso e per il momento si rinuncia a potenziare la capacità di audit di questo servizio. Da anni il Controllo federale delle finanze (CDF) svolge infatti audit di elevata qualità ed esami trasversali nell'ambito della sicurezza delle informazioni. Questi audit si incentrano sui rischi su cui si focalizza il servizio specializzato della Confederazione per la sicurezza delle informazioni e coprono così il fabbisogno a livello di Confederazione.

Art. 14 Rapporti

Per conseguire un miglioramento duraturo della sicurezza delle informazioni in seno alla Confederazione, sono necessari una verifica critica continua dell'efficacia della sicurezza delle informazioni e un costante adeguamento di misure opportune nell'ambito della sicurezza. Il rapporto comprenderà, in particolare, lo stato e l'efficacia del SGSI delle unità amministrative, lo stato degli oggetti da proteggere, dell'attuazione delle misure di sicurezza e dell'assunzione dei rischi residui, lo stato della formazione, i dati concernenti i controlli di sicurezza relativi alle persone e le procedure di sicurezza relative alle aziende svolti per la CaF o il dipartimento, le conoscenze ottenute dagli incidenti legati alla sicurezza e dalle lacune in materia di sicurezza e le relative misure di miglioramento adottate e previste come pure le conoscenze derivanti dai controlli e dagli audit e le relative

misure di miglioramento adottate e previste. Il servizio specializzato della Confederazione per la sicurezza delle informazioni stabilisce le modalità per la stesura dei rapporti.

Capoverso 3: secondo l'articolo 83 capoverso 1 lettera h LSIn, anche il rapporto al Consiglio federale rileva lo stato della sicurezza presso le altre autorità assoggettate, ragion per cui dovrà essere coordinato con esse. Ciò avverrà in primo luogo nell'ambito della Conferenza di cui all'articolo 82 LSIn.

Art. 15 Direttive concernenti la gestione della sicurezza delle informazioni

Questo articolo è retto dall'articolo 85 LSIn. Il servizio specializzato riceve dal Consiglio federale il compito di emanare per l'Amministrazione federale e l'esercito le istruzioni per la gestione della sicurezza delle informazioni (art. 5–14). In merito alla disposizione transitoria cfr. articolo 50 capoverso 6.

Sezione 4: Informazioni classificate

Gli articoli 18–20 descrivono i presupposti materiali per la classificazione delle informazioni (cfr. messaggio LSIn, commento ad art. 13). Essi sono in gran parte in sintonia con i criteri applicati nell'ambito della gestione dei rischi della Confederazione per la valutazione dell'entità dei danni di un evento. Rispetto all'attuale OPrI sono stati innalzati i valori soglia per la classificazione AD USO INTERNO, CONFIDENZIALE e SEGRETO. Tale aumento consentirà in futuro di classificare le informazioni in modo più mirato, a fronte di una loro migliore protezione.

Art. 16 Principi

Capoverso 1: la classificazione è obbligatoria, purché siano soddisfatti i relativi criteri di cui agli articoli 18 segg. Deve essere rispettato rigidamente il principio del *«need-to-know»* di cui all'articolo 14 LSIn. La classificazione di materiale è un caso d'applicazione della classificazione di informazioni per le quali, in linea di principio, valgono gli stessi metodi di valutazione e le stesse misure di protezione (incl. prescrizioni ai sensi di OCSP e OPSAz; cfr. messaggio LSIn, pag. 2633).

Capoverso 2: dalla raccolta di informazioni classificate o informazioni non classificate o di supporti di dati (quali documenti cartacei e dispositivi di archiviazione con file di testo, di immagini o sonori) può risultare una collezione che presenta una necessità di protezione superiore rispetto a un'informazione isolata contenuta nella stessa. Questo è il caso tipico delle banche dati.

Se in base al principio di trasparenza un documento ufficiale viene consegnato, ad esempio, a un giornalista non dipende dall'eventuale menzione di classificazione di quest'ultimo, bensì si determina unicamente in virtù dei criteri della legge del 17 dicembre 2004[17] sulla trasparenza (LTras). I criteri che giustificano una classificazione di informazioni sono armonizzati con quelli di cui all'articolo 7 LTras in virtù dei quali il diritto di accesso a un documento ufficiale è limitato, differito o negato. Determinante in ogni caso è la giurisprudenza del Tribunale federale sulla nozione di segreto, in particolare sulla distinzione tra segreto formale e segreto materiale.

Peraltro, le leggi cantonali in materia di trasparenza non si applicano, in linea di principio, ai documenti ufficiali della Confederazione (p. es. informazioni classificate della Confederazione). Domande di accesso in tal senso sono rette esclusivamente dal diritto federale. Se, per esempio, un Cantone riceve una domanda di accesso a un'informazione classificata della Confederazione, dovrà essere consultato il servizio federale competente per la protezione dell'informazione classificata.

Art. 17 Servizi incaricati della classificazione

Capoverso 1: gli uffici, le segreterie generali, i gruppi, la CaF e i dipartimenti (o gli organi che agiscono per loro conto) sono i servizi che, nel proprio all'ambito di competenza, possono valutare al meglio per quali informazioni sussiste un interesse alla protezione oggettivamente giustificato. Essi rappresentano quindi i servizi veri e propri incaricati della classificazione dotati di ampie competenze per la classificazione, la modifica o la soppressione della classificazione (art. 12 cpv. 2 LSIn). Il capoverso 1 li incarica di elencare in un catalogo di classificazione le informazioni più complete possibili per il loro ambito di competenza. Ciò include anche la durata prevista della classificazione. Poiché queste informazioni vengono costantemente elaborate, nella maggior parte dei casi è possibile stabilire in anticipo fino a quando l'informazione va classificata a quale livello. L'ordinanza non specifica un termine minimo o massimo. Fissare il termine di classificazione non dispensa

[17] RS **152.3**

dall'obbligo di cui all'articolo 25 di verificare ogni cinque anni, nel caso concreto, la necessità di protezione di un determinato documento.

I cataloghi di classificazione delle unità amministrative sono materialmente vincolanti per i collaboratori. Dovranno classificare le informazioni ivi contenute in modo formale apponendo un contrassegno formale di classificazione al documento (cfr. cpv. 5). Se la classificazione è manifestamente errata, si deve applicare la normativa dell'articolo 24 OSIn.

Capoverso 2: con questa verifica si intende garantire che nell'allestire i cataloghi di classificazione i criteri legali per la classificazione all'interno dell'Amministrazione federale vengano applicati secondo parametri comparabili. La competenza decisionale finale degli uffici, segreterie generali, gruppi, CaF e dipartimenti viene mantenuta.

Capoverso 3: nell'Amministrazione federale e nell'esercito vengono trattate molte informazioni che non possono essere assegnate specificamente a un ufficio o a un dipartimento (p. es. protezione di oggetti e persone, mezzi informatici, affari del Consiglio federale). Il servizio specializzato della Confederazione per la sicurezza delle informazioni si dovrà occupare di questo catalogo di classificazione generale vincolante.

Capoverso 4: i cataloghi di classificazione secondo i capoversi 1 e 3 non contengono elenchi esaustivi. Chi tratta informazioni prima o poi sarà confrontato con la situazione in cui, pur valutando un'informazione degna di protezione, non la troverà però nei cataloghi. In questo caso i collaboratori della Confederazione e i militari (lett. a) hanno l'obbligo di inserire ex novo l'informazione in questione sia per analogia con un'iscrizione in un catalogo di classificazione sia di classificarla direttamente in base ai criteri di classificazione di cui agli articoli 18–20. Lo stesso obbligo si applica ai mandanti che affidano a terzi il trattamento di informazioni degne di protezione (lett. b).

Capoverso 5: in generale, occorre garantire che l'informazione degna di protezione venga protetta esattamente a partire dal momento in cui è percepibile visivamente e/o acusticamente. Ciò è il caso non appena questa informazione si trova su un supporto di dati. È quindi importante che la protezione intervenga direttamente alla fonte e che venga effettuata da tutte le persone che si occupano del trattamento mediante il contrassegno formale (apposizione della menzione di classificazione). Una forma particolare di questo contrassegno si applica allo scambio verbale di informazioni, richiamando in precedenza l'attenzione sul fatto che a breve le informazioni classificate verranno comunicate oralmente. Le persone di cui al capoverso 5 non hanno il diritto di abbassare o sopprimere una classificazione dell'informazione. Questa competenza rimane sempre appannaggio degli uffici, della CaF e dei dipartimenti.

Art. 18 Livello di classificazione «ad uso interno»

Affinché si giustifichi una classificazione AD USO INTERNO sono necessari due presupposti cumulativi: la conoscenza di informazioni da parte di persone non autorizzate deve poter comportare un *potenziale* pregiudizio causale per gli interessi pubblici della Svizzera e il pregiudizio non può essere semplicemente trascurabile, senza che vi siano indicazioni concrete per un danno finanziario. Questi interessi pubblici vengono riportati nell'articolo 1 capoverso 2 lettere a–d LSIn; di per sé, la lettera e non costituisce appunto un interesse alla protezione proprio dell'istituzione federale (cfr. messaggio LSIn, pag. 2635 seg.). Queste informazioni sono protette per legge o convenzione; il segreto d'ufficio di cui all'articolo 320 del Codice penale svizzero del 21 dicembre 1937[18] (CP) o la LTras nei casi previsti in queste leggi assicurano, parimenti, la protezione di determinate informazioni.

Art. 19 Livello di classificazione «confidenziale»

Affinché si giustifichi una classificazione CONFIDENZIALE sono necessari due presupposti cumulativi: la conoscenza di informazioni da parte di persone non autorizzate deve poter comportare un *considerevole* pregiudizio causale e potenziale per gli interessi pubblici della Svizzera. Questi interessi pubblici vengono riportati nell'articolo 1 capoverso 2 lettere a–d LSIn. Con «considerevole» si intende che per la Svizzera o per la Confederazione potrebbe derivarne un danno importante.

Art. 20 Livello di classificazione «segreto»

Affinché si giustifichi una classificazione SEGRETO sono necessari due presupposti cumulativi: la conoscenza di informazioni da parte di persone non autorizzate deve potere comportare un

[18] RS **311.0**

grave pregiudizio causale e potenziale per gli interessi pubblici della Confederazione. Questi interessi pubblici vengono riportati nell'articolo 1 capoverso 2 lettere a–d LSIn. Con «grave» si intende che per la Svizzera potrebbe derivarne un danno catastrofico.

Art. 21 Direttive concernenti il trattamento

Capoversi 1 e 2: sulla base dell'articolo 85 LSIn il servizio specializzato della Confederazione per la sicurezza delle informazioni emana direttive inerenti al trattamento di informazioni classificate nonché i requisiti organizzativi, tecnici, edili e riguardanti il personale per garantire la loro protezione. Si tratta di direttive minime uniformi che dovranno essere armonizzate alle direttive di partner esteri della Svizzera (cfr. cpv. 3 nonché art. 3 cpv. 3 OSIn). Le unità amministrative decentralizzate e le organizzazioni ai sensi dell'articolo 2 capoverso 4 LOGA sono soggette ai requisiti quando trattano informazioni classificate della Confederazione o il dipartimento le assoggetta al campo d'applicazione della LSIn. Le unità amministrative e l'esercito possono stabilire un livello di protezione più elevato per il proprio ambito di competenza. Non possono tuttavia esigere dalle altre organizzazioni della Confederazione il rispetto di eventuali misure di protezione rafforzate se vogliono o devono scambiare con altri le loro informazioni classificate, perché ciò violerebbe altrimenti il principio di uno standard uniforme.

Capoverso 3: in applicazione dell'articolo 84 capoverso 1 LSIn il Consiglio federale delega alla CaF la competenza di disciplinare il trattamento degli affari classificati del Governo.

Capoverso 4: trattati internazionali nell'ambito della sicurezza delle informazioni, come con l'UE e con la NATO, contengono elenchi di concordanza sull'applicazione di classificazioni, standard di sicurezza nell'ambito dell'informatica o della sicurezza delle comunicazioni nonché normative sull'esecuzione di controlli reciproci (cfr. messaggio LSIn, commento ad art. 88).

Art. 22 Misure di sicurezza specifiche all'impiego

Può capitare che l'esigenza di condividere rapidamente informazioni all'interno di un gruppo venga ritenuta superiore alla tutela della confidenzialità. Ciò si verifica, in particolare, negli impieghi delle forze di sicurezza o delle forze di polizia. In questi casi, una semplificazione mirata delle normali prescrizioni di sicurezza può agevolare l'adempimento dei compiti senza causare rischi inaccettabili. Secondo il diritto attuale (cfr. art. 18 cpv 3 OPrI), i servizi d'informazione e fedpol possono gestire in modo semplificato informazioni classificate. La medesima esigenza si riscontra in ulteriori unità amministrative della Confederazione alle quali sono affidati compiti di sicurezza, in particolare l'Aggruppamento Difesa, motivo per cui il trattamento semplificato dovrebbe essere messo a disposizione di ulteriori servizi. Tuttavia, questa possibilità non dovrà comportare che per gli uffici più critici sotto il profilo della sicurezza si applichino, *in generale*, requisiti di sicurezza inferiori rispetto agli altri uffici. Le condizioni e le modalità di trattamento semplificato verranno perciò inasprite leggermente.

Art. 23 Certificazione in materia di sicurezza di mezzi informatici

Di norma la certificazione in materia di sicurezza viene richiesta all'estero quando informazioni classificate CONFIDENZIALE vengono trattate in un sistema informatico. Nelle relazioni internazionali è richiesta ogniqualvolta si intende trattare informazioni protette di uno Stato in un sistema di un altro Stato. Se una certificazione simile è richiesta anche per un sistema d'informazione della Svizzera, ad esempio poiché in esso si trattano informazioni classificate dell'UE, il servizio specializzato della Confederazione per la sicurezza delle informazioni potrà verificare e certificare il relativo sistema in collaborazione con i crittografi dell'esercito e gli specialisti della sicurezza di armasuisse. Per la certificazione è determinante la prova del rispetto dei requisiti minimi ai sensi dell'articolo 21 capoverso 1 OSIn. L'OSIn colma una lacuna che finora ha reso difficile la cooperazione internazionale nell'ambito della sicurezza. Per la cooperazione nazionale sinora non era necessaria la certificazione di sicurezza ai sensi dell'articolo 23 OSIn. Anche i sistemi informatici che necessitano l'accesso a un sistema informatico certificato dovranno eventualmente essere certificati. L'OSIn lascia quindi aperta la possibilità di eseguire, in caso di necessità, la certificazione anche per la cooperazione nazionale.

Art. 24 Protezione in caso di pericolo per le informazioni classificate

Corrisponde al diritto attuale (cfr. art. 15 OPrI). La notifica ai competenti organi di sicurezza avviene secondo la disposizione riguardante la gestione degli incidenti (art. 12).

Art. 25 Verifica della necessità di protezione e cerchia delle persone autorizzate

Corrisponde al diritto attuale (cfr. art. 14 OPrI).

Art. 26 Archiviazione

Capoverso 1: le disposizioni concernenti l'archiviazione disciplinano la tutela di documenti della Confederazione che hanno un valore archivistico (inclusi documenti classificati) e la loro comunicazione al pubblico, tenendo conto di interessi legittimi della protezione della personalità e della protezione dello Stato nonché della trasparenza e della tracciabilità. Le informazioni classificate della Confederazione rimangono documenti della Confederazione ai sensi della legislazione in materia di archiviazione, anche quando vengono elaborate da Cantoni e terzi nell'ambito di uno scambio di informazioni. La procedura per l'archiviazione a livello federale è retta quindi anche in questi casi, *mutatis mutandis*, dalla suddetta legislazione.

Capoverso 2: l'AFS ha il compito di garantire la protezione degli archivi archiviati e classificati centralmente. Esso può così derogare ai requisiti e alle misure standard del servizio specializzato della Confederazione per la sicurezza delle informazioni previsti all'articolo 85 LSIn. L'AFS deve tuttavia proteggere gli archivi classificati in modo da garantire una sicurezza conforme al rischio che essi rappresentano.

Capoverso 3: il termine di protezione degli archivi (incl. archivi classificati) non viene prorogato automaticamente alla sua scadenza. La classificazione decade invece automaticamente con la scadenza del termine di protezione. Ciò significa che successivamente a essa vi sarà un diritto generale di consultare gli archivi (cfr. art. 10 cpv. 1 dell'ordinanza dell'8 settembre 1999[19] sull'archiviazione [OLAr]). La maggior parte delle informazioni classificate non necessita di una proroga del termine di protezione di 30 o di 50 anni dopo che è scaduto. Per contro, ad esempio nel caso di edifici o progetti militari, può essere giustificato prorogare il termine di protezione prima che scada (cfr. art. 12 della legge del 26 giugno 1998[20] sull'archiviazione [LAr] in combinato disposto con l'art. 14 OLAr).

L'ufficio competente è responsabile dell'avvio tempestivo di una proroga del termine di protezione. I termini di protezione per i documenti versati figurano nell'elenco di versamento che l'unità amministrativa competente gestisce nei sistemi GEVER. I fondi i cui termini di protezione sono stati prorogati in virtù di interessi pubblici e privati preponderanti degni di protezione (cfr. art. 12 LAr e art. 14 OLAr) vengono elencati nell'allegato 3 dell'OLAr (cfr. art. 14 cpv. 5 OLAr).

Sezione 5: Sicurezza nell'impiego di mezzi informatici

Art. 27 Procedura di sicurezza

In linea di massima, è stata ripresa l'attuale procedura di sicurezza secondo gli articoli 14b–14e OCiber.

Capoverso 1: l'attuale necessità di protezione deve essere rilevata mediante i criteri dei livelli di sicurezza secondo l'articolo 28.

Capoverso 2: le eccezioni alle direttive necessitano sempre di un'autorizzazione esplicita del servizio che le ha emanate (v. commento sull'autorizzazione di deroghe di cui ad art. 9 OSIn).

Il metodo di gestione dei rischi per ridurre lo spionaggio dei servizi di informazione sinora previsto nelle prescrizioni in materia di informatica viene disciplinato mediante le normative concernenti la procedura di sicurezza relativa alle aziende e non necessita più di una normativa separata (cfr. art. 55–58 LSIn).

Capoverso 3: in linea di massima, un rischio residuo può essere un rischio accettato o un rischio ignoto (cfr. manuale sulla gestione dei rischi della Confederazione). Soltanto il primo è un rischio residuo ai sensi dell'OSIn. Se il rischio originario viene ridotto a un livello ragionevole grazie a misure di gestione dei rischi (p. es. per evitare, ridurre o trasferire i rischi), si parla di rischio residuo.

Capoverso 4: l'accettazione «comprovabile» (v. commento ad art. 8 cpv. 1 lett. d) di rischi residui è importante, in quanto conferma lo svolgimento di un processo di analisi e decisionale e quindi una decisione consapevole sui rischi residui ammessi. In linea generale, la delega di tale decisione

[19] RS **152.11**
[20] RS **152.1**

consapevole può avvenire per il tramite di un'istruzione oppure, in casi specifici (p. es. nell'ambito di un progetto informatico), a un altro membro della direzione (parimenti comprovabile).

Capoversi 5 e 6: la presenza di una minaccia nuova o ricorrente può mettere in discussione, in tutto o in parte, un'analisi dei rischi esistente, motivo per cui il concetto in materia di rischi, se del caso, dovrà essere adeguato. Spetta all'ufficio valutare se una modifica della situazione di minaccia è sostanziale.

Alla luce dei rapidi progressi dello sviluppo tecnologico e delle minacce sempre più complesse nel settore della sicurezza delle informazioni, è necessario verificare ogni anno se c'è stato un cambiamento rilevante per la sicurezza. Pertanto decade anche il termine di cinque anni per la ripetizione della procedura di sicurezza ai sensi dell'articolo 14*e* capoverso 1 OCiber.

Capoverso 7: il servizio specializzato della Confederazione per la sicurezza delle informazioni emana direttive minime per la cosiddetta cibersicurezza. Tali direttive si applicano d'altronde anche alle unità amministrative decentralizzate e alle organizzazioni di cui all'articolo 2 capoverso 4 LOGA se accedono a mezzi informatici dei fornitori di prestazioni interni o se fanno gestire loro i propri mezzi informatici.

Art. 28 Assegnazione ai livelli di sicurezza «protezione elevata» e «protezione molto elevata»

I prodotti informatici (cfr. la definizione legale ad art. 5 lett. a in combinato disposto con l'art. 17 LSIn) saranno suddivisi in tre livelli di sicurezza: «protezione di base», «protezione elevata» e «protezione molto elevata», diversamente dall'attuale OCiber che ne prevede soltanto due: «protezione di base» e «protezione elevata». Ai fini dell'attribuzione a uno dei tre nuovi livelli di sicurezza sono determinanti gli interessi pubblici della Confederazione ai sensi dell'articolo 1 capoverso 2 lettere a–e LSIn.

I criteri materiali per la classificazione delle informazioni si applicano in linea di principio anche alla classificazione dei mezzi informatici. Essi sono in gran parte in sintonia con i criteri applicati nell'ambito della gestione dei rischi della Confederazione per la valutazione dell'entità dei danni di un evento.

Contrariamente a quanto avviene per i criteri di attribuzione delle informazioni classificate ai vari livelli di sicurezza, per l'attribuzione dei mezzi informatici ci si piò rifare anche a criteri finanziari. Ciò è dovuto al fatto che una violazione della disponibilità o dell'integrità delle informazioni trattate con mezzi informatici è meglio quantificabile rispetto, ad esempio, a una violazione della confidenzialità di un documento classificato.

Art. 29 Misure di sicurezza

Capoverso 1: le direttive emanate finora dall'UFCS concernenti i requisiti minimi per i relativi livelli di sicurezza secondo l'articolo 17 LSIn per l'Amministrazione federale e l'esercito dal 2025 verranno emanate dal servizio specializzato della Confederazione per la sicurezza delle informazioni. Tali direttive si applicheranno anche alle unità amministrative decentralizzate che non sono assoggettate dal proprio dipartimento all'intera LSIn e alle organizzazioni di cui all'articolo 2 capoverso 4 LOGA se accedono a mezzi informatici dei fornitori di prestazioni interni dell'Amministrazione federale o se fanno gestire i propri mezzi informatici da questi ultimi (p. es. dall'Ufficio federale dell'informatica e della telecomunicazione). La «protezione di base» si applica anche ai Cantoni (cfr. art. 3 LSIn), a condizione che rientri nel campo di applicazione della LSIn.

Capoverso 2: il servizio specializzato si adopera per un coordinamento opportuno con l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) e i consulenti per la protezione dei dati (cfr. anche art. 82 cpv. 1 LSIn) in merito alle questioni relative alla protezione dei dati e alla sicurezza dei dati basata sul rischio. Le istruzioni di cui al capoverso 1 dovranno essere allineate alle vigenti disposizioni in materia di protezione dei dati. In tale contesto occorre osservare che le nozioni di «protezione elevata» e «protezione molto elevata» di cui all'articolo 17 LSIn non corrispondono, ad esempio, alle nozioni di «rischio», «rischio esiguo» o «rischio elevato» del diritto in materia di protezione dei dati.

Capoverso 3: con le lettere a e b si distingue tra due tipi di rischio che richiedono un'attenzione particolare quanto all'efficacia delle misure di sicurezza. Per tale motivo, è necessaria una verifica pertinente appena si delineano cambiamenti sostanziali dei rischi, al più tardi però ogni cinque anni. La base giuridica per la verifica periodica si trova nell'articolo 18 capoverso 3 LSIn.

Capoverso 4: cfr. articolo 10 capoverso 2 LSIn e il commento ad articolo 5 capoverso 4 OSIn.

Art. 30 Sicurezza durante l'esercizio

Capoversi 1–3: i fornitori di prestazioni interni della Confederazione rivestono un duplice ruolo nell'attuazione della sicurezza delle informazioni. Da un lato, sono normali unità organizzative che devono attuare l'OSIn come tutte le altre unità organizzative. Dall'altro, hanno un'importanza cruciale anche per la sicurezza dei beneficiari di prestazioni. È quindi essenziale per la sicurezza che la ripartizione dei compiti e delle competenze sia chiara. I fornitori di prestazioni hanno un obbligo generale di fornire le proprie prestazioni informatiche secondo lo stato della tecnica e di mettere a disposizione dei propri beneficiari di prestazioni, in tempo utile, le necessarie informazioni rilevanti per la sicurezza. Tra queste rientrano i meccanismi di protezione adottati che comprendono più livelli come security, compliance e backup. In tal modo non solo ci si può proteggere da attacchi malware e ransomware, ma anche contro danni come per esempio guasti di sistema, errori umani (p. es. diritti d'accesso sbagliati o obsoleti ecc.) oppure anche contro utenti malintenzionati della propria organizzazione. Tuttavia i beneficiari di prestazioni devono provvedere affinché le responsabilità per la sicurezza a livello operativo, anche per la gestione delle vulnerabilità, siano definite chiaramente nelle convenzioni sulle prestazioni. Sono infatti responsabili della sicurezza dei propri dati e compiti.

Capoverso 4: questa vigilanza è una faccenda di mera sicurezza tecnica e non ha nulla a che vedere con un'eventuale sorveglianza dei collaboratori. I terzi, per esempio, possono essere persone nell'ambito di un programma *bug bounty*.

Sezione 6: Misure relative alle persone e protezione fisica

Art. 31 Verifica dell'identità di persone e macchine

Si tratta di stabilire in che misura una persona debba dimostrare la propria identità fisica o elettronica per poter accedere alle informazioni, ai mezzi informatici, ai locali e alle altre infrastrutture della Confederazione. Il livello di sicurezza richiesto (il cosiddetto «level of assurance») sarà superiore per i sistemi sensibili rispetto alle applicazioni normali. Non solo le persone, ma anche i computer e persino i processi devono «identificarsi». Nel diritto attualmente in vigore le relative disposizioni fanno parte della protezione IT di base emanata nell'Amministrazione federale dall'UFCS. Al momento non è necessaria una regolamentazione separata, ma potrebbe essere opportuna a causa della crescente importanza di questo «level of assurance».

Art. 32 Sicurezza delle persone

La prassi ha mostrato che, dopo il superamento di un controllo di sicurezza relativo alle persone, soltanto in casi eccezionali la questione dei rischi per la sicurezza riferiti a persone viene nuovamente affrontata. Ai sensi di una gestione a posteriori (cosiddetta «aftercare»), usuale a livello internazionale, i collaboratori che sono stati sottoposti a CSP dovranno comunicare al proprio datore di lavoro le circostanze, nel proprio contesto privato e professionale, che pregiudicano la sicurezza. Queste circostanze rappresentano una particolare vulnerabilità dei collaboratori (p. es. indebitamento nel contesto di una dipendenza da gioco, alcolismo o tossicodipendenza rivelato da un terzo, relazione extraconiugale emersa) oppure sono attività che comportano maggiori rischi (p. es. viaggi in Paesi particolarmente critici o contatti intensi con persone di questi Paesi). Per i collaboratori soprattutto la vulnerabilità percepita può essere particolarmente stressante dal punto di vista psicologico. Per il datore di lavoro non si tratta di spiare, sorvegliare costantemente o addirittura punire i collaboratori, bensì di definire insieme a loro, in un rapporto di fiducia, le misure o le strategie di riduzione del rischio eventualmente adeguate. In caso di comunicazione sensibile, bisognerà concordare con il servizio del personale o con un organo di mediazione come procedere.

Gli uffici, le segreterie generali, i gruppi e la CaF sono inoltre tenuti ad assicurare ogni anno la sensibilizzazione dei collaboratori soggetti a un CSP. I superiori dovranno assumersi attivamente la responsabilità dei rischi per la sicurezza riferiti a persone e integrarla nei compiti direttivi permanenti, per esempio, nell'ambito dei colloqui con i collaboratori. Tale aspetto verrebbe così affrontato almeno una volta all'anno.

Art. 33 Sospetto di reato

Capoverso 1: la disposizione mira a garantire che eventuali reati siano inoltrati il più rapidamente possibile alle competenti autorità preposte al perseguimento penale senza che la CaF e i dipartimenti debbano fare considerazioni dettagliate di diritto penale o addirittura di diritto processuale penale. In tal senso, un reato «è già ipotizzabile» se primi indizi, anche non del tutto concludenti, suggeriscono un comportamento punibile.

Capoverso 2: qui si tratta di accertare rapidamente prove tangibili e in parte effimere. A tal fine, non possono essere eretti ostacoli eccessivi. È importante che nell'ambito dell'accertamento delle prove le unità amministrative non cancellino, lascino o addirittura causino tracce fisiche o elettroniche. In questa sede il concetto di «mettere al sicuro le prove» non comporta anche la loro valutazione; ciò spetta, se del caso, alle autorità preposte al perseguimento penale su ordine del tribunale.

Art. 34 Misure di protezione fisica

Capoverso 1: oggi, nella Confederazione, le direttive volte a garantire la protezione fisica delle informazioni e dei mezzi informatici vengono definite da più servizi (fedpol e Ufficio federale delle costruzioni e della logistica UFCL per l'Amministrazione federale civile, Stato maggiore dell'esercito per l'Aggruppamento Difesa e l'esercito). Attualmente le direttive esistenti coprono a sufficienza le esigenze in materia di sicurezza. Qualora dovessero essere necessarie direttive supplementari o consolidate a livello federale, per esempio riguardo all'armonizzazione internazionale delle prescrizioni di protezione, previa consultazione dei suddetti servizi il servizio specializzato della Confederazione per la sicurezza delle informazioni *potrà* emanare per l'Amministrazione federale e l'esercito requisiti minimi per la protezione fisica delle informazioni e dei mezzi informatici. Tali direttive si applicano alle unità amministrative decentralizzate e alle organizzazioni di cui all'articolo 2 capoverso 4 LOGA soltanto se trattano informazioni classificate, accedono a mezzi informatici dei fornitori di prestazioni TIC interni o se affidano la gestione dei propri mezzi informatici a questi fornitori.

Capoversi 1–2: sono considerate misure di protezione fisica, ad esempio, l'allestimento di zone di sicurezza (cfr. art. 35 OSIn e il messaggio LSIn, pag. 2644 seg.), i controlli all'ingresso degli edifici, la sorveglianza mediante telecamere in determinate zone, i dispositivi di distruzione dei supporti di dati o i controlli sul posto di lavoro.

Art. 35 Zone di sicurezza

Capoversi 1–3: la creazione di zone di sicurezza ha lo scopo di ridurre il potenziale di danno a seguito di spionaggio o sabotaggio in zone molto sensibili (come locali dei server e locali di condotta o locali a prova d'intercettazione) (cfr. messaggio LSIn pag. 2628, 2644 seg.). Se persone o aziende hanno necessità di accedere a una zona di sicurezza ai sensi di questa ordinanza, dovranno essere dapprima sottoposte a un CSP o a una procedura di sicurezza relativa alle aziende. Occorre pertanto garantire che le zone di sicurezza siano allestite in modo appropriato e corretto. Prima della messa in servizio è perciò richiesto un controllo, da ripetere periodicamente. Il servizio specializzato della Confederazione per la sicurezza delle informazioni emanerà le direttive necessarie.

Capoverso 4: la protezione delle informazioni e dei mezzi informatici in una zona di sicurezza inizia già al di fuori di essa. I potenziali aggressori dispongono oggi di mezzi per spiare da lontano i segnali elettromagnetici. Pertanto, le unità amministrative dovrebbero essere autorizzate a installare, nei dintorni della zona di sicurezza, sensori per rilevare tentativi di spionaggio e respingerli. Queste misure vengono, di norma, raccomandate dagli organi di sicurezza della Confederazione. L'attuazione rientra tuttavia nella responsabilità dell'unità amministrativa che allestisce la zona di sicurezza.

Sezione 7: Organizzazione di sicurezza

Una novità importante nell'OSIn riguarda le direzioni degli uffici. Infatti l'OSIn assegnati loro compiti, competenze e responsabilità concreti nell'ambito della sicurezza delle informazioni. I direttori degli uffici potranno delegare i compiti a un membro della loro direzione (responsabili della sicurezza delle informazioni). Questi responsabili vigilano sul SGSI dell'ufficio e prendono tutte le decisioni importanti in questo ambito. Per contro le attività di vigilanza operativa sono compito degli incaricati della sicurezza delle informazioni. L'OSIn riunisce quindi gli attuali ruoli degli «incaricati della sicurezza informatica» e degli «incaricati della protezione delle informazioni» nel nuovo ruolo degli «incaricati della sicurezza delle informazioni». I loro attuali compiti sono quindi precisati e completati con compiti rilevanti per il SGSI.

A livello dei dipartimenti si applica un modello analogo. Secondo gli articoli 37, 38, 41 e 42 LOGA, i dipartimenti sono responsabili della direzione, del coordinamento e della vigilanza della sicurezza delle informazioni nel dipartimento stesso. Definiscono in particolare la politica in materia di sicurezza delle informazioni e l'organizzazione della sicurezza del dipartimento. La responsabilità operativa per la sicurezza è assunta dal segretario generale. Come è avvenuto finora, gli incaricati della sicurezza delle informazioni svolgeranno i compiti di coordinamento e di vigilanza operativi (cfr. art. 81 LSIn).

L'organizzazione di sicurezza nella sezione 7 descrive i vari ruoli e le varie funzioni previsti. A seconda delle esigenze di un ufficio, alcuni ruoli, per esempio quello degli incaricati della sicurezza delle informazioni delle unità amministrative (cfr. art. 37 OSIn), potranno essere occupati da più persone in funzione di temi specifici. Lo stesso vale per tutti gli altri ruoli di cui all'articolo 37 segg. OSIn. Nessun ruolo è vincolato a una sola persona. Fa eccezione quello del responsabile della sicurezza delle informazioni che può essere unicamente assunto da una sola persona.

I sostituti dovranno essere idonei per tutti i compiti del ruolo primario dal punto di vista tecnico e personale. Dovranno essere istruiti o formati per poter supplire al ruolo primario in modo adeguato in qualsiasi momento e, soprattutto, in situazioni di emergenza.

Il sistema basato sui ruoli dell'OSIn è pensato per la grande maggioranza delle unità amministrative nelle quali la sicurezza delle informazioni costituisce un compito trasversale. Per i fornitori di prestazioni TIC della Confederazione garantire la sicurezza in azienda è invece un compito fondamentale. Di norma, i fornitori di prestazioni dispongono anche di un reparto di sicurezza condotto da un membro della direzione. Poiché presso questi fornitori di prestazioni la sicurezza è già organizzata e attuata in modo gerarchico, a determinate circostanze può essere ipotizzabile una fusione dei ruoli di «responsabili della sicurezza» e «incaricati della sicurezza».

Art. 36 Responsabili della sicurezza delle informazioni delle unità amministrative di cui all'articolo 2 capoverso 1 lettera c

Capoverso 1: con «responsabile» si intende l'obbligo personale di rendere conto all'organo superiore. Esso presuppone che la persona responsabile abbia il potere, in particolare finanziario, di adottare, controllare o correggere misure. Questo obbligo va delimitato dall'obbligo di attuare misure di vigilanza. In tal caso, è la persona incaricata a essere responsabile dello svolgimento nonché l'unica tenuta a rispondere di esso.

Capoverso 2: con la delega della responsabilità per la sicurezza delle informazioni si delega anche l'obbligo personale di rendere conto. Per tale motivo, la delega dovrebbe essere comprovabile (v. commento ad art. 8 cpv. 1 lett. d).

Capoverso 3 lettera b: in linea di principio, tutte le decisioni importanti concernenti la sicurezza delle informazioni sono prese da questo ruolo.

Capoverso 4: gli incaricati della sicurezza delle informazioni di cui all'articolo 37 OSIn possono, per esempio, essere incaricati per il tramite di istruzioni interne o nell'ambito della definizione di obiettivi annuali ai sensi dell'articolo 5 capoverso 2. Sull'espressione «conflitto d'interessi», si rimanda al messaggio LSIn, commento ad art. 82 capoverso 3.

Art. 37 Incaricati della sicurezza delle informazioni delle unità amministrative di cui all'articolo 2 capoverso 1 lettera c

La designazione di un sostituto ufficiale è una novità. Questo ruolo corrisponde in buona parte al precedente incaricato della sicurezza informatica a livello di unità organizzativa (ISIU) nelle unità amministrative.

L'incaricato della sicurezza delle informazioni della CaF verifica presso terzi secondo l'articolo 8 OCSP l'esistenza di un'attività sensibile sotto il profilo della sicurezza, qualora ciò non fosse coperto nell'ambito della procedura di sicurezza relativa alle aziende. Presso i dipartimenti, il compito verrà svolto dall'incaricato della sicurezza delle informazioni del livello dipartimentale.

Art. 38 Sicurezza delle informazioni nei servizi standard

In linea di principio, questo ruolo nei servizi standard ha gli stessi compiti del ruolo degli incaricati della sicurezza delle informazioni delle unità amministrative secondo l'articolo 37.

Art. 39 Responsabilità in materia di sicurezza dei dipartimenti

Capoversi 1e 2: la gestione e la vigilanza relative alla sicurezza delle informazioni rappresentano compiti strategici e compiti fondamentali dei dipartimenti (cfr. art. 38 LOGA; commento ad art. 5 cpv. 1).

In base all'articolo 47 capoverso 4 OLOGA i dipartimenti possono avocare a sé i compiti e le competenze che l'OSIn assegna a uffici, segreterie generali, gruppi e CaF. Un dipartimento come il

DFAE, che ha una forma organizzativa centralizzata, potrà così attuare le proprie esigenze organizzative nel contesto dell'OSIn.

Capoverso 4: per le direttive, le misure e gli audit a livello dipartimentale la miglior soluzione è che vengano decise dai segretari generali. Se la responsabilità della sicurezza negli uffici è assunta dai rispettivi direttori, essi si aspettano una collocazione conseguentemente elevata della persona che dispone della competenza decisionale a livello di dipartimento. Il caso Xplain nell'Amministrazione federale ha inoltre mostrato che può essere necessario un accompagnamento di natura politico-strategica in materia di incidenti da parte dei segretari generali. La soluzione «segretario generale» ha l'ulteriore vantaggio che il coordinamento interdipartimentale può avere luogo nella Conferenza dei segretari generali.

Art. 40 Incaricati della sicurezza delle informazioni dei dipartimenti

La designazione di un sostituto ufficiale è una novità (cfr. art. 81 cpv. 1 LSIn). Questo ruolo unisce il ruolo degli attuali incaricati della sicurezza informatica dei dipartimenti (ISID) e quello incaricati della protezione delle informazioni dei dipartimenti. Oltre ai compiti e alle competenze elencati, questo ruolo è anche competente per il nuovo compito nell'ambito dei CSP. Nello specifico, la verifica dell'esistenza di un'attività sensibile sotto il profilo della sicurezza presso terzi ai sensi dell'articolo 8 OCSP, per la quale si rinuncia alla procedura di sicurezza relativa alle aziende.

Lettera f: poiché gli incaricati della sicurezza delle informazioni secondo gli articoli 37 e 40 devono collaborare strettamente, l'incaricato della sicurezza delle informazioni del dipartimento di cui all'articolo 40 dovrebbe essere coinvolto nella scelta di una nuova persona per il ruolo di incaricato della sicurezza delle informazioni delle unità amministrative secondo l'articolo 37. Potrà valutare in particolare la competenza specialistica della persona da scegliere. Le modalità dell'«obbligo di consultazione» dovranno essere definite tra gli uffici e il dipartimento.

Lettera g: la procedura del controllo dei documenti segreti è ripresa invariata.

Lettera h: finora i rapporti annuali degli ISID dovevano essere inviati all'UFCS. In base alla nuova disposizione i detentori dei ruoli dovranno fare rapporto alla persona responsabile in materia di sicurezza del dipartimento secondo l'articolo 39 (cfr. art. 14). In seguito, quest'ultima invia il rapporto al servizio specializzato della Confederazione per la sicurezza delle informazioni affinché, a sua volta, esso possa redigere annualmente per il Consiglio federale un rapporto sullo stato della sicurezza delle informazioni (cfr. art. 83 cpv. 1 lett. h LSIn).

Art. 41 Incaricato della sicurezza delle informazioni del Consiglio federale

In futuro anche il Consiglio federale in veste di autorità assoggettata riceverà un incaricato della sicurezza delle informazioni e un sostituto conformemente all'articolo 81 LSIn. L'incaricato nominato assumerà contemporaneamente secondo l'articolo 83 capoverso 3 LSIn la direzione del servizio specializzato della Confederazione per la sicurezza delle informazioni. Poiché il servizio specializzato farà parte della SEPOS nel DDPS, quest'ultimo avrà il compito di nominare l'incaricato della sicurezza delle informazioni.

Art. 42 Servizio specializzato della Confederazione per la sicurezza delle informazioni

Capoverso 1: i compiti generali e in gran parte di supporto e coordinamento del servizio specializzato della Confederazione per la sicurezza delle informazioni figurano nell'articolo 83 LSIn e nell'articolo 41 OSIn; i compiti specifici al contesto in ulteriori disposizioni dell'OSIn (p. es. direttive concernenti la gestione della sicurezza delle informazioni secondo l'art. 15, ulteriori direttive in vari settori secondo gli art. 17, 21, 23, 27, 29, 31, 34 e 35). Riguardo alla collaborazione tra servizio specializzato e l'UFCS, si veda il numero 2.3 lettera i.

Lettera f: oggi il Settore «Trasformazione digitale e governance delle TIC» (Settore TDT) della CaF gestisce i cosiddetti servizi standard (cfr. art. 4 cpv. 4 dell'ordinanza del 25 novembre 2020[21] sulla trasformazione digitale e l'informatica [OTDI]). Si tratta di prestazioni fornite a livello centrale nell'Amministrazione federale, utilizzate più volte e che soddisfano esigenze uguali o simili. In tale contesto è responsabile anche di servizi di sicurezza, come l'impiego di Threema, l'applicazione della Confederazione per la comunicazione sicura su dispositivi intelligenti. Finora mancava un servizio richiedente a livello federale per soluzioni di sicurezza utilizzate da vari dipartimenti e dall'esercito e per le soluzioni secondo l'articolo 23 OSIn, certificate per trattare informazioni classificate

[21] RS **172.010.58**

CONFIDENZIALE o SEGRETO. Ciò ha reso più difficile l'acquisizione, la cura e l'ulteriore sviluppo di soluzioni di sicurezza per la crittografia di file o la videoconferenza sicura. Occorre pertanto che il servizio specializzato della Confederazione ne assuma la responsabilità. Ciò non interessa né mette in discussione la competenza del Settore TDT della CaF per i servizi standard.

Capoverso 2: la Conferenza degli incaricati della sicurezza delle informazioni di cui all'articolo 82 capoverso 2 lettera c LSIn offrirà consulenza al servizio specializzato della Confederazione per la sicurezza delle informazioni in tutte le questioni relative al coordinamento dell'esecuzione e in questioni di importanza strategica.

Capoverso 3: il ruolo dell'autorità di sicurezza nazionale, finora assunto dalla Segreteria generale del DDPS, verrà assegnato al servizio specializzato della Confederazione per la sicurezza delle informazioni. I compiti e le competenze secondo le lettere d e f saranno oggetto dei trattati internazionali di cui all'articolo 87 LSIn (cfr. messaggio LSIn, commento ad art. 88, pagg. 2683–2684; pag. 2703).

Art. 43 Compiti e competenze dell'UFSC

L'Ufficio federale della cibersicurezza (UFSC) è il centro di competenza della Confederazione per le questioni di cibersicurezza. Il suo compito fondamentale riguarderà la cibersicurezza in Svizzera. Al riguardo la Confederazione sarà, in sostanza, un «cliente» come molti altri. Il NCSC assumerà però vari compiti a favore delle autorità federali, in particolare per quanto riguarda la gestione degli incidenti (cfr. art. 12 OSIn). Inoltre, fornirà consulenza e sosterrà le autorità federali e sarà rappresentato negli organi della Confederazione.

Per migliorare la cibersicurezza della Confederazione, l'UFCS sarà autorizzato a cercare minacce e vulnerabilità di natura tecnica nelle reti dell'Amministrazione federale o su Internet. Potrà anche incaricarne terzi, ad esempio nell'ambito di un programma *bug bounty*. Ovviamente non potrà cercare senza autorizzazione nelle reti dell'esercito o del Servizio informazioni.

L'UFCS e il servizio specializzato della Confederazione per la sicurezza delle informazioni dovranno coordinare le loro attività per evitare doppioni e impiegare le risorse nel modo più efficiente possibile. Entrambi saranno aggregati al DDPS, il che facilita la collaborazione (v. anche il numero 2.3 lettera i).

Sezione 8: Costi e valutazione

Art. 44 Costi

Le unità amministrative assumeranno i costi della propria sicurezza. Tali costi dovranno essere pianificati e riportati già in sede di pianificazione dei progetti. Ne è, in particolare, il caso per i costi delle misure per la sicurezza informatica.

Art. 45 Valutazione

Cfr. messaggio LSIn, commento ad articolo 89 LSIn, pagina 2684.

Sezione 9: Trattamento di informazioni e di dati personali

Gli articoli 46–48 disciplinano il trattamento di informazioni e di dati personali nell'ambito della gestione della sicurezza delle informazioni secondo l'ordinanza oggetto del presente commento. La gestione degli incidenti legati alla sicurezza presuppone il trattamento di dati riguardanti potenziali autori che possono essere connessi a perseguimenti e sanzioni amministrativi o penali e che sono pertanto considerati dati personali degni di particolare protezione ai sensi dell'articolo 5 lettera c LPD. La legislazione sulla protezione dei dati esige a tal fine una base legale esplicita, finora mancante, a livello di legge. Nell'ambito della corrente revisione della LSIn (v. n. 2.1) viene creata la necessaria base legale formale (cfr. art. 10*a* LSIn).

Art. 46 In generale

Capoversi 1 e 2: le unità amministrative e i loro organi di sicurezza non sono in grado di adempiere i propri compiti senza un reciproco scambio di informazioni e di dati personali. Riguardo al trattamento di dati personali degni di particolare protezione nell'ambito della gestione degli incidenti si veda il commento alla sezione 9. Il trattamento di dati personali derivanti dall'utilizzo dell'infrastruttura elettronica della Confederazione è disciplinato, in linea di principio, dagli articoli 57*i*–57*q* LOGA. Con il nuovo articolo 10*a* LSIn viene tuttavia creata la propria base legale necessaria a trattare dati personali degni di particolare protezione e si applicherà anche al trattamento in forma non elettronica di dati e migliora le modalità dello scambio di dati.

Capoversi 4 e 5: in caso di ciberattacco accade regolarmente che l'aggressore pubblichi dati rubati su Internet se la vittima non paga il denaro del ricatto. Nonostante una potenziale inchiesta penale, le unità amministrative della Confederazione e in particolare i loro organi di sicurezza devono poter scaricare e analizzare questi dati al fine di valutare i danni per la Confederazione e avviare le necessarie misure atte a contenerli (p. es. informare le persone interessate). Se il ciberattacco avviene presso un'azienda che lavora per la Confederazione, il più delle volte sono interessate non soltanto informazioni di quest'ultima, ma anche dati di altri clienti per il cui trattamento la Confederazione non dispone di alcuna base legale. Le disposizioni del capoverso 4 autorizzano quindi gli uffici federali a trattare questi dati. Il trattamento dei dati di terzi è consentito solamente se sono necessari alla valutazione del danno per la Confederazione.

Art. 47 Applicazione SGSI

Questa disposizione crea la base legale per l'impiego di applicazioni SGSI con le quali vengono digitalizzati i compiti e i processi dell'OSIn. Riguardo al trattamento di dati personali degni di particolare protezione, v. commento alla sezione 9.

Art. 48 Servizi di modulistica elettronica

Capoverso 1: un servizio di modulistica è una semplice, piccola applicazione che permette di compilare e inviare moduli elettronicamente. I servizi di modulistica secondo il capoverso 1 servono a emettere in modo automatizzato cosiddette richieste di visita (*«Request for Visit»*, cpv. 1 lett. a), attestazioni di sicurezza (cpv. 1 lett. b) e attestazioni internazionali di sicurezza aziendale (*«Facility Security Clearances»*, cpv. 1 lett. c).

Capoverso 2: i dati nell'allegato 2 sono dati personali che, analogamente a quanto avviene in un processo di autorizzazione di viaggio ESTA, vengono richiesti per viaggi negli Stati Uniti. I dati contrassegnati da un asterisco (*) nell'allegato 2 sono inoltrati ad autorità straniere. Le disposizioni del diritto in materia di protezione dei dati sulla comunicazione di dati all'estero (in particolare art. 16 cpv. 1 e art. 17 LPD) sono rispettate. Senza l'indicazione di questi dati la persona richiedente non ottiene l'accesso al progetto classificato all'estero.

Capoversi 3–6: nel contesto di una notifica di sicurezza possono venire trattate informazioni classificate o dati personali. Con l'invio della notifica, i dati finiscono immediatamente nell'applicazione SGSI, nella quale vengono trattati la notifica e l'incidente. Per motivi di sicurezza delle informazioni e di protezione dei dati, i dati potenzialmente sensibili non possono essere memorizzati per oltre 24 ore nel servizio di modulistica. Riguardo al trattamento di dati personali degni di particolare protezione nell'ambito della gestione degli incidenti, v. commento alla sezione 9.

Sezione 10: Disposizioni finali

Art. 49 Disposizioni esecutive particolari

Sempreché la legge non lo preveda esplicitamente, soltanto il Consiglio federale o il dipartimento competente può emanare prescrizioni (cfr. art. 48 cpv. 1 LOGA) vincolanti per i Cantoni. Poiché il servizio specializzato della Confederazione per la sicurezza delle informazioni non dispone della necessaria competenza giuridico-formale, il DDPS dovrà dichiarare vincolanti le proprie direttive tecniche. Ciò riguarda in particolare le direttive di cui agli articoli 21 e 29 OSIn.

Art. 50 Abrogazione e modifica di altri atti normativi

L'OCiber è abrogata. L'OPrI si applica ancora soltanto fino al 31 dicembre 2023, per cui il passaggio al nuovo diritto sarà graduale (v. più sotto).

Art. 51 Disposizioni transitorie

Oltre a queste disposizioni transitorie, se ne trovano ulteriori nella LSIn, nell'OCSP e nell'OPSAz. Queste disposizioni transitorie dovrebbero permettere di pianificare e attuare in modo sistematico e regolare il nuovo diritto entro sei anni dall'entrata in vigore (cfr. anche art. 90 LSIn).

Capoversi 1 e 2: le attuali direttive dell'UFSC non saranno tutte abrogate e sostituite con l'entrata in vigore della nuova legge. Alcune di esse sono state adeguate poco prima dell'entrata in vigore del nuovo diritto e tengono conto di molti dei nuovi requisiti (p. es. direttive della protezione di base della Confederazione). Durante il periodo transitorio, a seconda dell'ambito di competenza ai sensi dell'OSIn il servizio specializzato della Confederazione per la sicurezza delle informazioni o l'UFCS deciderà in merito alle autorizzazioni eccezionali. Entrambi decideranno in merito al caso specifico.

Capoversi 3 e 5: la CSG ha allestito il catalogo di classificazione della Confederazione. Esso verrà sostituito dai cataloghi di classificazione di cui all'articolo 17 OSIn, che dovranno essere realizzati entro un anno dall'entrata in vigore dell'OSIn (cfr. art. 50 cpv. 4). La CSG ha inoltre ripreso le istruzioni dell'organo di coordinamento per la protezione delle informazioni in seno alla Confederazione concernenti prescrizioni dettagliate sulla protezione delle informazioni. Queste istruzioni verranno completamente rielaborate entro due anni e approvate dal servizio specializzato della Confederazione per la sicurezza delle informazioni.

Capoverso 4: un SGSI non può essere sviluppato «su due piedi». Sarà necessario eseguire analisi ed elaborare concetti, che richiedono tempo. Inoltre, verosimilmente dal 2025 la Confederazione disporrà di un'apposita applicazione per digitalizzare i processi SGSI. Il termine di cui al capoverso 4 intende consentire agli uffici, alla CaF e ai dipartimenti di pianificare e attuare con cura i lavori.

Capoversi 6 e 7: con l'entrata in vigore della LSIn e dell'OSIn, il servizio specializzato della Confederazione per la sicurezza delle informazioni verrà sviluppato progressivamente in seno alla SEPOS. Fino alla metà del 2025 l'UFCS continuerà pertanto a svolgere i suoi compiti attuali nel settore della sicurezza informatica e persino a emanare direttive. La durata di validità di tali direttive, tuttavia, sarà limitata, in linea con il termine di cui al capoverso 3.

Art. 52 Entrata in vigore

L'OSIn verrà posta in vigore il 1º gennaio 2024 assieme alla LSIn e alle rimanenti ordinanze.

Allegato 1

V. commento ad articolo 48.

Allegato 2

Con la sostituzione dell'OPrl e dell'OCiber, in varie ordinanze i rinvii verranno aggiornati in virtù del nuovo diritto e, laddove necessario, l'espressione «sicurezza informatica» sarà adeguata in «sicurezza delle informazioni».

Numero 31: ordinanza del 24 giugno 2009[22] sui contatti militari internazionali (OCMI): con la LSIn e le sue ordinanze d'esecuzione bisogna aggiornare gli organi e le ordinanze rilevanti.

[22] RS **510.215**

3.2 Modifica dell'ordinanza sui sistemi di gestione delle identità e sui servizi di elenchi della Confederazione (OIAM)

Osservazioni preliminari

Nell'ambito di questo atto normativo, all'OIAM vengono apportate soltanto le modifiche necessarie secondo la LSIn e la LMeCA. L'ulteriore fabbisogno di adeguamenti dell'OIAM individuato non è invece parte di questo atto normativo, ma è oggetto di una revisione totale di cui la CaF si sta occupando.

Modifiche in virtù della LSIn

Finora l'OIAM si è fondata in linea di principio sulla LOGA. Con gli articoli 24–26 LSIn viene creata una base legale formale specifica a cui l'OIAM farà principalmente riferimento in futuro. Sulla base dell'articolo 20 capoverso 2 LSIn sarà inoltre ammesso, a determinate condizioni, utilizzare in generale dati biometrici nei sistemi IAM. Di conseguenza, occorre procedere ai necessari adeguamenti nell'OIAM.

Modifiche in virtù della LMeCA

Nell'ambito del servizio standard eIAM, l'Amministrazione federale ha creato un servizio di autenticazione per l'accesso alle rispettive applicazioni tecniche e ai servizi del Governo elettronico (servizi amministrativi online). Nel frattempo tale servizio si è diffuso in modo capillare (oltre 10 mio. di accessi al mese, più di 800 applicazioni collegate e circa 2 mio. di identità elettroniche) e avendo dimostrato la sua validità, dovrebbe ora essere messo a disposizione dei Cantoni interessati (e dei rispettivi Comuni) in virtù della LMeCA, per poi essere integrato nelle rispettive applicazioni. In tal modo, sarà possibile realizzare e fornire alla popolazione una procedura di accesso integrale per l'utilizzo dei servizi amministrativi digitali di tutti e tre i livelli federali sfruttando al contempo le sinergie esistenti a livello amministrativo.

Il servizio sarà introdotto nei Cantoni a partire dal 1° gennaio 2024 e assumerà la denominazione di AGOV («Authentifizierungsdienst der Schweizer Behörden», ovvero servizio di autenticazione delle autorità svizzere). Tale servizio consentirà:

- alle persone fisiche di generare un'identità elettronica e di utilizzarla per effettuare l'accesso a tutte le applicazioni collegate al fine di usufruire dei servizi amministrativi digitali;
- alle persone fisiche di utilizzare le identità elettroniche già esistenti e riconosciute da AGOV per effettuare l'accesso a tutte le applicazioni collegate al fine di usufruire dei servizi amministrativi digitali;
- ai fornitori di servizi amministrativi digitali di eseguire in modo sicuro l'autenticazione dei propri clienti senza dover realizzare e gestire tale servizio autonomamente; nonché
- alle amministrazioni di tutta la Svizzera di predisporre il futuro impiego della Id-e come strumento di identificazione contribuendo così alla sua diffusione.

Alla luce di quanto precede sono state apportate diverse modifiche all'ordinanza sui sistemi di gestione delle identità e sui servizi di elenchi della Confederazione (OIAM).

Ingresso

Modifiche in virtù della LSIn

Con gli articoli 24–26 LSIn è stata creata una base legale formale specifica per l'attuale OIAM elevando a livello di legge le principali disposizioni dell'ordinanza. Finora l'ordinanza si basava sulla competenza organizzativa del Consiglio federale e, indirettamente, sulle basi legali di tutti i sistemi collegati ai sistemi IAM. In futuro l'OIAM, invece che sulla LOGA, si baserà principalmente sui menzionati articoli della LSIn. Saranno così contemplati anche i sistemi IAM degli archivi delle identità. I servizi di elenchi, invece, non sono contemplati dalla LSIn, per cui in questo ambito la LOGA dovrà continuare a figurare.

In virtù dell'articolo 20 capoverso 2 LSIn, a determinate condizioni sarà inoltre consentito il trattamento di dati biometrici nei sistemi IAM. Secondo la LPD, i dati biometrici sono considerati dati

personali degni di particolare protezione (FF 2020 6695, art. 5 lett. c n. 4). Viene così relativizzato il principio secondo cui questi ultimi non possono essere trattati nei sistemi IAM (art. 11 cpv. 3). Sulla base di disposizioni di legge specifiche al di fuori della LSIn, permane quindi la possibilità di trattare nei sistemi IAM dati personali degni di particolare protezione. I profili della personalità non sono più un criterio rilevante nella LPD e pertanto non occorrerà più menzionarli. Una profilazione ai sensi dell'articolo 5 lettere f e g LPD non sarà effettuata in sistemi IAM e servizi di elenchi poiché servono a *valutare* gli aspetti personali delle persone.

Modifiche in virtù della LMeCA

L'OIAM disciplina già il collegamento di sistemi IAM, nella fattispecie il collegamento dei sistemi IAM esterni ai sistemi IAM della Confederazione (art. 21 segg.) nonché il collegamento di questi ultimi a sistemi IAM esterni (art. 24). Con la LMeCA, in particolare con il rispettivo articolo 11, sono state create le basi legali in virtù delle quali la Confederazione può fornire servizi direttamente ai Cantoni nell'ambito di tale collegamento. L'AGOV è parte integrante del servizio standard eIAM e con l'estensione del suo impiego ai Cantoni e ai Comuni si dà attuazione all'articolo 11 LMeCA. Per quanto concerne l'AGOV, l'OIAM disciplina in particolare l'esecuzione dell'articolo 11 capoversi 3-5 LMeCA. La presente revisione contiene i disciplinamenti aggiuntivi necessari per l'implementazione dell'AGOV.

Art. 1 (Oggetto) *non* viene modificato, poiché tutti i servizi che ora devono obbligatoriamente sottostare all'OIAM (v. commento ad art. 2 di seguito) sono stati inclusi nell'attuale definizione «della Confederazione». Ciò vale in particolare anche per le organizzazioni ai sensi dell'articolo 2 capoverso 4 LOGA che sono attribuibili all'Amministrazione federale in quanto vengono affidati loro compiti amministrativi.

Art. 2 Campo d'applicazione

Capoverso 1

La lettera a risulta dall'articolo 2 capoverso 2 lettera b LSIn e corrisponde all'attuale capoverso 1.

Lettera b: il campo d'applicazione per l'esercito è nuovo e risulta dall'articolo 2 capoverso 2 lettera d LSIn.

Capoverso 2

L'espressione «Amministrazione federale» utilizzato nell'articolo 2 capoverso 2 lettera b LSIn comprende sia l'Amministrazione federale centralizzata, sia quella decentralizzata (cfr. messaggio LSIn, pag. 2625), per cui in linea di principio il campo d'applicazione viene esteso alle unità amministrative dell'Amministrazione federale decentralizzata. Fondandosi sull'articolo 2 capoversi 3 e 4 LSIn, il Consiglio federale ha tuttavia la possibilità di limitare il campo d'applicazione della LSIn. Analogamente all'Amministrazione federale decentralizzata, ora anche le organizzazioni di cui all'articolo 2 capoverso 4 LOGA sono assoggettate alla LSIn (cfr. art. 2 cpv. 2 lett. e LSIn; l'espressione «compiti amministrativi» comprende soltanto le attività sovrane; possono così rientrarvi eventualmente anche compiti dell'amministrazione di necessità, se sono sovrani [ipotizzabili p. es. nell'ambito di una procedura d'acquisto], ciò che però dovrebbe costituire l'eccezione). Anche in questo caso il Consiglio federale ha tuttavia la possibilità, sulla base dell'articolo 2 capoverso 3 LSIn, di limitare il campo d'applicazione della LSIn alle organizzazioni rilevanti per la sicurezza. Sia per l'Amministrazione federale decentralizzata, sia per le organizzazioni menzionate ai sensi della LOGA, il campo d'applicazione dell'OIAM e delle rimanenti ordinanze d'esecuzione LSIn va definito in modo uniforme nell'OSIn, motivo per cui nell'OIAM si prevede unicamente un rinvio in tal senso.

I contenuti attuali del capoverso 2 non costituiscono una lista positiva esaustiva e possono pertanto essere stralciati senza sostituzione (per un'autorità o un servizio è possibile impegnarsi volontariamente a rispettare l'OIAM sempreché non sussistano disposizioni contrarie del diritto federale).

Art. 5 Sistemi IAM

Capoverso 1: oltre agli organi responsabili dell'Amministrazione federale centrale sinora elencati nell'IAM, vengono elencati gli ulteriori organi federali dell'Amministrazione federale centrale responsabili (lett. a n. 2, d e f) di sistemi IAM.

Lett. a n. 1: giacché il settore Trasformazione digitale e governance delle TIC della Cancelleria federale è competente per il sevizio standard eIAM all'interno dell'Amministrazione federale, ai fini

di una gestione coerente, tale responsabilità è ora estesa anche alla parte relativa all'AGOV di tale servizio standard.

Lett. c: invece della Base d'aiuto alla condotta (BAC) si menziona l'Aggruppamento Difesa, poiché in generale in futuro la responsabilità dovrebbe incombergli; in che modo dovrà essere concretamente disciplinata la responsabilità all'interno della Difesa non dovrebbe essere oggetto della normativa dell'OIAM.

Capoverso 2: attualmente non ha luogo alcun controllo del trattamento dei dati personali in sistemi IAM. In base all'articolo 26 lettera e LSIn, che prevede un controllo periodico del trattamento di dati personali da parte di un servizio esterno, riguardo ai sistemi IAM dell'Amministrazione federale centrale viene inserito un relativo capoverso supplementare.

Capoverso 3: tenuto conto delle autonomie organizzative – più o meno pronunciate – dell'esercito, delle unità amministrative dell'Amministrazione federale decentralizzata e delle organizzazioni secondo l'articolo 2 capoverso 4 LOGA, a livello di ordinanza occorre stabilire solamente che gli organi menzionati sono sempre responsabili per i propri sistemi IAM. Per lo stesso motivo, presso questi organi si rinuncia a prevedere obbligatoriamente un controllo periodico del trattamento di dati personali da parte di un organo esterno.

Per quanto riguarda i sistemi IAM dell'esercito occorre inoltre evidenziare che essi approvvigionano i sistemi fondamentali dell'esercito per gli impieghi, mentre i sistemi IAM ai sensi dell'articolo 5 capoverso 1 lettera c approvvigionano i sistemi dell'amministrazione militare. In virtù di norme giuridiche differenti in materia di trattamento dei dati e responsabilità, i sistemi IAM in questione dovranno essere distinti e assoggettati separatamente all'OIAM.

Capoverso 4: in virtù dell'articolo 84 capoverso 3 LSIn, l'OIAM si applica per analogia anche alle autorità assoggettate di cui all'articolo 2 capoverso 1 lettere a e c–e LSIn, sempreché queste non emanino proprie disposizioni. Affinché tale costrutto funzioni, le altre autorità assoggettate dovranno quanto meno stabilire chi, nel loro ambito, detiene la responsabilità a livello di diritto in materia di protezione dei dati.

Capoverso 5: in virtù dei nuovi capoversi 2–4, l'attuale capoverso 2 diventa il capoverso 5, riprendendone integralmente il relativo contenuto.

Art. 6 lett. b n. 3

Anche qui (cfr. commento ad art. 5 cpv. 1 lett. c sopra) si deve ora menzionare l'Aggruppamento Difesa in luogo della BAC.

Art. 7 lett. b

Le persone che si avvalgono di AGOV allo scopo di usufruire dei servizi per il Governo elettronico devono poter contare su un servizio di contatto chiaro per l'esercizio del proprio diritto di correzione e cancellazione dei dati. Come per il diritto di lettura, anche in questo caso si tratta dell'organo responsabile ai sensi dell'articolo 5.

Art. 9 lett. b

Nell'ambito dell'AGOV, nel sistema eIAM non sono gestiti unicamente i dati personali di utenti delle applicazioni (per il Governo elettronico) della Confederazione, bensì anche i dati degli utenti dei sistemi d'informazione dei Cantoni e dei Comuni. Sovente si tratta delle medesime persone che si avvalgono talora di un'applicazione della Confederazione e talvolta di un'applicazione cantonale o comunale per usufruire dei rispettivi servizi amministrativi digitali. L'obiettivo di AGOV è far sì che gli utenti non debbano creare un'identità elettronica per ciascun servizio per poi doversi autenticare in occasione di ogni singolo accesso.

Art. 11 cpv. 2 e 3

I capoversi 2 e 3, secondo cui nei sistemi IAM non possono essere trattati profili personali e, in assenza di una base legale specifica in materia, non vi si possono trattare neanche dati personali degni di particolare protezione devono essere rielaborati, da un lato, in virtù dell'articolo 20 capoverso 2 LSIn e, dall'altro, in virtù della revisione totale della legge sulla protezione dei dati.

Capoverso 2: al divieto del trattamento di profili della personalità subentra un divieto di profilazione nonché di profilazione a rischio elevato (cfr. art. 5 lett. f e g LPD). In linea di principio, questo divieto comprende qualsiasi tipo di trattamento automatizzato di dati personali che consiste nel loro

utilizzo per valutare determinati aspetti della personalità di una persona fisica, in particolare per analizzare o prevedere elementi concernenti il rendimento professionale, la situazione economica, la salute, le preferenze, gli interessi, l'affidabilità, il comportamento, il luogo di soggiorno e gli spostamenti di tale persona. Se però, ad esempio, i metadati e quindi il comportamento degli utenti vengono valutati allo scopo di rilevare irregolarità e potenziali attacchi informatici (*Fraud Detection*), questi processi di trattamento dei dati non rientrano nel concetto di profilazione della LPD, poiché l'obiettivo principale non è la raccolta e l'analisi dei più svariati aspetti personali di una determinata persona, bensì la tutela della sicurezza delle informazioni.

Poiché la nuova ordinanza sulla protezione dei dati del 31 agosto 2022 ha abrogato il capoverso 2 con effetto dal 1º settembre 2023, da questa data al 31 dicembre 2023 (la presente modifica entrerà in vigore il 1º gennaio 2024) vi sarà una lacuna nell'ambito del divieto di trattamento di profili personali o della profilazione e della profilazione a rischio elevato che tuttavia, a causa della breve durata, dovrebbe essere accettabile.

Capoverso 3: i dati biometrici, che identificano chiaramente una persona, saranno considerati, genericamente, dati personali degni di particolare protezione. Per il loro trattamento viene però creata una base generale nell'articolo 20 capoverso 2 LSIn. Secondo l'allegato (lett. a n. 13), questi dati biometrici potranno quindi essere trattati, in linea di principio, in tutti i sistemi IAM nei quali ciò risulti necessario per l'identificazione in funzione dei rischi. Si veda in merito anche il commento all'allegato lettera a più avanti.

Art. 12 cpv. 4

Affinché possa svolgere la funzione di intermediazione di identità elettroniche riconosciute anche dei Cantoni (broker ID), il servizio IAM della Confederazione può ottenere automaticamente dati provenienti dai sistemi IAM dei rispettivi Cantoni. I processi, le interfacce e le misure di sicurezza sono oggetto delle istruzioni di cui all'articolo 24 capoverso 2 e dell'accordo di cui all'articolo 24 capoverso 1 lettera b.

Art. 13 cpv. 4 lett. a

Per motivi di chiarezza, alla lettera a si afferma esplicitamente che la base giuridica in questione dovrà prevedere (anche) il trattamento dei dati da mettere a disposizione.

Art. 14 cpv. 2

Questa disposizione rimane invariata sotto il profilo materiale, tuttavia il rimando non va più fatto all'articolo 2*a* della legge federale del 3 ottobre 2008[23] sui sistemi d'informazione militari (LSIM), bensì alla LSIn.

Titolo prima dell'art. 18 nonché art. 18 cpv. 1 e 2

La sicurezza delle informazioni e il rispetto delle relative direttive non devono applicarsi esclusivamente ai sistemi IAM, ma anche ai servizi di elenchi. Ciò vale anche per offerenti esterni alla Confederazione di servizi di elenchi, in particolare se non gestiscono già un sistema IAM. Il testo dell'ordinanza viene quindi integrato di conseguenza.

Inoltre, nell'ultima parte del periodo del capoverso 2 viene stralciato il termine «predefiniti», cosicché si parla ancora solamente di «requisiti minimi» (il termine stralciato non apporta alcun valore aggiunto). La disposizione rimane invariata sotto il profilo materiale.

Art. 20 Sistema globale IAM

Secondo l'attuale articolo 20 in vigore, i sistemi IAM dell'Amministrazione federale possono essere collegati in modo ottimale tra loro nonché con i sistemi IAM dei Servizi del Parlamento o dell'esercito per permettere una ripartizione dei compiti efficiente. Ciò significa anche che i dati degli utenti possono essere scambiati tra loro come in una federazione di dati. Questi sistemi IAM dovranno quindi poter essere collegati anche con i rimanenti sistemi IAM della Confederazione (p. es. dei Tribunali federali), per cui in futuro si parlerà di sistemi IAM *della Confederazione*.

Come finora e conformemente alla prassi, un collegamento tra sistemi IAM esterni e sistemi IAM della Confederazione (sistema singolo o sistema globale) dovrà essere possibile (cfr. attuale

[23] RS **510.91**

art. 21, che prevede che, a determinate condizioni, i sistemi IAM esterni possano essere collegati ai sistemi IAM della Confederazione). Con la modifica ciò sarà previsto già nell'articolo 20.

Art. 21 Frase introduttiva e lett. a

In generale: l'articolo 21 disciplina le condizioni alle quali i sistemi IAM esterni (alla Confederazione) possono essere collegati ai sistemi IAM della Confederazione. Questo collegamento sarà sempre completo. Tuttavia ciò non significa affatto una rinuncia a ogni sovranità in materia di dati. Secondo l'articolo 9 lettera a, per esempio, possono essere trattati unicamente dati personali che utilizzano risorse dell'Amministrazione federale; questa è una condizione quadro aggiuntiva anche per l'articolo 21. Se, per esempio, un Cantone si collega a IAM Confederazione gestisce però soltanto i dati personali necessari per l'utilizzo della risorsa federale, in nessun caso tutti i dati forfettariamente. Inoltre, al riguardo non è prevista una messa a disposizione passiva, bensì un invio proattivo da parte del sistema IAM cantonale. Il Cantone ha quindi sempre il controllo su quali dati di quali persone vengono divulgati.

Frase introduttiva: se un sistema IAM esterno secondo l'articolo 21 deve essere collegato con i sistemi IAM della Confederazione è, in particolare, imperativo per motivi di sicurezza che i gestori in questione, fatta eccezione per i Cantoni, si assoggettino all'OIAM. Per il collegamento dei sistemi IAM dei Cantoni a quelli della Confederazione, è essenziale che nei sistemi IAM cantonali venga garantita una sicurezza delle informazioni almeno equivalente. Tuttavia, non è necessario che tutti i (restanti) requisiti posti dall'OIAM siano applicati contemporaneamente anche ai Cantoni. Ciò è opportuno anche alla luce della ripartizione delle competenze tra la Confederazione e i Cantoni sancita dalla Costituzione. La frase introduttiva è completata in base a quanto esposto sopra.

La lettera a corrisponde alla versione attuale, tuttavia completata con i sistemi IAM del Principato del Liechtenstein. Si risponde in tal modo a una richiesta di quest'ultimo.

Art. 24 cpv. 1 lett. a

Affinché l'AGOV possa espletare appieno i suoi benefici, il sistema IAM della Confederazione deve essere collegato con quelli dei Cantoni e dei Comuni interessati. Questo caso è ora disciplinato nell'articolo 24. Per motivi di sistematicità, nel capoverso 1 lettera a è ora integrata la fattispecie summenzionata. Per effettuare il collegamento è sancito un accordo ai sensi del capoverso 1 lettera b che disciplina il rapporto sotto il profilo legale, organizzativo e tecnico. Fanno parte delle disposizioni organizzative anche le disposizioni in materia di finanze ai sensi dell'articolo 11 capoverso 4 LMeCA. Possono essere collegati unicamente i sistemi che dispongono delle necessarie basi legali, perché il loro utilizzo riguarda i diritti e gli obblighi di privati in relazione alla protezione dei dati o al diritto procedurale (art. 11 cpv. 5 LMeCA).

Allegato

Modifiche in virtù della LSIn

Lettera a: secondo l'articolo 20 capoverso 2 LSIn i dati biometrici vengono trattati non soltanto per persone figuranti in sistemi gestiti dall'esercito, bensì per tutte le persone figuranti in sistemi IAM (finora secondo l'art. 2*a* LSIM ciò era possibile soltanto per sistemi dell'esercito). I dati biometrici che attualmente sono menzionati alla lettera g, saranno integrati nella lettera a (n. 13) (la lettera g può così essere abrogata). Tuttavia, essi non potranno figurare sistematicamente in tutti i sistemi IAM ed essere impiegati a piacimento. Piuttosto, occorrerà verificare per ogni sistema IAM e per ogni scenario d'utilizzo se l'impiego di dati biometrici è necessario ai fini dell'identificazione delle persone in funzione dei rischi. Inoltre per mancanza di una base legale formale i dati biometrici non potranno essere resi noti tra i sistemi di diversi responsabili. Infine, venuta meno l'autorizzazione di accesso, i dati biometrici dovranno essere distrutti (cfr. art. 20 cpv. 3 LSIn e art. 14 cpv. 2 OIAM).

L'attuale numero 11 (Immagine del viso per documenti d'identificazione) dovrà figurare in un numero separato (n. 14), poiché l'immagine del viso non biometrica o la semplice fotografia va registrata in tutti i sistemi IAM (e dunque in tutte e tre le colonne). In futuro si parlerà soltanto di «Immagine del viso», poiché non si intendono solamente immagini su documenti d'identificazione ma anche, ad esempio, le immagini su Skype.

Lettera c: la registrazione del numero dell'ufficio è prevista anche nei sistemi IAM con persone di cui agli articoli 8 e 9 lettera b, poiché i processi di supporto del posto di lavoro digitale necessitano di questa informazione.

Lettera e: nel numero 7 si precisa che le password dovranno essere protette mediante cifratura sufficientemente confidenziale o «hashing with salting» sufficientemente affidabile. Ciò in effetti dovrebbe essere ovvio (tutte le norme di gestione interne per le password contengono la direttiva di memorizzarle esclusivamente cifrate, salate o mediante funzione hash). Tuttavia, nella prassi capita di tanto in tanto che le password siano mal protette e possano essere «violate»

Lettera f: in questa sede, conformemente al tenore della LSIn, (frase introduttiva e n. 2) si procede a due adeguamenti linguistici.

Lettera g: abrogata (v. commento sopra).

Modifiche in virtù della LMeCA

Lett. a n. 4 e 5, lett. c n. 2 e lett. e n. 11

Tra i dati personali trattati nell'AGOV vi sono anche la nazionalità, il luogo di nascita, l'indirizzo postale privato e la qualità dell'autenticazione. Tali dati sono trasmessi ai sistemi d'informazione utenti nell'ambito dei servizi di autenticazione. Le rispettive applicazioni tecniche utilizzano tali dati per il trattamento degli affari (p. es. procedure di autorizzazione, tassazione, aiuti finanziari, servizi ecc.). La nazionalità e il luogo di nascita saranno trattati anche nell'ambito della futura Id-e (cfr. art. 2 cpv. 2 lett. e e f dell'avamprogetto di legge federale del 29 giugno 2022 sul mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici [Legge sull'Id-e, LIdE]). Nell'ambito delle applicazioni per il Governo elettronico è inoltre necessario conoscere la qualità dell'autenticazione per l'ulteriore trattamento da parte delle applicazioni tecniche. I requisiti per la verifica dell'identità possono variare a seconda dell'applicazione tecnica e dell'oggetto della prestazione.

Per il trattamento dei dati, i sistemi d'informazione utenti devono disporre delle necessarie basi legali (in materia di protezione dei dati; art. 11 cpv. 5 LMeCA). I Cantoni devono creare le basi legali necessarie nelle loro legislazioni.

3.3 Ordinanza sui controlli di sicurezza relativi alle persone (OCSP)

Titolo

Con l'espressione «controllo di sicurezza relativo alle persone», oltre ai controlli di sicurezza relativi alle persone (CSP) secondo la LSIn, si riassumono tutti i controlli nonché tutte le valutazioni e le verifiche ai sensi di leggi diverse da quest'ultima a cui, direttamente o per analogia, si applica la procedura dei CSP secondo la LSIn.

Ingresso

L'ingresso rinvia a tutte le norme di legge che conferiscono al Consiglio federale una competenza normativa nell'ambito dei CSP.

Sezione 1: Disposizioni generali

Art. 1 Oggetto

Con l'OCSP si intende emanare un'ordinanza del Consiglio federale per tutte le competenze esecutive di cui all'articolo 48 LSIn concernenti i CSP ai sensi della LSIn e i controlli, le valutazioni e le verifiche ai sensi di altre leggi.

Nella sistematica della LSIn il Consiglio federale è, in linea di principio, una tra le molteplici autorità assoggettate, tutte equiparate, ai sensi dell'articolo 2 capoverso 1 LSIn. Conformemente all'articolo 84 capoverso 1 LSIn, in quanto autorità assoggettata esso è responsabile dell'emanazione delle disposizioni esecutive necessarie per il suo ambito di competenza. Per conseguire un'armonizzazione dei livelli di sicurezza tra le autorità assoggettate, nell'articolo 84 capoverso 3 LSIn il legislatore ha stabilito che le disposizioni esecutive che il Consiglio federale emana per il proprio ambito di competenza si applichino per analogia anche alle altre autorità assoggettate, sempreché esse non emanino disposizioni esecutive proprie. Vi sono tuttavia settori per i quali la LSIn priva le altre autorità assoggettate di questa competenza «opt-out». Non ha quindi senso, che sia il Consiglio federale sia, per esempio, il Parlamento, i tribunali federali o la Banca nazionale definiscano ciascuno una procedura di verifica per i controlli di sicurezza relativi alle persone o disciplinino l'organizzazione dei servizi specializzati CSP. A tal fine può esistere un unico disciplinamento e il legislatore ha espressamente conferito al Consiglio federale la pertinente competenza legislativa. Se il Consiglio federale emana disposizioni esecutive in quanto «autorità assoggettata» (cfr. p. es. art. 26 e 28 LSIn), le altre autorità assoggettate possono emanare disposizioni esecutive proprie. Se la legge conferisce espressamente al Consiglio federale una competenza esecutiva (cfr. p. es. art. 48, 73, 80 o 83 cpv. 3 LSIn), esso è l'unico competente. In questi casi non esiste una propria competenza normativa per le altre autorità federali.

Nell'articolo 48 LSIn il legislatore ha espressamente conferito *unicamente* al Consiglio federale la competenza di emanare disposizioni esecutive sugli oggetti della normativa dei capoversi 1 e 2. In quanto autorità assoggettata di cui all'articolo 2 capoverso 1 LSIn il Consiglio federale svolge invece compiti esecutivi specifici per il settore proprio, ovvero l'Amministrazione federale e l'esercito. Si veda anche il commento all'articolo 2.

Art. 2 Campo d'applicazione

L'OCSP si applica, in linea di principio, a tutte le autorità e organizzazioni che sottostanno alla LSIn. Per le unità amministrative decentralizzate e le organizzazioni con compiti amministrativi ai sensi dell'articolo 2 capoverso 4 LOGA il campo d'applicazione è limitato: soltanto quelle che rientrano nel campo d'applicazione dell'OSIn rientrano in quello dell'OCSP per quanto riguarda i CSP secondo la LSIn. Le unità amministrative decentralizzate che rientrano nel campo d'applicazione della LPers possono parimenti essere interessate dalle verifiche dell'affidabilità di cui all'articolo 20*b* LPers e, in tale contesto, rientrare nel campo d'applicazione dell'OCSP.

L'OCSP si applica anche alle autorità federali assoggettate ai sensi dell'articolo 2 capoverso 1 LSIn. Nell'articolo 48 LSIn il legislatore ha infatti conferito al Consiglio federale la competenza esclusiva di disciplinare le modalità della procedura di controllo e l'organizzazione dei servizi specializzati CSP. Per contro, le autorità assoggettate rimangono competenti per l'emanazione dei propri elenchi di funzioni o per la designazione dei servizi promotori e decisori (v. commento ad art. 1).

Sezione 2: Elenchi delle funzioni

Art. 3 Attribuzione

Capoversi 1–3: per ogni tipo di CSP è emanato un proprio elenco delle funzioni quale allegato all'ordinanza. Secondo l'articolo 41*b* capoverso 2 della legge federale del 16 dicembre 2005[24] sugli stranieri e la loro integrazione e l'articolo 6*a* capoverso 2 della legge del 22 giugno 2001[25] sui documenti d'identità, nell'ambito del rilascio di documenti d'identità, anche per determinate persone possono essere eseguiti controlli di sicurezza ai sensi dall'articolo 6 dell'attuale OCSP. Nell'OCSP non figurerà, volutamente, alcun elenco delle funzioni a tale scopo. Qualora fosse imperativo un CSP, esso sarebbe coperto attraverso una procedura di sicurezza relativa alle aziende presso l'impresa interessata.

Gli elenchi delle funzioni non possono contenere funzioni che non rispettano i rigidi presupposti degli articoli 10–14.

Le autorità assoggettate secondo l'articolo 2 LSIn che non rientrano nell'ambito di competenza del Consiglio federale (p. es. il Ministero pubblico della Confederazione) dovranno emanare autonomamente i propri elenchi delle funzioni.

Capoverso 4: il contenuto di questo capoverso è conforme al vigente disciplinamento di cui all'articolo 1 capoverso 3 OCSPN. Già nella fase progettuale i progettisti trattano informazioni classificate CONFIDENZIALE o SEGRETO, ragion per cui l'esigenza di un controllo dell'affidabilità sussiste già in questo momento. Inserendo i progettisti di un nuovo impianto nucleare e titolari di un'autorizzazione quadro si copre quindi l'intero ciclo in cui devono essere trattate informazioni classificate CONFIDENZIALE o SEGRETO.

Art. 4 Modifica

Per contenere il numero dei controlli entro i limiti perseguiti, nell'allestire e nell'aggiornare gli elenchi delle funzioni in cui figurano le funzioni da controllare è necessario controllare meglio di quanto fatto sinora la legalità delle iscrizioni. Il DDPS dovrà quindi gestire a livello centrale gli elenchi delle funzioni e aggiornarli costantemente su richiesta dei dipartimenti e della CaF. A tale scopo occorre coinvolgere il servizio specializzato della Confederazione per la sicurezza delle informazioni. La società nazionale di rete presenta al Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni sottoporrà le proposte di modifica dell'elenco delle funzioni secondo la LAEl soltanto dopo aver sentito la Commissione dell'energia elettrica.

Art. 5 Pubblicazione, conservazione e comunicazione

I servizi e le persone che per l'adempimento dei propri compiti devono poter consultare elenchi delle funzioni non pubblicati, potranno farlo tramite il DDPS. Si tratta in particolare dei servizi promotori e degli organi di sicurezza secondo l'OSIn. Riguardo alla sensibilità sotto il profilo della sicurezza degli elenchi delle funzioni, v. numero 3.5 lettera e.

Art. 6 Verifica dell'aggiornamento

Capoverso 1: la verifica della correttezza degli elenchi delle funzioni richiede una considerevole mole di lavoro. Vi è però una chiara necessità di tenere aggiornati gli elenchi delle funzioni e di avere uno sguardo critico sulle classificazioni delle funzioni una volta che sono state effettuate, affinché siano sottoposte a un controllo sempre soltanto le persone per la cui funzione è necessaria una verifica in virtù del rischio potenziale. Occorre quindi definire un approccio pragmatico di verificare in generale gli elenchi delle funzioni ogni tre anni nonché, nello specifico, in caso di riorganizzazioni o modifiche di compiti.

Capoverso 2: alla luce delle esperienze acquisite, è necessario garantire che la verifica della correttezza degli elenchi delle funzioni sia effettivamente eseguita. Occorre pertanto disciplinare l'obbligo di presentare rapporto in tal merito al DDPS. Se dalla verifica della correttezza degli elenchi delle funzioni risulta una necessità di modifica di tali elenchi, questi ultimi dovranno essere rielaborati di conseguenza.

Art. 7 Controllo straordinario

Se una funzione adempie i criteri per un controllo, ma non è ancora stata inserita nel relativo elenco delle funzioni, è possibile svolgere un controllo secondo l'articolo 29 capoverso 3 LSIn

[24] RS **142.20**
[25] RS **143.1**

previo consenso dell'autorità assoggettata. A livello di Amministrazione federale occorre delegare la corrispondente competenza decisionale per un controllo eccezionale al DDPS, che consulta il servizio specializzato della Confederazione per la sicurezza delle informazioni. La domanda è presentata dalla CaF o dai dipartimenti che, in via preliminare, consultano i propri incaricati della sicurezza delle informazioni. Gli elenchi delle funzioni dovranno essere aggiornati di conseguenza. Le altre autorità assoggettate disciplinano le competenze autonomamente.

Art. 8 Controlli presso gli impiegati cantonali e i terzi

Capoverso 1: in linea di principio, spetta ai Cantoni stabilire le funzioni di impiegati cantonali che sono soggette a un controllo di cui all'articolo 29 capoverso 1 lettera b LSIn. Affinché sia possibile assicurare una gestione uniforme, in questo ambito il DDPS va tuttavia dotato di una funzione regolatrice. A tale scopo dovrà consultare preliminarmente il servizio specializzato della Confederazione per la sicurezza delle informazioni.

Capoverso 2: le funzioni di terzi, che eseguono un mandato per conto di un'autorità o un'organizzazione assoggettata, che comporta lo svolgimento di un'attività sensibile sotto il profilo della sicurezza, non possono essere prestabilite, bensì risultano dalle necessità dei singoli mandati. Per garantire anche in questo caso la necessità del controllo, le decisioni dovranno essere prese a livello centrale. La decisione riguarda la verifica della legalità dell'esecuzione del controllo e la questione: nel caso concreto, siamo effettivamente in presenza di un'attività sensibile sotto il profilo della sicurezza?

Art. 9 Controllo di affidabilità straordinario da parte dell'Ispettorato federale della sicurezza nucleare

Il contenuto di questo articolo corrisponde al vigente disciplinamento di cui all'articolo 5 OCSPN.

Sezione 4: Attribuzione ai livelli di controllo

L'attribuzione della verifica dell'affidabilità secondo la legge sull'asilo al livello di controllo di sicurezza di base viene già stabilita nell'articolo 29*a* della legge del 26 giugno 1998[26] sull'asilo (LAsi) e non deve quindi più essere disciplinata nell'ordinanza.

Art. 10 Controlli di sicurezza relativi alle persone secondo la LSIn

Capoverso 1 lettera a: con «trattamento» si intende ogni gestione di informazioni, indipendentemente dai mezzi e dalle procedure applicati, in particolare la raccolta, la conservazione, la memorizzazione, l'utilizzazione, la modificazione, la comunicazione, l'archiviazione o la distruzione di informazioni. Determinante è se, nell'ambito della funzione, il trattamento di informazioni classificate è necessario per l'adempimento dei compiti. Per quanto riguarda il criterio della regolarità per l'assoggettamento a CSP, confronta il messaggio LSIn (n. 1.25, pag. 2597, nonché commento ad art. 29 LSIn, pag. 2649 seg.).

Capoverso 1 lettera b: con «l'amministrazione, l'esercizio, la manutenzione e la verifica di mezzi informatici» sono prese in considerazione tutte le attività di cui all'articolo 5 lettera b LSIn che contemplano diritti d'accesso particolari ai mezzi informatici della Confederazione oppure le attività il cui esercizio potrebbe comportare il rischio di pregiudicare considerevolmente gli interessi pubblici di cui all'articolo 1 capoverso 2 LSIn, ad esempio attraverso il sabotaggio. Se gli utenti di mezzi informatici esercitano un'attività sensibile sotto il profilo della sicurezza, si decide unicamente in base alla classificazione delle informazioni da trattare. Di conseguenza, vengono inclusi principalmente amministratori e responsabili delle applicazioni dei sistemi. Il termine «esercizio» si riferisce all'attività dei fornitori di prestazioni ai sensi dall'articolo 19 LSIn. Tale termine va chiaramente distinto dall'espressione «gestire sistemi d'informazione» utilizzata nella legislazione sulla protezione dei dati per disciplinare l'impiego di sistemi d'informazione da parte dei beneficiari di prestazioni (cfr. p. es. art. 24 cpv. 1 LSIn). Attività sensibili sotto il profilo della sicurezza nell'ambito dello sviluppo o della creazione di sistemi d'informazione sono incluse nella lettera b quale parte dell'amministrazione e dell'esercizio.

Capoverso 1 lettera c: l'esclusione di locali o settori quali zone di sicurezza rappresenta una misura fisica di sicurezza delle informazioni, in particolare per proteggere locali dei server o determinati locali di condotta. Una zona di sicurezza deve essere protetta adeguatamente. Le persone che

[26] RS **142.31**

devono avere accesso a zone di sicurezza 1 vanno quindi assoggettate a un controllo di sicurezza di base.

Capoverso 1 lettera d: se un trattato internazionale prevede un controllo, il livello di controllo si rifà alle pertinenti direttive del trattato. Se il trattato non contiene alcuna normativa specifica, il controllo avviene sempre soltanto al livello di controllo di sicurezza di base.

Capoverso 1 lettere a–c: v. commento al capoverso 1 lettere a–c.

Capoverso 2 lettere d ed e: le persone che svolgono attività sensibili sotto il profilo della sicurezza per il Servizio delle attività informative della Confederazione (SIC) o per la sua Autorità di vigilanza, il Servizio informazioni militare (SIM) o il servizio Azioni ciber ed elettromagnetiche (ACE) normalmente lo fanno in settori estremamente sensibili. Le loro attività vanno quindi attribuite al livello di controllo di sicurezza relativo alle persone ampliato.

Capoverso 2 lettera f: v. commento al capoverso 1 lettera d.

Art. 11 Verifica dell'affidabilità secondo la LPers

Capoverso 1 lettera a: nel caso delle attività di sovranità nazionale degli impiegati che sono in servizio all'estero e del personale del DFAE soggetto al regime dell'obbligo di trasferimento (cfr. art. 3 lett. a e b dell'ordinanza del DFAE del 20 settembre 2002[27] concernente l'ordinanza sul personale federale; O-OPers–DFAE) possono essere pregiudicati considerevolmente interessi essenziali della Confederazione. Le persone che esercitano queste attività saranno sottoposte al livello di controllo di sicurezza di base.

Capoverso 1 lettera b: potenziali danni finanziari di 50–500 milioni di franchi vengono ritenuti considerevoli nel presente contesto.

Capoverso 1 lettera c: a seconda della loro interpretazione, la gamma di compiti di perseguimento penale o di polizia può essere molto grande. Il campo di applicazione di questo motivo del controllo deve pertanto essere limitato ai compiti e alle organizzazioni che possono pregiudicare considerevolmente gli interessi pubblici della Confederazione.

Capoverso 2 lettere a e b: i detentori delle funzioni per i quali la competenza di costituire, modificare e risolvere il rapporto di lavoro spetta al Consiglio federale secondo l'articolo 2 capoverso 1 dell'ordinanza del 3 luglio 2001[28] sul personale federale (OPers) o al capo del dipartimento secondo l'articolo 1bis OPers, soddisfano regolarmente almeno uno dei motivi del controllo di cui all'articolo 20*b* capoverso 1 lettere a e b LPers. Ciò vale anche per i detentori delle funzioni di cui all'articolo 2 capoverso 1 lettera e LPers. Visto l'elevato danno di reputazione in caso di inadempienze di questi detentori, essi vanno assoggettati al controllo di sicurezza ampliato.

Capoverso 2 lettere a e b: i detentori delle funzioni per i quali, secondo l'articolo 2 capoverso 1 OPers, spetta al Consiglio federale la competenza di costituire, modificare e risolvere il rapporto di lavoro, soddisfano regolarmente uno dei motivi del controllo di cui all'articolo 20b capoverso 1 lettere a e b LPers. In virtù dell'elevato danno reputazionale ivi connesso in caso di inadempienze di suddetti detentori, essi vanno assoggettati al livello di controllo di sicurezza relativo alle persone ampliato.

Capoverso 2 lettera c: per responsabile di unità organizzative decentralizzate si intendono i direttori. Anch'essi, a causa dell'elevato danno di reputazione in caso di inadempienze, vanno sottoposti a un CSP ampliato (cfr. art. 11 cpv. 2 lett. a e b). Tuttavia, rientra in queste lettere soltanto chi è assoggettato alla LPers. Per esempio, non rientrano nel campo d'applicazione della LPers la direzione delle commissioni extraparlamentari o della FINMA. Per le rimanenti unità organizzative decentralizzate sono determinanti i motivi del controllo ai sensi della LSIn.

Capoverso 2 lettera d: in questo contesto, un potenziale danno finanziario di oltre 500 milioni di franchi corrisponde alla ripercussione «elevata» e uno di oltre 1 miliardo di franchi alla ripercussione «molto elevata».

Capoverso 2 lettera e: una prestazione contraria alle prescrizioni o non appropriata del personale di fedpol nell'ambito della lotta contro le forme più gravi di criminalità di competenza federale, quali la lotta al terrorismo, all'estremismo violento e alla criminalità organizzata nonché ad altre

[27] RS **172.220.111.343.3**
[28] RS **172.220.111.3**

forme di criminalità transnazionale può compromettere considerevolmente gli interessi pubblici della Confederazione.

Capoverso 2 lettera f: anche le attività dei dipendenti dei servizi specializzati CSP secondo l'articolo 16 capoverso 1, considerate attività di polizia di sicurezza, dovranno essere sottoposte al controllo di sicurezza ampliato.

Art. 12 Controlli secondo la legge militare del 3 febbraio 1995[29] (LM)

Capoverso 1 lettera a: non ogni attività all'estero di militari in uniforme rientra nella definizione della «rappresentanza sovrana» della Svizzera. La mera rappresentanza visiva della Svizzera o attività nell'ambito di contingenti di truppe internazionali non deve bastare per una verifica dell'affidabilità. Sono necessarie attività che prevedono competenze decisionali sovrane con ripercussioni all'esterno in rappresentanza della Svizzera.

Capoverso 1 lettera b: v. commento all'articolo 11 capoverso 2 lettera b.

Capoverso 1 lettera c: in caso di bisogno, per decidere se una persona soggetta all'obbligo di leva non debba essere reclutata oppure se un militare debba essere degradato o escluso dall'esercito, è sufficiente un controllo di sicurezza di base.

Capoverso 2: finora era possibile svolgere un controllo di sicurezza relativo alle persone per tutti gli aspiranti, a prescindere da un motivo materiale del controllo. Questa possibilità viene meno con la nuova OCSP. In futuro potranno essere controllati soltanto in presenza di un suddetto motivo ai sensi della LSIn o della LM. Se la persona interessata dispone già di un CSP valido ed è aspirante a una funzione che ne presuppone uno, il CSP può essere ripetuto anzitempo purché sia scaduto il termine minimo di cui all'articolo 43 capoverso 1 LSIn.

Capoversi 3 e 4: sotto il profilo del contenuto questo capoverso corrisponde in buona parte all'attuale disciplinamento di cui all'articolo 5 capoversi 2 e 3 OCSP.

Art. 13 Controlli di affidabilità secondo la legge federale del 21 marzo 2003[30] sull'energia nucleare (LENu)

Dal punto di vista del contenuto questo articolo corrisponde sostanzialmente all'attuale disciplinamento dell'articolo 3 OCSPN, che integra i progettisti di un nuovo impianto nucleare e i titolari di un'autorizzazione quadro. Il capoverso 1 lettera b sostituisce varie categorie di persone per le quali, secondo l'OCSPN, era necessario un CSP con la menzione di attività rilevanti sotto il profilo della sicurezza come motivo del controllo, in analogia ad altre disposizioni orientate alle attività nell'OCSP. La formulazione «seriamente compromettere» esclude le attività il cui potenziale di danno in caso di esercizio infedele non giustifica un CSP. Il capoverso 1 lettera b segue i principi della sicurezza nucleare e dell'utilizzazione dell'energia nucleare, in virtù dei quali, a titolo precauzionale, devono essere adottati tutti provvedimenti necessari in base all'esperienza e allo stato della scienza e della tecnica e, sempreché siano appropriati, contribuiscono a un'ulteriore riduzione della minaccia (art. 4 cpv. 3 LENu). Per quanto riguarda la cerchia di persone la disposizione corrisponde alla prassi.

Art. 14 Verifiche dell'affidabilità secondo la LAEI

Sulla base della Strategia nazionale per la protezione delle infrastrutture critiche 2018–2022 sono «informazioni critiche» tutte le informazioni che sono essenziali per il funzionamento della sicurezza d'approvvigionamento, delle applicazioni critiche o delle infrastrutture critiche. Sono «informazioni estremamente critiche» tutte le informazioni assolutamente essenziali per il funzionamento della sicurezza d'approvvigionamento, delle applicazioni critiche o delle infrastrutture critiche.

Devono essere sottoposti a un controllo di sicurezza relativo alle persone, ad esempio, le persone che hanno un accesso autonomo a impianti elettrici, in quanto sono in grado di influire entro breve tempo sulla sicurezza dell'approvvigionamento.

Sezione 5: Esecuzione

Nell'ambito dei lavori preparatori al progetto di ordinanza è stato altresì suggerito di prevedere termini massimi per la durata della valutazione del rischio per la sicurezza, in modo che i risultati siano disponibili entro un termine più attuabile. Alla luce delle esperienze fatte, occorre rinunciare

[29] RS **510.10**
[30] RS **732.1**

volutamente a questi termini. La durata della valutazione dipende in larga misura dalla possibilità di procurarsi i dati da raccogliere e dal loro contenuto effettivo. Un termine assoluto, in particolare termini troppo brevi, comporterebbe un aumento delle dichiarazioni di constatazione poiché non sarebbe possibile chiarire approfonditamente gli indizi di rischi o i dati non sarebbero disponibili in tempo utile.

Art. 15 Servizi promotori e decisori

Capoverso 1: i dipartimenti e la Cancelleria federale devono potere stabilire autonomamente, per l'Amministrazione federale, l'assegnazione di competenze più idonee per la propria organizzazione.

Capoverso 3: nel caso di una procedura di sicurezza relativa alle aziende, il servizio specializzato PSA è il servizio promotore e decisore. Se però, conformemente all'articolo 53 capoverso 2 LSIn, si rinuncia alla procedura e si esegue unicamente il CSP, il mandante avvierà la CSP dopo che l'incaricato della sicurezza delle informazioni del dipartimento ha verificato se un'attività sensibile sotto il profilo della sicurezza è effettivamente svolta dai dipendenti terzi. Inoltre il mandante è anche il servizio decisore e, nella pratica, solitamente il servizio d'acquisto.

Capoverso 4: questo capoverso corrisponde agli attuali articoli 2 capoverso 2 e 4 capoverso 1 OCSPN ed è completato dall'inserimento dei progettisti di un nuovo impianto nucleare e dei titolari di un'autorizzazione quadro (v. commento ad art. 4 cpv. 4).

Capoverso 6: affinché i servizi specializzati CSP possano svolgere il proprio lavoro in modo efficiente, devono sapere chi presso le singole autorità è competente per l'avvio dei controlli e per la decisione riguardante l'esercizio della funzione.

Capoverso 7: in virtù del fatto che continuano a essere avviati controlli mediante formulari fisici, il servizio promotore dovrà conservare questi documenti originali e li conserverà fintanto che l'interessato esercita l'attività sensibile sotto il profilo della sicurezza, ma al massimo dieci anni.

Art. 16 Servizi specializzati CSP

L'attuale sistema affermato consistente in due servizi specializzati CSP con differenti competenze va mantenuto.

Secondo l'articolo 16 capoverso 3 lettera d, il servizio specializzato CSP CaF deve verificare le funzioni della SEPOS nel DDPS che comprendono compiti di condotta nei confronti del servizio specializzato CSP DDPS. In particolare si tratta del segretario generale, del suo supplente nonché del responsabile del servizio specializzato CSP DDPS. Oltre a queste tre funzioni della SG-DDPS, il servizio specializzato CSP CaF non verifica altre funzioni di cui alla lettera d.

Per il resto, si applicano le prescrizioni sulla ricusazione di cui all'articolo 10 della legge federale del 20 dicembre 1968[31] sulla procedura amministrativa.

Art 17 Verifica delle condizioni per il controllo

Le autorità assoggettate sono responsabili di valutare la sensibilità sotto il profilo della sicurezza delle funzioni. Per i servizi specializzati CSP gli elenchi delle funzioni sono quindi vincolanti. Non possono verificare per ogni CSP avviato se la funzione è effettivamente sensibile sotto il profilo della sicurezza, poiché il relativo onere sarebbe sproporzionato. Per contro, possono e devono verificare se i controlli sono stati avviati correttamente. Incombe peraltro al servizio promotore provare che è disponibile il consenso della persona da controllare e che questo consenso soddisfa i requisiti posti all'articolo 6 capoverso 6 LPD.

I servizi specializzati verificano inoltre se sono disponibili le indicazioni necessarie per il controllo. Si tratta in particolare dei dati necessari all'identificazione della persona, dei luoghi di domicilio precedenti nonché i dati di contatto elettronici come l'indirizzo e-mail.

Art. 18 Collaborazione

Se vi fosse la possibilità di non rispondere alle domande sull'abuso di alcol o stupefacenti, su debiti personali, su occupazioni accessorie o simili appellandosi ai diritti fondamentali e, grazie a questo espediente, le corrispondenti informazioni non potessero confluire nella valutazione del rischio per la sicurezza, l'intero controllo di sicurezza sarebbe inefficace. Nell'ambito dell'obbligo di collaborazione, la persona sottoposta al controllo è quindi tenuta a cooperare all'accertamento dei fatti.

[31] RS **172.021**

Essa ha il diritto di non volere rispondere a determinate domande. I servizi specializzati avranno però il compito di valutare il rifiuto di informare o il rifiuto di presentare ulteriori documenti quali referti medici e test antidroga, poiché un certo margine di manovra per le domande sulla sfera segreta personale è lecito. Al riguardo occorre prendere in considerazione eventuali obblighi di segretezza legali della persona da controllare.

Art. 19 Raccolta dei dati

Capoverso 1: finora le consultazioni di banche dati avvenivano principalmente per il tramite del servizio specializzato CSP DDPS. Con l'entrata in vigore della LSIn e dell'OCSP, saranno i due servizi specializzati a raccogliere i dati dei casi loro assegnati. I servizi specializzati CSP non devono per forza ricorrere a tutti i mezzi disponibili per valutare il rischio. Ciò è importante in particolare nel controllo ampliato poiché la riduzione dei livelli di controllo non deve comportare un aumento massiccio dei costi dei CSP. Occorre quindi anche rinunciare consapevolmente a stabilire quali dati e quando dovranno essere raccolti e trattati. I servizi specializzati CSP possono valutare al meglio quali dati sono necessari per le loro valutazioni dei rischi.

Capoversi 2 e 3: l'audizione della persona interessata di cui all'articolo 34 capoverso 2 lettera d LSIn serve a tematizzare fatti che non risultano, o risultano soltanto in modo poco chiaro, dalle rimanenti raccolte di dati. Può essere eseguita anche in assenza di indizi relativi all'esistenza di un rischio per la sicurezza e la sua entità non è limitata. A causa del relativo onere, l'audizione dovrà limitarsi al minor numero di funzioni possibile. L'elenco è quindi esaustivo. In tutte le funzioni elencate i collaboratori interni ed esterni vengono equiparati. Nel caso di una ripetizione ordinaria del controllo di cui all'articolo 26, i servizi specializzati CSP decideranno liberamente sulla necessità dell'audizione se la situazione di rischio è praticamente immutata. Nella prassi, ciò sarà piuttosto un'eccezione.

Capoverso 4: per il chiarimento di particolari circostanze rilevanti per la sicurezza o per ottenere dati supplementari su un periodo di tempo più lungo, i servizi specializzati CSP potranno anche sentire terzi. Il capoverso 4 menziona nelle sue lettere a–c i gruppi di persone più importanti noti dalla prassi sinora applicata. Inoltre, a seconda del caso vi sono altre persone (p. es. familiari o ex partner commerciali) che dispongono di preziose informazioni. Queste persone vengono riassunte in una formulazione generale nella lettera d. Da più parti è stato proposto che con l'ordinanza si obblighino i terzi che possono essere interrogati a fornire informazioni veritiere. Le basi legali non prevedono tuttavia alcun obbligo di rispondere. Il terzo interessato può quindi rinunciare in ogni momento a fornire qualsivoglia informazione.

Art. 20 Assistenza amministrativa

I servizi specializzati CSP non raccolgono tutti i dati in modo autonomo. Ciò riguarda in particolare la raccolta di dati all'estero che, in linea di principio, avviene per il tramite di fedpol e del SIC. Soltanto questi servizi sono in grado di valutare l'affidabilità dei dati e delle fonti di dati.

Art. 21 Raggruppamento di procedure di controllo

Le funzioni contemplano le attività più disparate che possono soddisfare differenti motivi di controllo. Se per una persona vi sono svariati motivi di controllo, i controlli vanno raggruppati per motivi d'economia procedurale. Se una persona deve essere controllata da entrambi i servizi specializzati CSP, soltanto il servizio specializzato CSP CaF svolgerà il controllo. La scelta del servizio specializzato CSP CaF è motivata dall'articolo 16 capoverso 2, in virtù del quale esiste un elenco delle funzioni esaustivo che dovrà essere rispettato. Grazie al raggruppamento sarà possibile evitare un onere supplementare inutile. I risultati dei controlli dovranno essere illustrati separatamente per ciascun motivo del controllo.

Art. 22 Condizioni

I servizi specializzati CSP raccomandano ai servizi decisori condizioni adeguate per ridurre a un livello accettabile il rischio per la sicurezza valutato dai primi. I servizi decisori non sono vincolati a tali raccomandazioni. Possono accettare le condizioni raccomandate, prevederne altre o rinunciarvi. Queste misure di diritto in materia di personale volte alla riduzione dei rischi si basano sull'articolo 39 capoverso 1 lettera b o sull'articolo 41 capoverso 3 LSIn (cfr. anche messaggio, art. 42, pag. 2660) e vengono specificate all'articolo 22 lettera b OCSP. Il datore di lavoro può ordinare queste misure in base all'articolo 24 capoverso 2. Per la Confederazione la base per trattare dati

personali degni di particolare protezione risulta dall'articolo 27 capoverso 2 LPers, sempreché ciò sia necessario per la tutela di interessi importanti.

Art. 23 Comunicazione

Capoverso 1: se, per diversi motivi di controllo, determinate persone sono assoggettate a più controlli che non si svolgono contemporaneamente, le constatazioni rilevanti sotto il profilo del rischio che emergono in occasione di un controllo successivo dovranno potere essere comunicate ai servizi decisori del controllo precedente affinché, in caso di bisogno, possano essere adottate misure di sicurezza. Ciò è importante, in particolare, per i controlli di cui all'articolo 113 LM ai quali sono assoggettati tutti i militari. Se nell'ambito di uno dei controlli si constata un rischio in relazione all'arma dell'esercito, i servizi specializzati CSP potranno comunicarlo alla competente autorità militare.

Capoverso 2: in caso di riserva motivata riguardo alla sicurezza e di urgenza, nell'ottica della prevenzione dai pericoli i servizi specializzati CSP possono informare i servizi competenti in merito alle proprie constatazioni prima che la procedura sia conclusa. Il servizio competente potrà quindi adottare misure di sicurezza preventive. Ciò è particolarmente importante per il reclutamento di persone soggette all'obbligo di leva, un processo che dura al massimo tre giorni. Le riserve riguardo alla sicurezza (p. es. l'uso precedente di droghe) possono essere essenziali anche per la valutazione dell'idoneità al servizio militare da parte dei medici e degli psicologi del reclutamento.

Sezione 6: Conseguenze della dichiarazione

Art. 24 Comunicazione della decisione in merito all'esercizio dell'attività

Il servizio decisore si assume la responsabilità delle attività delle persone sottoposte a controllo e decide pertanto in merito all'esercizio dell'attività. Eventuali condizioni raccomandate dai servizi specializzati CSP non sono vincolanti per i servizi decisori (cfr. art 22). Essi possono accettarle, prevederne altre o rinunciarvi del tutto. Se però l'esercizio dell'attività sensibile sotto il profilo della sicurezza è vincolato a condizioni da parte del servizio decisore, quest'ultimo deve disciplinare anche l'assunzione di eventuali costi legati a queste condizioni. A tal proposito occorre rispettare soprattutto eventuali prescrizioni in materia di diritto del lavoro o di diritto contrattuale. Tuttavia, la mancata osservanza di eventuali condizioni dovrebbe comportare, quale ultima soluzione, la revoca dell'attività sensibile sotto il profilo della sicurezza, in quanto senza le condizioni non è possibile ridurre il rischio per la sicurezza a un livello accettabile.

La comunicazione tempestiva della decisione in merito all'esercizio dell'attività è tra l'altro necessaria ai fini dell'accesso a opere militari o a zone di sicurezza. Essa è altresì determinante per il rilascio di un'attestazione di sicurezza di cui all'articolo 30 capoverso 2 lettera b.

Art. 25 Uso plurimo di una dichiarazione

Capoverso 1: se la persona interessata è già in possesso di una dichiarazione ancora valida ed equivalente, in linea di principio per motivi di economicità non è opportuno eseguire un nuovo controllo. Nel singolo caso la decisione spetta al portatore del rischio. Per i militari, la valutazione del potenziale di pericolo o di abuso di cui all'articolo 113 capoverso 4 lettera d LM corrisponde a un controllo di sicurezza di base secondo la LSIn.

Capoverso 2: se per un nuovo controllo si utilizza la dichiarazione di un controllo precedente, qualora il controllo procedente sia stato eseguito a un livello di controllo superiore, dal punto di vista diritto in materia di protezione dei dati ciò potrebbe essere problematico. Infatti i dati raccolti al livello di controllo più elevato, che non potrebbero essere raccolti a un livello inferiore, potrebbero confluire nella valutazione. La richiesta di ignorare questi risultati secondo il diritto in materia di protezione dei dati, nel singolo caso, può condurre a risultati sconcertanti dal punto di vista della politica di sicurezza. Pertanto per analogia con i disciplinamenti restrittivi applicabili allo sfruttamento di scoperte fortuite presenti in altre basi giuridiche, dovrebbe quindi essere possibile un'utilizzabilità chiaramente limitata.

Art. 26 Ripetizione ordinaria

La LSIn rinuncia a prescrivere intervalli fissi per la ripetizione ordinaria, bensì fissa unicamente principi generali. Per poter gestire anche qui in modo adeguato la quantità dei controlli, in funzione dell'esigenza in materia di sicurezza occorre fissare chiare scadenze per la ripetizione. La LSIn, inoltre, conferisce al Consiglio federale la competenza di rinunciare a una ripetizione del controllo per quanto riguarda i militari o i militi della protezione civile. Ciò va applicato ai casi in cui la

ripetizione appare sproporzionata rispetto al periodo di servizio residuo. Ne sono un esempio le valutazioni del potenziale di pericolo o di abuso di cui all'articolo 113 capoverso 4 lettera d LM, che vengono ripetute solo in via straordinaria, ad esempio in casi sospetti ai sensi dell'articolo 12 capoverso 3 lettera c OCSP.

Art. 27 Ripetizione straordinaria

Capoverso 1: per una ripetizione straordinaria possono essere determinanti soltanto i nuovi rischi essenziali per la valutazione dei rischi ai fini dell'esercizio delle attività. Non sono per contro motivo per l'avvio di una ripetizione anticipata le violazioni delle condizioni di impiego. Per queste violazioni sono previste misure di diritto in materia di personale.

Capoverso 2: la LSIn prevede una ripetizione straordinaria soltanto in caso di fondato sospetto di nuovi rischi. Per il datore di lavoro può essere rilevante anche il fatto che vengano meno rischi accertati in precedenza. In questo caso le eventuali restrizioni all'esercizio di attività sensibili sotto il profilo della sicurezza non sarebbero più necessarie, motivo per cui anche in questo caso dovrà essere possibile avviare una ripetizione straordinaria.

Art. 28 Effetto della ripetizione

L'effetto della ripetizione vale sia per una ripetizione ordinaria, sia per una ripetizione straordinaria. Dato che la ripetizione serve a una nuova valutazione della persona da controllare, in attesa dei risultati la valutazione precedente sarà determinante per l'esercizio delle attività sensibili sotto il profilo della sicurezza. Tuttavia, se ancora durante la ripetizione del controllo si individuano nuovi rischi, il servizio decisore dovrà eventualmente provvedere fino alla conclusione del controllo con misure adeguate ai sensi dell'articolo 21 capoverso 2 LSIn affinché tali rischi non si realizzino. Ciò può avvenire, in particolare, mediante la revoca provvisoria di alcune attività o modifiche provvisorie dell'elenco degli obblighi.

Art. 29 Tutela giurisdizionale

Ai sensi dell'articolo 31 capoverso 2 LSIn, nell'effettuare la loro valutazione i servizi specializzati CSP non sono vincolati a istruzioni. Ciò deve valere anche per la promozione di procedure di ricorso relative alle valutazioni, in modo tale che gli organi superiori ai servizi specializzati CSP non possano influenzare indirettamente le valutazioni negando la possibilità di interporre ricorso. I servizi specializzati CSP devono quindi potere decidere autonomamente se vogliono interporre ricorso contro le decisioni del Tribunale amministrativo federale.

Art. 30 Attestazione di sicurezza

Le autorità di sicurezza estere accordano unicamente a persone che sono state sottoposte al CSP l'accesso a informazioni e materiale classificati o a zone di sicurezza. Per il rilascio della cosiddetta *«personnel security clearance»* occorre stabilire la procedura. Per la *«clearance»* è determinante la decisione del servizio decisore di cui all'articolo 24 e non l'esito della valutazione da parte dei servizi specializzati CSP. Nella misura in cui la *«clearance»* non avviene nell'interesse della Confederazione, l'attestazione di sicurezza deve essere rilasciata a pagamento. Finora una *«clearance»* era richiesta soltanto nel contesto internazionale. Sempre più spesso anche le autorità nazionali si aspettano che le persone che partecipano a progetti o riunioni classificati presentino un'attestazione di sicurezza. Una *«clearance»* può essere richiesta e rilasciata per entrambi gli scopi.

Sezione 7: Trattamento di dati personali

Art. 31 Responsabilità della protezione dei dati e della sicurezza dei dati

In applicazione dell'articolo 33 LPD, l'organizzazione delle competenze e responsabilità per la protezione dei dati, che richiede anche la sicurezza dei dati, deve essere disciplinata in relazione con il sistema d'informazione di cui all'articolo 45 LSIn. A tal fine si applica il principio secondo cui la responsabilità incombe al rispettivo titolare dei dati.

Art. 32 Controllo periodico del trattamento dei dati personali

Siccome i dati trattati nell'ambito dei controlli sono particolarmente sensibili, la liceità del loro trattamento dovrà essere controllata periodicamente da un organo indipendente dai servizi coinvolti nella procedura di controllo. Questi organi indipendenti sono, ad esempio, la revisione interna, gli auditori esterni nonché i consulenti per la protezione dei dati o l'IFPDT.

Sezione 8: Disposizioni esecutive

Art. 33 Gestione elettronica degli affari

Per gli impiegati della Confederazione sarà ora obbligatoria la gestione elettronica degli affari con i servizi specializzati CSP. Secondo la prassi attuale non si può tuttavia ragionevolmente pretendere che vi sia un obbligo per la popolazione in generale di comunicare per via elettronica (cfr. messaggio sulla legge federale concernente l'impiego di mezzi elettronici per l'adempimento dei compiti delle autorità; FF 2022 804). Le persone che non sono impiegate presso la Confederazione possono pertanto esigere che la gestione degli affari con loro avvenga in forma cartacea. La corrispondenza tra autorità continua ad avvenire sotto forma elettronica. Riguardo alla comunicazione elettronica con i tribunali, l'articolo 48 LSIn in combinato disposto con l'articolo 35 OCSP costituisce una disposizione prevista da leggi speciali ai sensi dell'articolo 1 capoverso 2 del Regolamento d'esecuzione del 16 giugno 2020[32] del Tribunale amministrativo federale sulla comunicazione elettronica con le parti.

Art. 34 Riscossione di emolumenti

I costi derivanti dai controlli dell'Amministrazione federale centrale e dell'esercito saranno preventivati in modo centralizzato presso il DDPS. Tra questi rientrano anche i controlli secondo la LSIn e le verifiche secondo la LPers per tutte le autorità e le organizzazioni assoggettate. I costi dei controlli presso servizi al di fuori dell'Amministrazione federale centrale saranno assunti da questi in modo decentralizzato e dovranno essere riscossi mediante emolumenti. Tramite l'assegnazione adeguata di risorse finanziarie e di personale al DDPS, il Consiglio federale dovrà fare in modo che vi sia in ogni momento un equilibrio tra queste risorse e il numero di controlli da effettuare.

Art. 35 Prestazioni dei servizi specializzati CSP a favore dei Cantoni

Secondo l'articolo 86 capoverso 4 LSIn i Cantoni possono ricorrere alle prestazioni, soggette al pagamento di un emolumento, dei servizi specializzati di cui alla LSIn per la loro sicurezza delle informazioni, nella misura in cui sia stato stabilito dal Consiglio federale. Mediante l'articolo 16 si evince che il servizio specializzato CSP DDPS è competente per tali controlli di sicurezza relativi alle persone. Per ricorrere a queste prestazioni i Cantoni dovranno disporre di una propria base legale per i controlli mentre il servizio specializzato CSP DDPS dovrà essere in grado a livello tecnico di procedere alle valutazioni richieste. Trattandosi, di fatto, di prestazioni di servizio commerciali della Confederazione, bisogna applicare le relative condizioni ordinarie della Confederazione, in particolare il principio della copertura dei costi. Il DDPS stipula con i rispettivi Cantoni un accordo sulle prestazioni affinché il quantitativo dei controlli e dunque l'onere per il DDPS sia prevedibile e pianificabile. Qualora le prestazioni da fornire dovessero richiedere risorse supplementari del servizio specializzato, queste prestazioni potranno essere fornite soltanto se al servizio verranno effettivamente concesse tali risorse. È esclusa una loro compensazione interna alla Confederazione.

Sezione 9: Disposizioni finali

Art. 36 Abrogazione e modifica di altri atti normativi

Per contenere il numero dei controlli entro limiti ragionevoli gli elenchi delle funzioni dovranno essere allestiti e aggiornati in modo coerente. Il DDPS, che assume i costi dei CSP, gestirà pertanto questi elenchi a livello centrale. In quanto portatori del rischio effettivi, i dipartimenti e la CaF chiedono costantemente le necessarie modifiche degli elenchi. Le attuali corrispondenti ordinanze dipartimentali dovranno quindi essere abrogate. Verrà parimenti abrogata la vigente ordinanza sui controlli di sicurezza relativi alle persone, che con la nuova OCSP è stata completamente riveduta. Verrà inoltre abrogata l'ordinanza sui controlli di sicurezza relativi alle persone nell'ambito degli impianti nucleari poiché i suoi contenuti, sempreché siano ancora necessari, sono integrati nella nuova OCSP. A causa dell'entità delle modifiche degli altri atti normativi, la relativa regolamentazione è disciplinata nell'allegato 8 (v. commento più sotto).

Art. 37 Disposizioni transitorie

Se al momento dell'entrata in vigore dell'ordinanza vi saranno ancora valutazioni pendenti, i servizi specializzati CSP, in collaborazione con i servizi promotori, dovranno verificare se il controllo deve ancora essere svolto e, se del caso, a quale livello di controllo. I controlli che non vengono più svolti saranno abbandonati secondo l'articolo 17 capoverso 3. Il CSP ampliato con audizione secondo

[32] RS **173.320.6**

il diritto attuale sarà attribuito al CSP ampliato. Nel SIBAD i controlli con audizione verranno appositamente contrassegnati.

Le dichiarazioni riguardanti i controlli attuali non hanno un termine di scadenza formale e il controllo verrà semplicemente ripetuto dopo un determinato periodo. Il disciplinamento proposto offre continuità sia ai servizi promotori sia ai servizi specializzati CSP. Inoltre, concede un margine di manovra sufficiente per sottoporre a un nuovo controllo dapprima le funzioni della massima criticità. Per i controlli secondo la LAEI, che finora si svolgono su base di diritto privato, è necessario un disciplinamento specifico affinché il contratto esistente possa giungere a scadenza come previsto.

Art. 39 Entrata in vigore

Al momento, la data di entrata in vigore è un criterio di riferimento perseguito. Per la data effettiva sono fattori d'influenza rilevanti, tra gli altri, l'ulteriore iter legislativo e il tempo necessario per l'attuazione tecnica delle nuove norme nel sistema d'informazione CSP.

Allegati 1–6 Elenchi delle funzioni

Per salvaguardare la sicurezza interna ed esterna della Svizzera gli allegati 1, 4 e 6 non sono pubblicati (v. commento al capitolo 2.5 lettera b e ad art. 5).

Allegato 7 Raccolta e trattamento di dati

La natura stessa del CSP implica che si raccolgano e trattino dati di carattere altamente personale concernenti il modo di vita della persona da controllare, in particolare le sue relazioni personali strette e quelle familiari, la sua situazione finanziaria e i suoi rapporti con l'estero (cfr. art. 27 cpv. 2 LSIn). Senza questi dati non è possibile procedere a una corretta valutazione del rischio per la sicurezza. La LSIn stessa fissa i limiti necessari per il trattamento di tali dati, che vengono raccolti e trattati soltanto se sono rilevanti per la sicurezza (cfr. p. es. art. 27 cpv. 2 e 3 e art. 34 LSIn). È per esempio consentito trattare dati concernenti l'esercizio di diritti costituzionali unicamente qualora sussista un sospetto concreto che la persona da controllare eserciti tali diritti per preparare o compiere attività che potrebbero pregiudicare considerevolmente gli interessi pubblici di cui all'articolo 1 capoverso 2 LSIn (p. es. la capacità di decisione e d'azione delle autorità e organizzazioni della Confederazione o la sicurezza interna ed esterna della Svizzera). I dati vengono inoltre raccolti e trattati in funzione dei rischi. Non ha ad esempio molto senso raccogliere dati fiscali di persone soggette all'obbligo di leva, visto che in giovane età non hanno ancora presentato alcuna, o comunque non significativa, dichiarazione delle imposte. Se si raccolgono dati non rilevanti per la valutazione del rischio per la sicurezza, il maggior onere che ne deriva per i servizi specializzati CSP è inutile. Pertanto, sia il diritto sia gli stessi servizi specializzati CSP provvedono affinché raccolgano e trattino soltanto i dati necessari.

Per la raccolta e al trattamento dei dati da fonti pubblicamente accessibili (le cosiddette Open Source Information [OSINF]), si può constatare che non si tratta mai di informazioni private o confidenziali. Di conseguenza, le indagini OSINF non toccano né la sfera privata, protetta dalla Costituzione, né il segreto delle telecomunicazioni. Non si tratta nemmeno di una misura di sorveglianza segreta. In mancanza di una presa di contatto diretta da parte dell'agente con la persona oggetto dell'indagine non si è neppure in presenza di un'indagine in incognito. Le indagini OSINF sono un metodo di raccolta e trattamento delle informazioni legittimo e, in virtù della progressiva digitalizzazione, sempre più importante.

Allegato 8 Abrogazione e modifica di altri atti normativi

1. OMPAH

Affinché i servizi specializzati possano ottenere i dati da Hoogan mediante procedura di richiamo, è necessaria una base.

2. OPers

Art. 94e Estratto del casellario giudiziale e del registro delle esecuzioni

La possibilità per il datore di lavoro di richiedere un estratto del casellario giudiziale e del registro delle esecuzioni esiste soltanto se questi ha un interesse legittimo ai sensi del capoverso 1. La possibilità di cui all'articolo 94*e* OPers è da intendersi come lo strumento meno invasivo nei diritti personali degli interessati tra la gamma dei controlli di sicurezza. In linea di principio, questa

disposizione si applica soltanto quando la funzione in questione non è già coperta da un controllo di cui all'OCSP. La disposizione potrà tuttavia essere applicata anche quando il CSP è stato effettuato molto tempo prima e il datore di lavoro ha un sospetto fondato che vi sia un rischio. Non deve però diventare un automatismo per cui, per le funzioni non soggette ad altri controlli, vengono sistematicamente richiesti i suddetti estratti. Soltanto se in ragione del suo settore di compiti una funzione soddisfa chiaramente i presupposti del capoverso 1 il datore di lavoro potrà richiedere estratti. Per validi motivi quali un impiego concreto o un incarico particolare sarà possibile richiedere un nuovo estratto prima di cinque anni. Spetta al rispettivo datore di lavoro decidere se in ragione di un'iscrizione nel registro vi sia un rischio e, se del caso, quali misure di diritto in materia di personale adottare.

Art. 94f Verifica dell'affidabilità

I presupposti di una verifica dell'affidabilità di cui all'articolo 20*b* LPers devono essere disciplinati nell'OPers. Tuttavia la procedura riguardante verifica deve essere completamente inclusa nell'OCSP.

3. Ordinanza sul sistema nazionale di indagine

La LSIn assegna ai servizi specializzati una nuova base legale che deve essere adattata nell'ordinanza sul sistema nazionale di indagine.

4. OCMI

L'attuale riferimento all'OCSP vigente finora va adeguato al nuovo diritto.

5. Ordinanza del 16 dicembre 2009[33] sui sistemi d'informazione militari e su altri sistemi d'informazione nel DDPS (OSIM)

Con il disciplinamento del sistema d'informazione per i controlli di sicurezza relativi alle persone nella LSIn e nell'OCSP, nell'OSIM occorre abrogare l'articolo 67 e l'allegato 30. Inoltre, gli attuali riferimenti all'OCSP vigente finora vanno adeguati al nuovo diritto.

6. Ordinanza del 22 novembre 2017[34] concernente l'obbligo di prestare servizio militare (OOPSM)

Gli attuali riferimenti all'OCSP vigente finora vanno adeguati al nuovo diritto.

7. Ordinanza del 10 dicembre 2004[35] sull'energia nucleare (OENu)

A seguito dell'abrogazione dell'ordinanza sui controlli di sicurezza relativi alle persone nell'ambito degli impianti nucleari (OCSPN) e della sua integrazione nell'OCSP, nell'OENu va inserito un riferimento all'OCSP, in modo che il lettore interessato al diritto possa trovare più facilmente le disposizioni corrispondenti. La copertura dei costi deve invece essere inserita direttamente nell'OENu.

[33] RS **510.911**
[34] RS **512.21**
[35] RS **732.11**

3.4 Ordinanza sulla procedura di sicurezza relativa alle aziende (OPSAz)

Osservazioni preliminari

Per la comprensione della materia è opportuno fare alcune brevi considerazioni almeno riguardo alle seguenti disposizioni della LSIn:

- quando si parla di mandati sensibili sotto il profilo della sicurezza, si deve fare riferimento alle definizioni giuridiche dell'articolo 5 lettera b LSIn. Di conseguenza, questi mandati riguardano il trattamento di informazioni classificate CONFIDENZIALE o SEGRETO secondo l'articolo 13 LSIn, l'amministrazione, l'esercizio, e la verifica di mezzi informatici del livello di sicurezza «protezione elevata» o «protezione molto elevata» secondo l'articolo 17 LSIn nonché l'accesso a zone di sicurezza, in particolare alle zone di protezione previste dalla legislazione sulla protezione di impianti militari. La forma giuridica dei mandati è irrilevante;
- sono considerate aziende ai sensi dell'OPSAz le imprese, le imprese subappaltatrici o loro parti che adempiono un mandato pubblico che prevede l'esercizio di un'attività sensibile sotto il profilo della sicurezza (cfr. art. 49 LSIn);
- sono considerati mandanti ai sensi dell'OPSAz le autorità o le organizzazioni assoggettate di cui all'articolo 2 LSIn (cfr. art. 50 cpv. 1 lett. a LSIn);
- le normative della procedura di sicurezza relativa alle aziende si applicano parallelamente a quelle sugli acquisti pubblici. L'elaborazione dell'OPSAz è avvenuta in stretta collaborazione con i servizi d'acquisto centrali (Ufficio federale delle costruzioni e della logistica, armasuisse), al fine di coordinare in modo ottimale la procedura di sicurezza relativa alle aziende e la procedura d'acquisto.

Ingresso

All'interno del capitolo 4 della LSIn, la procedura di sicurezza relativa alle aziende (PSA) costituisce un complesso di norme a sé stante che funge da base per la relativa legislazione esecutiva. L'articolo 84 capoverso 1 LSIn stabilisce la competenza generale delle autorità assoggettate di emanare disposizioni esecutive relative alla LSIn. L'articolo 73 LSIn assegna concretamente al Consiglio federale gli ambiti da disciplinare nel dettaglio.

Sezione 1: Disposizioni generali

Art. 1 Oggetto e campo d'applicazione

Capoverso 1: ai fini della descrizione della materia normativa dell'OPSAz la disposizione si rifà agli ambiti che devono essere disciplinati dal Consiglio federale in virtù dell'articolo 73 LSIn.

Capoversi 2 e 3: nella misura in cui autorità e organizzazioni sottostanno al campo d'applicazione della LSIn o dell'OSIn, anch'essi entrano in linea di conto quali mandanti per mandati sensibili sotto il profilo della sicurezza. Il campo d'applicazione dell'OPSAz deve quindi coincidere con quelli della LSIn e dell'OSIn (v. anche n. 2.6 lett. b). Per quanto riguarda l'applicabilità alle autorità assoggettate, si veda il commento all'articolo 1 OCSP. La corrispondenza menzionata dei campi d'applicazione deve riferirsi anche all'Amministrazione federale decentralizzata della Confederazione. Il campo d'applicazione dell'OPSAz si basa sul corrispondente campo d'applicazione dell'OSIn.

Art. 2 Aziende interessate

Capoverso 1: l'aggiudicazione da parte di autorità e organizzazioni svizzere di mandati sensibili sotto il profilo della sicurezza ad aziende con sede in Svizzera costituisce la fattispecie di base per l'esecuzione della procedura di sicurezza relativa alle aziende. Le imprese subappaltatrici con sede in Svizzera vengono equiparate a queste aziende. Il termine «azienda» è da intendersi in senso lato. Né la forma giuridica, né le dimensioni hanno dunque importanza. Sono decisivi unicamente la sensibilità sotto il profilo della sicurezza del mandato e l'assoggettamento dell'azienda all'ordinamento giuridico svizzero.

Possono essere considerate aziende anche le unità amministrative decentralizzate dell'Amministrazione federale nonché organizzazioni e persone di diritto pubblico o privato alle quali sono attribuiti compiti federali, sempreché non rientrino nel campo d'applicazione della LSIn.

Capoverso 2: l'OPSAz contempla le fattispecie nazionali. L'esecuzione di procedure di sicurezza relative alle aziende per le aziende con sede all'estero è retta dai corrispondenti trattati internazionali.

Art. 3 Autorità competente

Capoverso 1: già la LSIn, all'articolo 51 capoverso 2, designa il servizio specializzato competente per l'esecuzione della procedura di sicurezza relativa alle aziende (servizio specializzato PSA). La disposizione dell'ordinanza si limita a sottolineare che esso verrà aggregato al DDPS.

Capoverso 2: in relazione con le procedure di sicurezza internazionali relative alle aziende, il servizio specializzato PSA dipende dalla collaborazione con l'autorità di sicurezza svizzera designata, l'unica attraverso la quale si tengono i contatti con l'estero. Il coordinamento della procedura di sicurezza relativa alle aziende (PSA) con gli iter procedurali della suddetta autorità incombe al servizio specializzato PSA.

Sezione 2: Avvio della procedura di sicurezza relativa alle aziende

Osservazione preliminare sulla sezione 2

In un processo d'acquisto la PSA deve poter essere avviata il più presto possibile. In questa prima fase occorre soprattutto chiarire se il mandato da aggiudicare è sensibile sotto il profilo della sicurezza e se è quindi soddisfatto il presupposto processuale centrale. Non vengono creati elementi pregiudicanti per la procedura di aggiudicazione. A seguito della nuova procedura di sicurezza relativa alle aziende sarà sostituito completamente il metodo di gestione del rischio per ridurre lo spionaggio da parte dei servizi di intelligence.

Art. 4 Domanda di avvio della procedura

Capoverso 1: gli incaricati della sicurezza delle informazioni garantiscono che aspetti inerenti alla sicurezza delle informazioni siano integrati già nelle fasi iniziali delle considerazioni di un'aggiudicazione a terzi.

Capoverso 2: il Consiglio federale (salvo per sé stesso) non è competente per l'avvio della procedura per le autorità assoggettate secondo l'articolo 2 capoverso 1 LSIn. Nell'OPSAz esso si limita pertanto a comunicare alle autorità assoggettate il servizio competente.

Capoverso 3 lettera a: la descrizione più possibile precisa della prestazione edile, fornitura o prestazione di servizio serve al servizio specializzato PSA in particolare come indicatore di identificazione, specialmente se un'azienda esegue più mandati sensibili sotto il profilo della sicurezza.

Capoverso 3 lettera b: poiché la sensibilità sotto il profilo della sicurezza del mandato costituisce il presupposto per l'avvio della PSA, si dovrà illustrare per lo meno con una motivazione sommaria fino a che punto sono soddisfatti i presupposti di cui all'articolo 5 lettera b LSIn.

Capoverso 3 lettera c: nel singolo caso la PSA dovrà essere coordinata fin da subito con le disposizioni procedurali nel settore degli appalti pubblici. È pertanto propizio all'economia procedurale se già in questo stadio iniziale il mandante ha le idee chiare sulla procedura di aggiudicazione applicabile.

Art. 5 Esame della domanda

Capoverso 1: riguardo all'avvio della procedura il servizio PSA gode di un margine discrezionale relativamente ampio, che deve però sempre sfruttare d'intesa con il mandate svizzero o estero (cfr. art. 53 cpv. 2 LSIn).

Capoverso 2: con questa disposizione il Consiglio federale limita il margine discrezionale del servizio specializzato PSA e stabilisce in via definitiva le fattispecie per le quali dovrà essere obbligatoriamente avviata la PSA. Si tratta delle quattro configurazioni seguenti:

- lettera a: le aziende che operano nell'ambito della massima necessità di protezione di informazioni e mezzi informatici dovranno sempre essere controllate, a prescindere dal genere o dal luogo di adempimento del mandato;
- lettera b: il Consiglio federale stabilisce che il trattamento di informazioni classificate CONFIDENZIALE per le quali l'interesse a conservare il segreto concerne più autorità o dipartimenti costituisce, senza eccezioni, un caso per la PSA;
- lettera c: per analogia con la lettera b, anche l'esercizio, la manutenzione e la verifica di mezzi informatici del livello di sicurezza «protezione elevata» devono attivare, senza eccezioni, la PSA qualora vengano impiegati per compiti che coinvolgono più autorità o compiti interdipartimentali;

- lettera d: un'attestazione di sicurezza aziendale internazionale deve disporre di una base solida, per la quale unicamente l'esecuzione della procedura di sicurezza relativa alle aziende secondo la LSIn offre la garanzia necessaria e sufficiente. Sebbene debba sostenere i costi della procedura, l'azienda non può tuttavia semplicemente «acquistare» in tal modo un marchio di qualità statale. Il servizio specializzato PSA avvierà la procedura soltanto in presenza di una pertinente domanda di un'autorità estera o di un'organizzazione internazionale e se si tratta effettivamente di un mandato sensibile sotto il profilo della sicurezza.

Capoverso 3: questo termine ordinatorio è inteso fornire ai mandanti un orientamento per la pianificazione e il coordinamento della procedura di aggiudicazione e sollecitare il servizio specializzato PSA al rispetto dell'imperativo di celerità.

Art. 6 Esame della domanda con autorità di sicurezza estere

Capoverso 1: se il mandante intende affidare a un'azienda estera, dunque non soggetta all'ordinamento giuridico svizzero, un mandato sensibile sotto il profilo della sicurezza (cfr. art. 49 LSIn), trasmette la corrispondente domanda allo stesso modo al servizio specializzato PSA. In seguito le necessarie fasi procedurali saranno svolte dal servizio specializzato della Confederazione per la sicurezza delle informazioni (cfr. art. 83 LSIn) assieme all'autorità di sicurezza estera.

Capoverso 2: purché esista un pertinente trattato internazionale (cfr. art. 87 LSIn), su richiesta del servizio specializzato della Confederazione per la sicurezza delle informazioni, l'autorità di sicurezza estera o confermerà che l'azienda dispone di una dichiarazione di sicurezza aziendale oppure avvierà una procedura di sicurezza relativa alle aziende. La procedura è interamente disciplinata dal diritto dello Stato in cui ha sede l'azienda e anche il rilascio di una pertinente attestazione di sicurezza aziendale avrà luogo in virtù del diritto estero.

Art. 7 Definizione dei requisiti di sicurezza

Capoverso 1: con l'OSIn e l'OCSP si menzionano entrambi gli atti normativi determinanti che dovranno essere considerati nel definire i requisiti di sicurezza nel singolo caso.

Capoverso 2: nelle relazioni internazionali il trattato internazionale prevale sull'OSIn e sull'OCSP.

Capoverso 3: fatto salvo l'articolo 6 capoverso 2, il mandante e il servizio specializzato PSA potranno trovare un'intesa sull'avvio della procedura. Una volta avviata la procedura, dovrà altresì essere possibile che si accordino su una ripartizione dei compiti sia nella procedura di aggiudicazione, sia nell'adempimento del mandato. Tale modo di procedere dovrebbe essere utile specialmente quando, dopo il rilascio dell'attestazione di sicurezza aziendale, per l'intera durata di quest'ultima siano opportune misure di controllo di ampia portata o permanenti. È nell'interesse diretto del mandante (titolare del segreto) poter effettuare controlli indipendentemente dal servizio specializzato PSA. Le misure coercitive delle autorità non sono trasferibili al mandante.

Capoverso 4: nel rapporto tra la procedura di aggiudicazione e la procedura di sicurezza relativa alle aziende, è sempre la prima a costituire la procedura direttiva. In quanto strumento della sicurezza delle informazioni, la PSA segue sempre gli iter della procedura di aggiudicazione. Per quest'ultima, tuttavia, le fasi della procedura di sicurezza devono essere integrate nel piano procedurale. Di conseguenza i pertinenti compiti di coordinamento incombono alla parte principalmente interessata nella procedura direttiva, ossia al mandante.

Sezione 3: Valutazione delle aziende

Art. 8 Notifica delle aziende idonee

Capoverso 1: contrariamente alla valutazione concernente del mero avvio della procedura, con la valutazione dell'idoneità il servizio specializzato PSA esegue atti ufficiali più onerosi e approfonditi di diversa portata. Per ragioni inerenti al diritto e all'economia procedurale, in questa fase della procedura di sicurezza relativa alle aziende è quindi imprescindibile che si sottopongano all'analisi soltanto le aziende che dal punto di vista del mandante entrano ancora in linea di conto per ottenere il mandato. In linea di principio, al servizio specializzato PSA non vanno comunicate più di cinque aziende per la valutazione dell'idoneità. Un'estensione deve potere avvenire soltanto in casi motivati. Questa clausola d'eccezione deve costituire, in particolare, una via d'uscita in caso di sviluppi imprevisti nella procedura di aggiudicazione e consentire ulteriori comunicazioni.

Capoverso 2: per lo svolgimento della PSA (cfr. art. 50 cpv. 2 LSIn) è necessario il consenso dell'azienda e dovrà essere verificato d'ufficio dal servizio specializzato PSA. Questo consenso può

essere esplicito o risultare già dalle condizioni di partecipazione elencate nella documentazione del bando di gara e accettate dall'azienda.

Capoverso 3: per analogia con l'articolo 5 capoverso 3, questo termine ordinatorio è inteso fornire ai mandanti un orientamento per la pianificazione e il coordinamento della procedura di aggiudicazione e sollecitare il servizio specializzato PSA al rispetto dell'imperativo di celerità.

Art. 9 Raccolta dei dati

Capoverso 1 lettere a–g: queste disposizioni concretizzano l'articolo 56 LSIn ed elencano in un'enumerazione non esaustiva i punti reputati idonei per valutare l'affidabilità e le relazioni con Stati e organizzazioni esteri dell'azienda sotto il profilo della sicurezza. La raccolta è effettuata dal servizio specializzato PSA. Conformemente all'articolo 56 capoverso 1 lettera a LSIn, per valutare l'idoneità di un'azienda il servizio specializzato PSA può raccogliere dati pertinenti presso la stessa azienda. Il fatto che un'azienda evidenzi una carente disponibilità alla collaborazione è equiparabile a un mancato consenso alla procedura. La procedura verrà quindi abbandonata per l'azienda in questione a causa della mancanza di un presupposto processuale.

Contrariamente alle indicazioni rifiutate, le indicazioni errate non costituiscono un ostacolo, dovranno però essere prese in considerazione nella valutazione dell'affidabilità e, di norma, fanno sì che l'azienda venga ritenuta un rischio per la sicurezza.

Capoverso 2: l'acquisizione dei dati di cui all'articolo 6 capoverso 1 lettera a della legge federale del 25 settembre 2015[36] sulle attività informative (LAIn) è di competenza del SIC. A tal proposito si esamina se finora l'azienda si è manifestata in relazione a terrorismo, spionaggio, proliferazione, attacchi contro infrastrutture critiche o estremismo violento. Le acquisizioni vengono effettuate dal SIC.

Art. 10 Esclusione dalla procedura di aggiudicazione

Capoverso 1: sia l'articolo 44 della legge federale del 21 giugno 2019[37] sugli appalti pubblici (LAPub), sia l'articolo 57 LSIn enumerano varie fattispecie in presenza delle quali il mandante può o deve escludere un'azienda dalla procedura di aggiudicazione. Per evitare che la procedura di aggiudicazione e la PSA si blocchino inutilmente l'un l'altra, la presenza di primi indizi che potrebbero motivare un'esclusione secondo l'articolo 44 LAPub non dovrà dissuadere il mandante dal comunicare l'azienda in questione al servizio specializzato PSA affinché svolga la valutazione dell'idoneità, senza che debba già decidere in merito a un'esclusione. Tuttavia, il mandante dovrà comunicare le proprie constatazioni in tal senso al servizio specializzato PSA ai fini della valutazione. Dal canto suo, il servizio specializzato PSA dovrà informare il più rapidamente possibile il mandante se, sulla base della propria raccolta di dati, emergono elementi che possono indurre il mandante a escludere l'azienda.

Capoverso 2: in virtù di questo continuo scambio di informazioni, è giustificato che il servizio specializzato PSA continui provvisoriamente a valutare l'idoneità di un'azienda dubbia fino a quando il mandante non avrà deciso in merito a un'eventuale esclusione.

Capoverso 3: se nella procedura di aggiudicazione si è già verificata un'esclusione da parte del mandante, alla procedura di sicurezza relativa alle aziende verrà a mancare l'oggetto della procedura. Si tratta quindi di un chiaro caso secondo l'articolo 51 capoverso 1 lettera c LSIn e la PSA dovrà essere abbandonata prontamente per l'azienda in questione.

Art. 11 Scambio di informazioni

Questa disposizione riguarda il contenuto dello scambio reciproco di informazioni. Per la valutazione dell'idoneità, ad esempio, si mettono a disposizione del servizio specializzato PSA e del mandante, rispettivamente, indicazioni utili dal punto di vista del diritto in materia di aggiudicazione e elementi rilevanti per la sicurezza ai fini della sua decisione sull'esclusione di cui all'articolo 44 LAPub.

[36] RS **121**
[37] RS **172.056.1**

Sezione 4: Piano in materia di sicurezza

Art. 12 Contenuto ed esame del piano in materia di sicurezza

Capoverso 1: ai fini dell'allestimento del piano in materia di sicurezza, il servizio specializzato PSA prescrive all'azienda un quadro nel quale essa dovrà adottare e documentare le misure di sicurezza adeguate alla situazione complessiva. Devono essere documentate misure organizzative (p. es. gestione delle chiavi, sorveglianza dei locali), di personale (formazione, controlli di sicurezza relativi alle persone), tecniche (p. es. impiego di mezzi informatici) e fisiche (protezioni antiscasso). Se nell'ambito della valutazione dell'idoneità di cui agli articoli 55–58 LSIn si accertano rischi che possono essere sufficientemente ridotti con misure organizzative, queste misure vengono integrate nel piano in materia di sicurezza.

Capoverso 2: l'ispezione garantisce che con il piano in materia di sicurezza si possono imporre in modo mirato all'azienda le misure necessarie, idonee e adeguate alla situazione complessiva. In tal modo, da una parte, l'ispezione serve alla sicurezza delle informazioni e, dall'altra, tutela però anche l'azienda da un onere sproporzionato.

Capoverso 3: l'allestimento di piani in materia di sicurezza può rivelarsi complesso, in particolare poiché all'azienda vengono accordati, consapevolmente, anche determinati margini di discrezionalità. Se il piano in materia di sicurezza non supera al primo tentativo la verifica da parte del servizio specializzato PSA (cfr. art. 59 cpv. 2 LSIn), quest'ultimo deve accordarle un ulteriore termine per migliorare il piano, impartendo anche istruzioni concrete riguardo ai punti da migliorare.

Capoverso 4: per analogia con l'articolo 5 capoverso 3, questo termine ordinatorio è inteso fornire ai mandanti un orientamento per la pianificazione e il coordinamento della procedura di aggiudicazione e sollecitare il servizio specializzato PSA al rispetto dell'imperativo di celerità.

Art. 13 Incaricati della sicurezza aziendale

Capoverso 1: un'azienda comunicata dal mandante per la valutazione dell'idoneità deve designare un incaricato della sicurezza aziendale e comunicarlo al servizio specializzato PSA. Affinché i requisiti di sicurezza definiti possano produrre l'effetto necessario, occorre estendere la responsabilità alla direzione dell'azienda. L'incaricato della sicurezza aziendale dovrà quindi disporre di diritti di impartire istruzioni in seno all'azienda, almeno nell'ambito della sicurezza. Idealmente l'incaricato è membro della direzione e potrà così intervenire nelle decisioni o per lo meno agire su mandato diretto di un membro.

Capoverso 2 lettera a: per esercitare un'influenza efficiente ed efficace sulla sicurezza delle informazioni dell'azienda, il servizio specializzato PSA necessita di un interlocutore attraverso il quale possano svolgersi tutti i contatti.

Capoverso 2 lettera b: l'incaricato della sicurezza risponde nei confronti del servizio specializzato PSA per l'attuazione del piano in materia di sicurezza. Il servizio specializzato PSA provvede affinché l'incaricato riceva una formazione e un perfezionamento adeguati.

Capoverso 2 lettera c: nei casi in cui l'azienda è stata autorizzata dal mandante a coinvolgere imprese subappaltatrici, l'incaricato della sicurezza aziendale è legittimato a presentare al servizio specializzato PSA la richiesta di avvio della procedura di sicurezza relativa alle aziende per queste imprese (cfr. art. 4 cpv. 1 lett. c).

Art. 14 Comunicazione dell'aggiudicazione

Capoverso 1: di norma, i contratti quadro dovrebbero essere l'elemento scatenante per il rilascio di una dichiarazione di sicurezza aziendale. Viceversa, i singoli rapporti di mandato connessi al contratto quadro possono, eventualmente, incidere sul rischio per la sicurezza delle informazioni tanto da richiedere un adeguamento del piano in materia di sicurezza. È quindi essenziale che il servizio specializzato PSA sia sempre al corrente della situazione dei mandati nell'azienda quanto alla loro sensibilità sotto il profilo della sicurezza.

Capoverso 2: le indicazioni che il mandante dovrà trasmettere e necessarie per l'allestimento del piano in materia di sicurezza comprendono in particolare:

- indicazioni sul livello della sensibilità sotto il profilo della sicurezza del mandato in base all'articolo 5 lett. b LSIn;
- i nominativi delle persone alle quali è affidata l'esecuzione del mandato sensibile sotto il profilo della sicurezza (per lo svolgimento di controlli di sicurezza relativi alle persone);

- indicazioni sull'impiego di mezzi informatici aziendali, in particolare se vengono utilizzati in rete o se ne vengono isolati.

Art. 15 Controlli di sicurezza relativi alle persone

Capoverso 1: per svolgere un mandato sensibile sotto il profilo della sicurezza l'azienda dovrà organizzarsi in modo tale che a un CSP debba essere sottoposto soltanto un numero minimo di persone, strettamente necessario all'adempimento del mandato. Le domande di controlli per persone che soltanto potenzialmente svolgono attività sensibili sotto il profilo della sicurezza sono illecite e vengono respinte dal servizio specializzato PSA.

Capoverso 2: per ragioni di economia procedurale può avere senso che soprattutto grandi aziende siano autorizzate ad avviare autonomamente CSP. Ciò non cambia il fatto che il servizio specializzato PSA decide in via definitiva quali persone vengono effettivamente controllate.

Sezione 5: Dichiarazione di sicurezza aziendale e ripetizione della procedura

Art. 16 Rilascio della dichiarazione di sicurezza aziendale

Sebben non prevista dalla legge, la possibilità di limitare la dichiarazione di sicurezza aziendale a singoli elementi di attività sensibili sotto il profilo della sicurezza ai sensi dall'articolo 5 lettera b LSIn appare tuttavia compatibile con gli obiettivi della LSIn stessa, se non addirittura imposta dal principio di proporzionalità. Da un lato, risulta palese che, ad esempio per il trattamento di informazioni classificate CONFIDENZIALE, a un'azienda non vengano imposte misure di protezione onerose come quelle necessarie per il trattamento di informazioni classificate SEGRETO. Dall'altro, un piano in materia di sicurezza per le informazioni classificate CONFIDENZIALE va obbligatoriamente adeguato se vengono ad aggiungersi anche informazioni classificate SEGRETO. Occorre garantire mediante decisione la certezza del diritto in merito al livello di trattamento ammesso.

Art. 17 Annunci dell'azienda

Capoversi 1–2: questi elenchi non esaustivi concretizzano l'articolo 63 capoverso 2 LSIn riguardo al contenuto dell'obbligo di annuncio concernente i cambiamenti rilevanti sotto il profilo della sicurezza nell'azienda.

Capoverso 3: oltre all'azienda, i cambiamenti e gli incidenti possono riguardare imprese subappaltatrici o fornitori dell'azienda. Mentre le imprese subappaltatrici autorizzate sono soggette autonomamente all'obbligo di annuncio primario di cui ai capoversi 1 e 2, ciò non vale per i fornitori che entrano in contatto soltanto indirettamente con l'attività sensibile sotto il profilo della sicurezza. Sempreché siano interessati da un incidente che può avere ripercussioni sull'attività sensibile sotto il profilo della sicurezza, anche tale incidente dovrà essere annunciato dall'azienda.

Capoverso 4: lo scopo di questa disposizione è impedire che la validità della dichiarazione di sicurezza aziendale scada durante un mandato in corso e che a causa di ciò il rapporto di mandato cada nell'illegalità e, in linea di massima, debba essere interamente annullato. Con l'avvio tempestivo di un rinnovo della dichiarazione di sicurezza aziendale si potrà evitare questa situazione (v. anche commento ad art. 20 cpv. 2).

Art. 18 Obblighi del mandante

Capoverso 1: per definizione i mandanti sono in contatto stretto e frequente con le aziende, per cui è anche assai probabile che si accorgano di eventuali irregolarità. Perciò, da una parte, l'obbligo di annuncio dell'azienda per cambiamenti o incidenti rilevanti sotto il profilo della sicurezza viene esteso al mandante se esso fa le relative constatazioni nell'azienda. Dall'altra, il mandante dovrà adottare misure immediate.

Capoverso 2 lettera a: le fattispecie di cui all'articolo 44 LAPub possono avere effetti negativi sull'attuazione del piano in materia di sicurezza e dovranno quindi, eventualmente, essere valutate anche alla luce della sicurezza delle informazioni. Se fa constatazioni in tal senso, il mandante avrà quindi un obbligo di annuncio nei confronti del servizio specializzato PSA. Tale obbligo sussiste anche se il mandante non intende revocare l'aggiudicazione.

Capoverso 2 lettera b: i cambiamenti del mandato rilevanti per la sicurezza spesso incidono sul piano in materia di sicurezza, per cui il servizio specializzato PSA deve essere tenuto al corrente.

Capoverso 2 lettera c: ciò che vale per il cambiamento di un mandato si applica per analogia anche all'assegnazione di un nuovo mandato. Si rinvia alle precedenti considerazioni sulla lettera b.

Art. 19 Attestazione internazionale di sicurezza aziendale

Capoverso 1: il rilascio di un'attestazione internazionale di sicurezza aziendale costituisce una procedura amministrativa senza particolarità o oneri di rilievo ed è pertanto riscosso un emolumento forfettario di 100 franchi.

Capoverso 2: la situazione è diversa se l'azienda non dispone ancora di un'attestazione di sicurezza aziendale svizzera. L'esecuzione della procedura di sicurezza relativa alle aziende necessaria previamente rappresenta un onere che dovrà essere fatturato in funzione del tempo impiegato. La tariffa oraria varia a seconda dell'urgenza e della necessaria qualifica del personale che esegue la procedura.

Capoverso 3: il rilascio di un'attestazione internazionale di sicurezza aziendale è, in linea di massima, un atto amministrativo tra il servizio specializzato PSA e l'azienda. Spesso, tuttavia, per fare esaminare la validità delle attestazioni che le vengono presentate, l'autorità di sicurezza estera si rivolgerà alla propria controparte svizzera. È pertanto opportuno che il servizio specializzato PSA comunichi o faccia comunicare su richiesta all'autorità di sicurezza estera, per il tramite del servizio specializzato della Confederazione per la sicurezza delle informazioni, il rilascio di un'attestazione internazionale di sicurezza aziendale.

Art. 20 Revoca della dichiarazione di sicurezza aziendale e ritiro del mandato

Capoverso 1: purché la sicurezza delle informazioni non sia in grave pericolo, conformemente al principio di proporzionalità inizialmente va concessa all'azienda la possibilità di rettificare le irregolarità constatate. Poiché in tale procedura il mandante gode, in via eccezionale, dei diritti di una parte legittimata a ricorrere, deve essere sentito ogni volta prima che vengano emanate decisioni procedurali.

Capoverso 2: nei rari casi di una revoca della dichiarazione di sicurezza aziendale occorre osservare che in tal modo si innescano due ulteriori circostanze giuridicamente contestabili. Da un lato, il mandante deve revocare l'aggiudicazione (decisione) e, dall'altro, fa seguito la rescissione di un contratto di diritto privato. Per garantire la sicurezza delle informazioni, fondandosi sull'articolo 55 capoverso 2 della legge federale del 20 dicembre 1968[38] sulla procedura amministrativa (PA) il servizio specializzato PSA, di norma, toglierà a titolo precauzionale l'effetto sospensivo a un ricorso contro la revoca di una dichiarazione di sicurezza aziendale. La decisione potrà quindi essere eseguita senza ritardi. Sempreché non invochi la clausola derogatoria dell'articolo 58 capoverso 3 LSIn, il mandante dovrà ritirare il mandato sensibile sotto il profilo della sicurezza e garantire che l'azienda sia immediatamente privata di ogni possibilità di incidere negativamente sulla sicurezza delle informazioni. Se la revoca della dichiarazione di sicurezza aziendale viene impugnata, questo varrà anche per la revoca dell'aggiudicazione. È ipotizzabile che le due procedure di ricorso vengano riunite dal Tribunale amministrativo federale. Su richiesta di una parte, nello stesso procedimento potranno essere giudicati anche diritti di carattere civile (cfr. art. 40 cpv. 1 della legge del 17 giugno 2005[39] sul Tribunale amministrativo federale [LTAF]).

Capoverso 3: questo termine ordinatorio vuole consentire al servizio specializzato PSA di fare chiarezza, in tempo utile, sull'eliminazione di una minaccia per la sicurezza e di decidere se eventualmente è ancora necessario il proprio intervento sovrano.

Art. 21 Ripetizione della procedura

Capoverso 1: la presente disposizione attribuisce al servizio specializzato PSA, che agisce d'ufficio, la competenza per avviare la procedura di ripetizione. Contrariamente alla procedura semplificata (cfr. art. 65 LSIn), in questo caso avrà luogo la procedura completa (incl. la valutazione dell'idoneità).

Capoverso 2: questa disposizione vuole impedire che i mandati in corso debbano essere interrotti e annullati se la procedura di ripetizione si protrae oltre la data di scadenza della dichiarazione di sicurezza aziendale. L'atto formale registrato relativo all'apertura degli atti della procedura da parte del servizio specializzato PSA dovrà essere sufficiente per prorogare fino alla nuova decisione la durata di validità della dichiarazione di sicurezza aziendale in scadenza.

Capoverso 3: nel corso della procedura di ripetizione, il servizio specializzato PSA può giungere alla conclusione che non sussistono i presupposti per un rinnovo della dichiarazione di sicurezza

[38] RS **172.021**
[39] RS **173.32**

aziendale o che la procedura deve essere abbandonata per altri motivi. Tutte queste decisioni pongono fine alla durata di validità prorogata di cui al capoverso 2. L'annullamento dei rapporti giuridici è retto dalle norme di revoca della dichiarazione di sicurezza aziendale (cfr. art. 20).

Sezione 6: Trattamento dei dati personali

Art. 22 Sistema d'informazione sulla procedura di sicurezza relativa alle aziende

I dati personali e i dati aziendali della procedura di sicurezza relativa alle aziende devono essere definiti a livello di ordinanza. Il relativo elenco si trova nell'allegato dell'OPSAz.

Art. 23 Controllo periodico del trattamento di dati personali

Il sistema d'informazione di cui all'articolo 70 capoverso 1 LSIn utilizzato nella procedura di sicurezza relativa alle aziende può eventualmente contenere dati personali degni di particolare protezione. È pertanto indicata una pertinente vigilanza indipendente. Il DDPS dispone di una certa discrezionalità riguardo alla scelta dell'organo di revisione.

Sezione 7: Prestazioni del servizio specializzato PSA a favore dei Cantoni

Art. 24

Secondo l'articolo 86 capoverso 4 LSIn i Cantoni possono ricorrere alle prestazioni dei servizi specializzati di cui alla LSIn per la propria sicurezza delle informazioni, purché lo stabilisca il Consiglio federale. Queste prestazioni sono soggette al pagamento di un emolumento. Dal punto di vista della Confederazione, una verifica completa e un controllo continuo di aziende che ottengono mandati cantonali non ha molto senso. La Confederazione non ha bisogno di rilasciare loro una dichiarazione di sicurezza aziendale. Può invece senz'altro essere utile una verifica dell'affidabilità di aziende in collaborazione con il SIC. I Cantoni dovranno poter beneficiare di tale possibilità, sempreché dispongano di una base legale formale sufficiente e che abbiano stipulato con il DDPS una convenzione sulle prestazioni che stabilisca le modalità e il finanziamento della prestazione percepita.

Sezione 8: Disposizioni finali

Art. 25 Abrogazione e modifica di altri atti normativi

Si vedano le spiegazioni all'allegato 2 più sotto.

Art. 26 Disposizioni transitorie

Un effetto retroattivo relativo ai mandati per i quali l'appalto è iniziato prima dell'entrata in vigore dell'OPSAz potrebbe eventualmente modificare i presupposti in base ai quali il mandato è stato messo a concorso o aggiudicato e, in ultima analisi, potrebbe persino comportarne la revoca e una loro nuova aggiudicazione. Questa incertezza del diritto non è giustifica, per cui in questi casi ci farà stato l'idoneità dal punto di vista del diritto d'aggiudicazione. Sotto il profilo materiale, ai pochi casi di procedure di tutela del segreto del DDPS pendenti al momento dell'entrata in vigore si applicano comunque già pertinenti direttive di sicurezza e dunque, per motivi di economia procedurale, si rinuncia alle nuove fasi procedurali sancite dall'OPSAz. Le dichiarazioni di sicurezza aziendale emesse in virtù del diritto previgente rimangono valide per cinque anni a decorrere dal loro rilascio (cfr. art. 90 cpv. 3 LSIn).

Art. 27 Entrata in vigore

L'entrata in vigore sarà coordinata con l'entrata in vigore dell'OSIn e dell'OCSP.

Allegato 1

Nell'allegato si trovano i dati del sistema d'informazione sulla procedura di sicurezza relativa alle aziende che secondo l'articolo 26 capoverso 5 OCSP vengono tolti dall'OSIM.

Allegato 2

I: Abrogazione di altri atti normativi

La procedura di tutela del segreto applicabile unicamente nel DDPS è disciplinata nell'ordinanza sulla tutela del segreto. La nuova procedura di sicurezza relativa alle aziende a livello federale copre il contenuto della materia normativa dell'ordinanza sulla tutela del segreto, per cui quest'ultima può essere abrogata senza sostituzione.

II: Modifica di altri atti normativi

1. Ordinanza del 16 agosto 2017[40] sulle attività informative (OAIn)

Nell'articolo 56 capoverso 1 lettera b LSIn il SIC è menzionato esplicitamente quale fonte d'informazione del servizio specializzato PSA. Secondo l'articolo 60 capoverso 1 LAIn, il SIC comunica dati personali ad autorità svizzere se ciò è necessario per la salvaguardia della sicurezza interna o esterna. Il Consiglio federale definisce le autorità interessate nell'allegato 3 OAIn, nel quale attualmente non figura ancora il servizio specializzato PSA. A ciò si pone rimedio inserendo il numero 10.6.

2. OCMI

Nell'OCMI si rinvia all'ordinanza sulla tutela del segreto, da abrogare, ciò che deve essere rettificato.

3. OSIM

I dati menzionati nell'OSIM figurano ora nell'allegato dell'OPSAz e possono pertanto essere stralciati.

[40] RS **121.1**