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

Rapporto sui risultati della procedura di consultazione

Indice

1 Situazione iniziale

Il 24 agosto 2022, il Consiglio federale ha incaricato il DDPS di svolgere una procedura di consultazione sul diritto d'esecuzione della nuova legge sulla sicurezza delle informazioni (LSIn) presso i Cantoni, i partiti politici, le associazioni mantello nazionali dei Comuni, delle città e delle regioni di montagna, le associazioni mantello nazionali dell'economia e le cerchie interessate. La procedura di consultazione è durata fino al 24 novembre 2022.

Il diritto d'esecuzione della LSIn comprende tre nuove ordinanze e la modifica di un'ordinanza in vigore:

- *ordinanza sulla sicurezza delle informazioni (OSIn; nuova)*: l'OSIn disciplina la gestione della sicurezza delle informazioni, la protezione di informazioni classificate, la sicurezza informatica e le misure per la sicurezza fisica e relativa alle persone per l'Amministrazione federale e l'esercito. Definisce i rispettivi compiti, competenze e responsabilità. La modifica principale consiste nell'introduzione di un sistema di gestione della sicurezza delle informazioni (SGSI) presso tutte le unità amministrative;
- *ordinanza sui controlli di sicurezza relativi alle persone (OCSP; nuova)*: l'OCSP comprende le disposizioni d'esecuzione concernenti i diversi controlli di sicurezza relativi alle persone (CSP). Secondo la LSIn il numero dei controlli sarà ridotto al minimo necessario all'identificazione di rischi rilevanti per la Confederazione;
- *ordinanza sulla procedura di sicurezza relativa alle aziende (OPSAz; nuova)*: l'OPSAz disciplina i dettagli della procedura di sicurezza relativa alle aziende (PSA) introdotta con la LSIn. LA PSA è applicabile a tutti mandati sensibili sotto il profilo della sicurezza attribuiti dalla Confederazione ad aziende dell'economia privata;
- *ordinanza sui sistemi di gestione delle identità e sui servizi di elenchi della Confederazione (OIAM; modifica)*: la revisione parziale comprende in particolare un'estensione del campo d'applicazione alle unità amministrative dell'Amministrazione federale decentralizzata, a condizione che abbiano accesso a sistemi informatici dell'Amministrazione federale centrale.

Nell'ambito della procedura di consultazione, i Cantoni sono stati invitati a esprimere il loro parere in merito alle seguenti quattro domande:

1. L'attuazione delle ordinanze è comprensibile per i Cantoni *(cap. 3.1.1)*?
2. In che modo i Cantoni intendono attuare le ordinanze *(cap. 3.1.1)*?
3. Quali ripercussioni finanziarie prevedono i Cantoni *(cap. 3.1.2)*?
4. Per le questioni concernenti la sicurezza delle informazioni i Cantoni dovranno inoltre designare un servizio che fungerà da interlocutore per le autorità federali. Chi è la persona di contatto nel vostro Cantone?

2 Risultati della procedura di consultazione

	Destinatari	**Numero dei partecipanti invitati**	**Numero pareri e riscontri** *(incl. risposte con una rinuncia esplicita a esprimere un parere)*
1	Cantoni	26	27* *(*FR: 2)*
2	Partiti politici	11	2
3	Le associazioni mantello nazionali dei Comuni, delle città e delle regioni di montagna	3	0
4	Le associazioni mantello nazionali dell'economia	8	2
5	Altre organizzazioni interessate	14	2
6	Partecipanti non invitati a titolo individuale		3
	Totale	**62**	**36**

Valutazione complessiva	**Numero**	**Partecipanti**
Sì approvazione senza riserve	12	AI, BS, BE, FR, GL, GR, SH, SZ, SO, SG, TI, VS
Sì, ma approvazione di principio con proposte di modifica o aspetti poco chiari	22	AG, AR, BL, FR (SITel), GE, JU, LU, NE, NW, OW, TG, UR, VD, ZG, ZH, PS, UDC, asut, MPC, APC, Swissgrid, X. D.
No, ma rigetto di principio con proposte di modifica o aspetti poco chiari	0	
No rigetto totale	1	usam
Nessun commento espressa rinuncia a formulare un parere	1	Unione svizzera degli imprenditori

3 Pareri sul diritto d'esecuzione e sul rapporto esplicativo

Nel corso della procedura di consultazione sono state inoltrate alcune domande e alcuni commenti che non sono stati presi in considerazione nel rapporto sui risultati. Le segnalazioni di errori ortografici o le proposte di miglioramenti della traduzione non sono riportate.

3.1 Pareri generali

Dalla procedura di consultazione è emerso che la grande maggioranza dei partecipanti (**AG, AI, AR, BL, BS, BE, FR, GE, GL, GR, LU, NE, NW, OW, SH, SZ, SO, SG, TI, TG, UR, VD, VS, ZG, ZH, PS, UDC, asut, APC, Swissgrid**) è sostanzialmente d'accordo con il diritto d'esecuzione della LSIn e vede con favore la sua introduzione. Oltre ad alcune richieste di modifiche, si lamenta la presenza di aspetti poco chiari riguardo all'attuazione e alla validità di alcune direttive per i Cantoni. Solo l'**Unione svizzera delle arti e mestieri (usam)** respinge il progetto nella sua integralità, poiché travalica la base legale e non vengono indicati i costi generati.

L'**UDC** accoglie con favore il notevole miglioramento con la nuova LSIn del confronto giuridico con gli altri Paesi ai fini di un miglioramento nella cooperazione internazionale nel settore della sicurezza delle informazioni. Tuttavia, i dati personali raccolti e memorizzati dalla Confederazione elvetica devono essere conservati in Svizzera almeno nella categoria di classificazione più elevata. Infine, per lo scambio di dati deve essere resa obbligatoria la via di servizio ufficiale. L'**UDC** auspica che i costi per l'attuazione delle misure e i posti di lavoro aggiuntivi siano indicati in modo trasparente. Chiede, inoltre, che le misure comportino un risparmio sui costi e un miglioramento della protezione dei dati.

Il **PS** concorda in linea di principio con le disposizioni di attuazione della legge sulla sicurezza delle informazioni. Tuttavia, la raccolta dei dati per il CSP si spinge troppo oltre e viene rigettata. In particolare, non è ammissibile che possano essere raccolti e trattati dati sulla sfera intima e sulla sessualità, sulle opinioni o sulle attività religiose, politiche, sindacali e filosofiche.

NW rileva che nella maggioranza dei casi sia la LSIn che le relative ordinanze interessano i Cantoni solo indirettamente, nel caso in cui accedano a dati della Confederazione o li elaborino. Inoltre, occorre rilevare che alcune disposizioni che saranno importanti per i Cantoni non sono ancora state disciplinate in modo definitivo. Ciò vale soprattutto per la revisione della LSIn e dell'ordinanza per quanto riguarda l'obbligo di notifica dei ciberattacchi alle infrastrutture critiche (cap. 5 dell'LSIn). Tuttavia, si condividono gli adeguamenti generali che si ritiene vadano nella giusta direzione, tenendo conto dell'ambiente digitalizzato interconnesso e del crescente scambio di dati secondo il principio «*once only*». La sicurezza delle informazioni come compito congiunto con responsabilità interconnessa, sulla base di obiettivi condivisi e secondo un approccio coordinato nel rispetto di standard minimi, è considerata importante.

NW e **OW** constatano che il concetto di «Cantoni» è stato ridefinito nel diritto d'esecuzione e comprende anche enti, istituti o fondazioni di diritto pubblico. Sarebbe auspicabile una definizione coerente con quella compresa nell'articolo 3 della Costituzione federale. Gli altri enti dovrebbero essere menzionati separatamente.

asut accoglie con favore il solido quadro normativo per la sicurezza delle informazioni, che corrisponde allo stato attuale della tecnologia e dei relativi scenari di rischio. Le ordinanze presentano il giusto grado di flessibilità e precisione per definire chiaramente le responsabilità di tutte le parti coinvolte, anche nel caso di nuovi sviluppi tecnologici. Allo stesso modo, **asut** accoglie con favore l'approccio adottato dall'Amministrazione federale che in futuro intende classificare meno e quindi, per quanto possibile, ridurre la burocrazia.

3.1.1 Valutazione dell'attuabilità e comprensibilità

Dalla procedura di consultazione è emerso che le disposizioni di attuazione della LSIn e la loro applicazione sono sostanzialmente comprensibili per quasi tutti i Cantoni (**AG, AI, AR, BL, BS, BE, GE, GL, GR, LU, NE, NW, OW, SH, SZ, SO, SG, TI, TG, UR, VD, VS, ZG** e **ZH**). Tuttavia, ci sono ancora degli aspetti poco chiari in merito alle ripercussioni. Oltre ai costi di attuazione, la mancanza di chiarezza riguarda anche la sicurezza delle informazioni «equivalente» e le direttive applicabili e prescrizioni minime non ancora disponibili. Per alcuni partecipanti alla consultazione (**FR (SITel)**, **JU** e **VD**), i costi di attuazione sono difficili da valutare a causa di questi aspetti poco chiari.

Diversi Cantoni prevedono di introdurre una propria legislazione sulla sicurezza delle informazioni (**AG, BE, FR**) o stanno esaminando se e in quale forma le disposizioni necessarie devono o possono essere emanate o le basi esistenti adattate **(NW, SH, UR** e **ZH**).

Secondo **BL** manca chiarezza per quanto riguarda i Comuni e altre organizzazioni, come gli istituti di diritto pubblico e le aziende dei Cantoni, anch'essi collegati ai sistemi di informazione della Confederazione. Il diritto d'esecuzione del 24 agosto 2022 non chiarisce chi è responsabile del rispetto delle misure di sicurezza da parte di queste organizzazioni. I Cantoni non potrebbero esserlo per i Comuni. Per questo motivo, una soluzione nell'ambito del quadro proposto sarebbe molto più efficace se tutti coloro che desiderano collegarsi alle risorse informative della Confederazione fossero tenuti a rispettare le direttive federali per le rispettive connessioni. Questa soluzione garantirebbe molta più chiarezza e semplicità e le misure di sicurezza potrebbero essere attuate in modo efficace.

Per **AR** non è chiaro se la Costituzione impegni i Cantoni a garantire la sicurezza generale delle informazioni – al di fuori delle direttive sulla sicurezza dei dati (personali) nel quadro della protezione dei dati personali, della personalità o della sfera privata. È ovvio, d'altra parte, che anche la protezione dei dati personali trarrebbe beneficio da un incremento della sicurezza generale delle informazioni.

FR (SITel) propone che nella definizione delle direttive ancora mancanti siano unificati i requisiti tecnici della Confederazione che risultano ancora eterogenei. Ad esempio, la Confederazione dispone attualmente di tre infrastrutture a chiave pubblica (Public Key Infrastructure, PKI) parallele. Per il Cantone **FR** è difficile capire quale sicurezza garantire se la Confederazione propone requisiti ambigui. Se l'Amministrazione digitale Svizzera potesse servire a qualcosa, sarebbe innanzitutto la funzione di organo federale in relazione ai sistemi di informazione e quindi anche nell'ambito della sicurezza delle informazioni. L'Amministrazione digitale Svizzera sarà maggiormente coinvolta nelle questioni riguardanti i Cantoni e i loro sistemi di informazione. Senza un organo federale, il panorama informativo cantonale diventerebbe difficile da gestire, soprattutto per quei Cantoni che non dispongono di bilanci simili a quelli della Confederazione.

JU e **VD** auspicano che le ordinanze illustrino quali saranno le ripercussioni e le aspettative nei confronti dei Cantoni.

SG definisce i requisiti di sicurezza del Cantone accordandoli il più possibile ai requisiti stabiliti dalla Confederazione in merito alla protezione di base. L'armonizzazione del SGSI cantonale in questo senso è già in via di attuazione. Un'analisi dell'impatto mostrerà quali misure concrete dovranno essere in seguito adottate nei progetti. In conformità con le direttive della Confederazione, i diritti di accesso devono essere concessi alle persone responsabili degli uffici che ne necessitano per adempiere i compiti attribuiti loro dalla legge.

Per **TI** non è chiaro in che misura i collaboratori delle unità amministrative e giudiziarie dell'amministrazione cantonale, così come altri servizi esterni che svolgono compiti in conformità con le norme federali, debbano essere sottoposti a CSP. L'impossibilità di consultare l'elenco completo ed esaustivo delle funzioni da controllare solleva dubbi sull'attuazione pratica.

VS può contare su una politica di sicurezza delle informazioni e di direttive quadro che definiscono gli obiettivi, i principi generali e l'organizzazione della sicurezza delle informazioni. Le direttive si applicano a tutte le autorità cantonali. Non riguardano, invece, Comuni e istituzioni cantonali. Tuttavia, tutti gli accessi alla Confederazione effettuati tramite il Cantone sono gestiti e protetti dall'amministrazione cantonale. Il Cantone offre un supporto sussidiario nell'ambito della sicurezza informatica ai Comuni che lo desiderano e mette a disposizione lo strumento eCyAd per la sensibilizzazione a partire dal 2023, che viene elaborato dalla Confederazione nell'ambito della seconda Strategia nazionale per la protezione della Svizzera contro i ciber-rischi.

Per **ZG**, le direttive sono comprensibili, ma non entrano in maniera sufficientemente dettagliata nel merito degli obblighi dei Cantoni. Inoltre, l'approccio federalista, secondo il quale le direttive federali si applicano solo se le norme cantonali non soddisfano i requisiti di sicurezza federali, rende il tutto più complicato.

ZG rileva che la responsabilità principale per la sicurezza nel trattamento delle informazioni classificate della Confederazione spetta agli organismi cantonali che trattano questi dati o accedono alle risorse informatiche della Confederazione (in particolare: l'Ufficio per la protezione civile e gli affari militari, l'Organizzazione per le emergenze, la Polizia di Zugo, l'Associazione per le misure del mercato del lavoro). Questi organismi dovranno definire i processi, le responsabilità e le misure necessarie per poter garantire il livello di sicurezza richiesto dalla Confederazione. Le disposizioni federali verrebbero applicate solo se i regolamenti e le misure dei Cantoni non soddisfano i requisiti di sicurezza della Confederazione. I dipendenti dei singoli organismi sono responsabili del rispetto delle direttive nel trattamento delle informazioni classificate e delle risorse informatiche. Il corretto trattamento di quest'ultime presuppone che le autorità federali definiscano delle direttive all'indirizzo di questi organismi.

3.1.2 Valutazione delle ripercussioni finanziarie

Dalla procedura di consultazione è emerso un quadro molto ampio per quanto riguarda le ripercussioni finanziarie legate all'attuazione della LSIn.

Per **AI, AG, BL, BS, GL** e **VS**, l'attuazione della LSIn non comporta cambiamenti significativi o costi aggiuntivi. **BL** prevede solo un limitato sforzo supplementare nell'ambito del rispetto delle norme (*compliance*) e un impegno temporaneo di risorse di personale. **VS** rileva la possibilità che intervengano cambiamenti in relazione alle funzioni che richiedono un CSP.

Diversi Cantoni (**AR, FR (SITel), GE**, **JU, SH, SZ, SG, TG, UR,** e **ZG**) al momento della procedura di consultazione non erano ancora in grado di valutare con precisione le ripercussioni finanziarie.

NE valuta i costi per l'attuazione di un SGSI e per il rafforzamento della sicurezza tra i 500 000 e i 3 milioni di franchi. I costi per adeguamenti tecnici supplementari potrebbero ammontare a diversi milioni.

NW stima i costi annuali supplementari a circa 100 000 franchi.

OW stima i costi annuali a 50 000 franchi.

SZ prevede sul piano del personale 425 posti a tempo pieno aggiuntivi e investimenti in SGSI e sistemi di sicurezza che sarebbero anche indirettamente collegati all'attuazione delle ordinanze. Gli oneri finanziari supplementari legati alla nuova LSIn sono stimati approssimativamente intorno ai 300 000 franchi per il primo anno in costi per il personale e investimenti.

TI e **ZG** calcolano, oltre a costi per il personale, come la formazione e i CSP, anche costi per l'attuazione di misure tecniche di sicurezza.

ZH prevede costi supplementari pari a circa 10 000-50 000 franchi svizzeri ciascuno per l'accreditamento in materia di sicurezza di mezzi informatici e per i controlli di sicurezza regolari durante il ciclo di vita. Al momento non possono essere stimati in modo definitivo ulteriori costi.

3.2 Pareri sull'ordinanza sulla sicurezza delle informazioni (OSIn)

3.2.1 Osservazioni generali sull'OSIn

L'unificazione del SGSI in tutte le unità amministrative nel quadro della nuova OSIn è accolta con favore (**UDC**). L'**UDC** ritiene che la centralizzazione porterà a una riduzione dei costi e a un funzionamento e una manutenzione efficienti. Auspica dunque che in tutti gli uffici sia introdotto il più rapidamente possibile lo stesso SGSI.

GE sottolinea la complessità dell'attuazione dell'ordinanza e gli oneri a livello di costi che la stessa comporta.

3.2.2 Pareri sugli articoli dell'OSIn

Articolo 2 Campo d'applicazione

Capoverso 6: dalla procedura di consultazione è emerso che per diversi Cantoni (**AG**, **BL** e **ZH**) è difficile dimostrare l'equivalenza delle proprie leggi con la LSIn.

AG auspica che si dimostri come i Cantoni potrebbero difendersi in caso di rifiuto di accesso da parte della Confederazione, altrimenti la disposizione derogatoria (art. 3 cpv. 2 LSIn) risulterebbe inutile.

Articolo 6 Cura delle basi legali e degli obblighi contrattuali

NE ritiene che non sia chiaro se i Cantoni debbano consultare il servizio specializzato della Confederazione per la sicurezza delle informazioni quando creano una propria base giuridica per raggiungere un livello di sicurezza equivalente o quando attuano, ad esempio, raccomandazioni tecniche.

Articolo 9 Autorizzazione ed elenco delle deroghe

Capoverso 2: **LU** auspica che si specifichi a chi il servizio specializzato della Confederazione per la sicurezza delle informazioni nonché i dipartimenti possono delegare l'autorizzazione di deroghe.

Capoverso 4 lettera b: **LU** si chiede se le unità amministrative, i dipartimenti e il servizio specializzato della Confederazione per la sicurezza delle informazioni siano sempre informati se la concessione di deroghe è stata delegata, in modo da potere registrare tali deroghe nel loro elenco. Per garantire il flusso di informazioni, sarebbe opportuno introdurre un obbligo di notificare e informare per l'organo a cui è stata delegata l'autorizzazione delle deroghe.

Articolo 12 Gestione degli incidenti

Capoverso 7 lettera a: **LU** auspica che sia precisato quali informazioni devono essere comunicate. In caso contrario potrebbero insorgere dei problemi, in particolare dal punto di vista della protezione dei dati.

Articolo 16 Principi

L'articolo è comprensibile (**AG**). Tuttavia, non è possibile stimare l'onere necessario.

TG e **ZH** rilevano una mancanza di chiarezza in merito alla competenza e alla procedura da seguire in caso di richieste al Cantone di consultare le informazioni classificate della Confederazione. **TG** auspica che al capoverso 3 si specifichi che non si applicano le leggi cantonali sulla trasparenza.

Articolo 17 Servizi incaricati della classificazione

Per **AG** non risulta chiaro in che misura questa disposizione possa essere rilevante per i Cantoni, dato che quest'ultimi non sono menzionati come enti classificatori.

Articolo 18-20 Livelli di classificazione AD USO INTERNO, CONFIDENZIALE e SEGRETO

Secondo **AG** le disposizioni sono comprensibili. Tuttavia, non è chiaro se e in che misura ci siano problemi di congruenza e difficoltà tra i livelli di classificazione dei Cantoni e quelli della Confederazione.

GE propone che il criterio «è resa nota l'identità di persone particolarmente esposte» al livello di classificazione CONFIDENZIALE di cui all'articolo 19 lettera c sia eliminato in modo che valga solo come criterio per il livello di classificazione SEGRETO all'articolo 20 lettera c. Non viene preso in considerazione l'aspetto del danno alla fonte stessa, nel caso in cui sia possibile accedere alla sua identità. Ciò costituisce un problema e potrebbe danneggiare anche lo Stato.

A proposito dell'articolo 18 lettera c, **VD** sottolinea che le conseguenze di una lesione psicologica possono essere più gravi di quelle di una lesione fisica. Alla lettera c, tuttavia, sono menzionate unicamente le lesioni fisiche.

VD propone che le disposizioni sui livelli di classificazione siano adeguate. In caso di attacco alla sicurezza delle informazioni dei sistemi della Confederazione non dovrebbero essere tutelati sul piano giuridico unicamente gli interessi della Confederazione, ma anche quelli di aziende e privati.

Articolo 21 Direttive concernenti il trattamento

Poiché secondo l'articolo 21 OSIn le istruzioni generali e astratte si applicherebbero solo ai servizi di cui all'articolo 2 capoversi 1-3 OSIn, per **AG** non è chiaro quali direttive si applichino ai Cantoni e da chi siano emanate.

Articolo 22 Misure di sicurezza specifiche all'impiego

Per **AG** non è chiaro, per quale motivo questa disposizione debba essere attuata da parte dei Cantoni.

X. D. propone che il capoverso 1 sia completato con il capo del Servizio informazioni militare e il Servizio di protezione preventiva dell'esercito nonché con il direttore dell'Ufficio federale della dogana e della sicurezza dei confini.

Articolo 23 Accreditamento in materia di sicurezza di mezzi informatici

Secondo **AG** non è chiaro, per quale motivo questa disposizione debba essere attuata da parte dei Cantoni.

Articolo 24 Protezione in caso di pericolo per le informazioni classificate

Per **AG** la disposizione è comprensibile e attuabile. L'onere per l'attuazione dovrebbe essere contenuto.

Articolo 25 Verifica della necessità di protezione e cerchia delle persone autorizzate

AG esprime il parere che la disposizione non è rilevante per i Cantoni, poiché in quest'ultimi non c'è nessun servizio incaricato della classificazione ai sensi dell'articolo 17 OSIn.

Articolo 26 Archiviazione

Per **AG** la disposizione è comprensibile e attuabile. Tuttavia, non è possibile stimare l'onere richiesto dall'attuazione.

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

Per **AG** la disposizione è comprensibile e attuabile. Tuttavia, non è possibile stimare l'onere richiesto dall'attuazione.

Articolo 29 Misure di sicurezza

Poiché secondo l'articolo 21 capoverso 1 OSIn le istruzioni generali e astratte si applicherebbero solo ai servizi di cui all'articolo 2 capoversi 1-3 OSIn, per **AG** non è chiaro quali direttive si applichino ai singoli Cantoni e da chi siano emanate.

Per **AG** la disposizione è comprensibile e attuabile nella misura in cui si applica ai Cantoni. La fattibilità dell'attuazione dipende dalle istruzioni sui requisiti minimi che non sono ancora disponibili.

Articolo 30 Sicurezza durante l'esercizio

Per **AG** la disposizione è comprensibile e attuabile. Tuttavia, non è possibile stimare l'onere richiesto dall'attuazione.

Articolo 34 Misure di protezione fisica

Poiché secondo l'articolo 34 capoverso 1 OSIn le istruzioni generali e astratte si applicherebbero solo ai servizi di cui all'articolo 2 capoversi 1-3 OSIn, per **AG** non è chiaro quali misure minime necessarie per la protezione fisica di informazioni e mezzi informatici si applichino ai Cantoni e da chi siano emanate. Per **AG** la disposizione è comprensibile e attuabile nella misura in cui si applica ai Cantoni. La fattibilità dell'attuazione dipende dai requisiti minimi che non sono ancora disponibili.

Articolo 35 Zone di sicurezza

GE rileva che le istruzioni generali e astratte sulle zone di sicurezza potrebbero portare a modifiche dei locali in modo che il livello di tutela del segreto possa comunque essere garantito.

X. D. propone che venga concesso il diritto di controllare l'uso abusivo di onde elettromagnetiche in prossimità delle zone di sicurezza.

Articolo 44 In generale

X. D. propone che venga verificata la base giuridica relativa allo scambio di dati personali e, se del caso, che l'articolo OSIn sia precisato.

3.3 Pareri sulla modifica dell'ordinanza sui sistemi di gestione delle identità e sui servizi di elenchi della Confederazione (OIAM)

3.3.1 Osservazioni generali sull'OIAM

VD prende atto con interesse che la nuova versione dell'ordinanza consente ora il collegamento con un sistema IAM cantonale e valuterà l'eventuale introduzione di questa nuova possibilità. Rileva che la revisione dell'ordinanza riguarda principalmente aspetti tecnici dei sistemi di gestione dei dati di identificazione. Questi potrebbero avere un impatto sulla gestione dell'identità del portale IAM del Cantone o di altre banche dati, in particolare per quanto riguarda l'obbligo di gestire gli accreditamenti e l'accesso ai sistemi di informazione della Confederazione. Si tratta di «terzi» che utilizzerebbero anch'essi questi sistemi di identificazione.

L'**UDC** accoglie con favore l'ampliamento del campo di applicazione alle unità amministrative dell'Amministrazione federale decentralizzata per quanto riguarda i CSP. Tuttavia, gli effetti sulla protezione dei dati, in particolare mediante il trattamento esteso dei dati biometrici, devono essere monitorati criticamente.

VS apprende con interesse che la nuova versione dell'ordinanza consente il collegamento con un sistema IAM cantonale e valuterà eventualmente l'introduzione di questa nuova possibilità.

3.3.2 Pareri sugli articoli dell'OIAM

Articolo 13 Archivio centralizzato delle identità per la distribuzione dei dati

Capoverso 4: **GE** chiede se per «il sistema interessato» si intende il sistema sorgente o un altro sistema di informazione interno dell'Amministrazione federale.

Articolo 18 Requisiti in materia di sicurezza delle informazioni

Capoverso 2: **GE** propone che si precisi da chi e in quale ambito sono definiti i requisiti minimi.

Articolo 21 Condizioni per il collegamento di sistemi IAM esterni

Lettera c: **GE** osserva che il suo sistema IAM cantonale contiene dati su persone che non utilizzano i sistemi di informazione forniti dalla Confederazione. **GE** chiede pertanto se nel suo sistema IAM può essere collegato al sistema IAM della Confederazione solo il sottogruppo di persone che accede ai sistemi di informazione della Confederazione.

Allegato

Lettera e: dati tecnici: **GE** propone che in merito alla categoria di dati «7. Password» sia specificato che i dati devono essere ben criptati o protetti tramite una funzione hash a seconda delle necessità.

3.4 Pareri sull'ordinanza sui controlli di sicurezza relativi alle persone (OCSP)

3.4.1 Osservazioni generali sull'OCSP

L'**UDC** desidera sottolineare positivamente la riduzione di almeno il 30 per cento del numero di casi sottoposti a controllo. La conseguente sostituzione delle ordinanze precedenti è comprensibile.

VD sottolinea che l'OCSP avrà un impatto sui servizi responsabili dei CSP in ambito cantonale. Non va dimenticato che l'ampia raccolta di dati prevista e il trattamento di dati personali sensibili richiederanno una vigilanza rigorosa che sia compatibile con la legislazione sulla protezione dei dati.

X. D. sottolinea che l'OCSP pone gravosi problemi per quanto concerne le basi costituzionali e legali. Da questo punto di vista, l'ordinanza dovrebbe essere sottoposta o fatta sottoporre a un nuovo esame.

3.4.2 Pareri sugli articoli dell'OCSP

Articolo 2 Campo d'applicazione

Swissgrid propone che la LAEI sia inclusa nel campo d'applicazione, in quanto costituisce una base giuridica indipendente: «*Fatti salvi l'articolo 84 capoverso 3 LSIn e l'articolo 2 capoversi 2-5 dell'ordinanza sulla sicurezza delle informazioni del ..., la presente ordinanza si applica alle autorità e alle organizzazioni assogettate ai sensi dell'articolo 2 LSIn nonché dell'articolo 20a LAEI.*»

Articolo 3 Attribuzione

Capoverso 3: **Swissgrid** propone il seguente complemento, dato che **Swissgrid** non appartiene né all'Amministrazione federale centrale né a quella decentralizzata:

«Per le funzioni secondo l'articolo 20a capoverso 1 LAEl vale l'elenco delle funzioni secondo l'allegato 6. In luogo del Dipartimento, l'autorità competente per le richieste di cui all'articolo 4, per le verifiche dell'aggiornamento di cui all'articolo 6 e per le richieste di controlli straordinari di cui all'articolo 7 è la Commissione dell'energia elettrica ai sensi dell'articolo 21 LAEl.»

Articolo 5 Pubblicazione, conservazione e comunicazione

Swissgrid auspica che l'elenco delle funzioni non sia pubblicato nella Raccolta ufficiale a causa della sua confidenzialità. Sarebbe così possibile proteggere **Swissgrid** e i suoi collaboratori.

Articolo 8 Controlli presso gli impiegati cantonali e terzi

Capoverso 1: **AG** auspica che siano definite le funzioni degli impiegati cantonali che devono essere sottoposti a un controllo ai sensi dell'articolo 29 capoverso 1 lettera b LSIn. Occorre inoltre stabilire la procedura di presentazione della domanda al DDPS.

Le funzioni all'interno del Cantone **VS** che richiedono un CSP sono note. Inoltre, già da diversi anni vengono effettuati controlli corrispondenti. **VS** prende atto tuttavia che, in base alla spiegazione relativa all'articolo 8 del rapporto esplicativo, il DDPS è stato incaricato di uniformare le pratiche. Ciò potrebbe comportare potenzialmente l'estensione dei controlli effettuati nel Cantone, comportando notevoli costi finanziari.

Articolo 11 Verifica dell'affidabilità secondo la LPers

Capoverso 1 lettera c e 2: il **MPC**, in qualità di autorità preposta al perseguimento penale, propone che si completi la base per il controllo di sicurezza di base e il CSP ampliato per il personale interno ed esterno del MPC. Sussiste, infatti, un rischio di pregiudizio da significativo a grave.

Articolo 14 Verifiche dell'affidabilità secondo la LAEl

Swissgrid è d'accordo con il tenore dell'articolo e ringrazia per avere tenuto conto delle indicazioni in merito.

Articolo 15 Servizi promotori e servizi decisori

Capoverso 4: **Swissgrid** accoglie con favore la disposizione secondo la quale la società nazionale di rete è servizio promotore e decisore.

Articolo 19 Raccolta dei dati

X. D. esprime forte perplessità in merito a questo articolo. L'articolo dovrebbe essere smembrato in 5-6 articoli più brevi e non è all'altezza dal punto di vista giuridico della qualità redazionale delle leggi e delle ordinanze del diritto svizzero.

Capoverso 2 lettera c: **Swissgrid** propone che la società nazionale di rete sia compresa in un nuovo numero 8, in base al quale si dovrebbe effettuare un'audizione per ogni caso di CSP ampliato. La proposta si basa su esperienze fatte nell'ambito dei CSP di diritto privato.

Articolo 26 seg. Ripetizione ordinaria e straordinaria

NE si chiede per quanto tempo sia valido un CSP e se in caso di una ripetizione a causa di un rischio di sicurezza il controllo integri o sostituisca la valutazione precedente.

Articolo 30 Attestazione di sicurezza nel contesto internazionale

X. D. propone di ampliare questo articolo introducendo il rilascio d'ufficio per diverse funzioni del SIC, del SIM e dell'AVI-AIn, al fine di ridurre l'onere amministrativo in termini di numero di richieste di rilascio di attestazioni.

Articolo 35 Prestazioni dei servizi specializzati CSP a favore dei Cantoni

Attualmente **AG** non prevede di trasferire in futuro CSP alla Confederazione. Tuttavia, i requisiti e il livello degli emolumenti possono essere ritenuti adeguati.

GE sottolinea che il livello degli emolumenti potrebbe essere considerevole, ad esempio per la polizia o per il l'Ufficio cantonale dei sistemi di informazione e della digitalizzazione.

GE intende verificare l'opportunità di creare una base per il CSP. Sarebbe così possibile garantire la propria sicurezza delle informazioni.

NE solleva la questione se i motivi di sicurezza fatti valere debbano essere definiti nella base giuridica cantonale o se siano gli stessi dell'OCSP.

Articolo 38 Disposizioni transitorie

Capoverso 4: **Swissgrid** propone che il capoverso sia adeguato come segue: «*I controlli di sicurezza ricevuti dalla società nazionale di rete prima e fino a un anno dopo l'entrata in vigore della presente ordinanza restano utilizzabili nel quadro dei termini di ripetizione secondo gli articoli 26 e 27 come indicato qui di seguito: […]*»

Capoverso 5: **Swissgrid** propone che il capoverso sia stralciato.

Allegato 6 Funzioni secondo l'articolo 20a capoverso 1 LAEl

Swissgrid propone una differenziazione delle funzioni per tipologia allo scopo di distinguere le funzioni in base alle singole attività.

Allegato 7 Raccolta e trattamento di dati

Dalla procedura di consultazione è emerso che diversi partecipanti (**GE**, **PS**, **TG**, **UR**, **PS**, **APC**, **usam** e **X. D.**) ritengono che l'allegato relativo al trattamento dei dati personali particolarmente degni di protezione si spinga troppo oltre.

Il **PS** chiede che la locuzione «in particolare» venga stralciata ovunque dall'allegato 7 dell'OCSP senza essere sostituita. La competenza dello Stato deve essere esplicitamente menzionata e definita in maniera inequivocabile. Non è possibile ammettere un elenco non esaustivo.

3.5 Pareri sull'ordinanza sulla procedura di sicurezza relativa alle aziende (OPSAz)

3.5.1 Considerazioni generali sull'OPSAz

L'OPSAz è necessaria (**UDC**) e la sostituzione dell'ordinanza sulla tutela del segreto è in ritardo.

AG auspica la possibilità di beneficiare di prestazioni per lo svolgimento di PSA, analogamente all'OCSP.

UR osserva che per i Cantoni non è richiesta l'attuazione dell'OPSAz.

usam rileva che l'attuazione mediante ordinanza sarebbe ancora più onerosa dal punto di vista normativo di quanto previsto dalla legge. Mancano inoltre informazioni sugli oneri normativi e i costi aggiuntivi che un'attuazione comporterebbe per i Cantoni.

.

3.5.2 Pareri sugli articoli dell’OPSAz

Articolo 2 Aziende interessate

VD propone di verificare il rapporto tra l’articolo 2 capoverso 1, secondo cui l’ordinanza si applica solo alle aziende con sede in Svizzera, e l’articolo 6, che disciplina le modalità d’avvio della PSA.

Articolo 14 Contenuto ed esame del piano in materia di sicurezza

VD propone che in caso di sviluppi tecnici o di cambiamenti dei rischi il piano in materia di sicurezza sia adattato.

Articolo 17 Annunci dell’azienda

GE propone che siano introdotti dei chiarimenti. Al capoverso 1 lettera a si dovrebbe specificare che lo stesso vale anche per le filiali. Il capoverso 1 lettera e dovrebbe essere completato con l’aggiunta «in Svizzera e in altri Paesi». Al capoverso 2, per quanto riguarda incidenti rilevanti dal profilo della sicurezza, è opportuno aggiungere le violazioni della protezione dei dati ai sensi della nLPD.

4 Allegato: Partecipanti alla procedura di consultazione e proposte di modifica

Abbreviazione	Partecipanti	Proposte di modifica e aspetti poco chiari Ordinanza/rapporto esplicativo				
		OSIn	**OIAM**	**OCSP**	**OPSAz**	**PG[1] rap. espl.**
Cantoni						
ZH	Zurigo	x				x
BE	Berna					
LU	Lucerna	x				
UR	Uri			x		
SZ	Svitto					
OW	Obvaldo					x
NW	Nidvaldo					x
GL	Glarona					
ZG	Zugo					x
FR	Friburgo					
FR (SITel)	Friburgo, Ufficio informatica e telecomunicazioni	x				
SO	Soletta					
BS	Basilea Città					
BL	Basilea Campagna	x				x
SH	Sciaffusa					
AR	Appenzello Esterno	x				
AI	Appenzello Interno					
SG	San Gallo					
GR	Grigioni					
AG	Argovia	x		x	x	
TG	Turgovia	x		x		
TI	Ticino					
VD	Vaud	x	x	x		
VS	Vallese					

[1] PG=Parte generale

Abbreviazione	Partecipanti	Proposte di modifica e aspetti poco chiari Ordinanza/rapporto esplicativo				
		OSIn	**OIAM**	**OCSP**	**OPSAz**	**PG[1] rap. espl.**
NE	Neuchâtel	x		x		
GE	Ginevra	x	x	x	x	
JU	Giura	x				
Partiti politici						
UDC	Unione democratica di centro UDC					
PS	Partito socialista svizzero PS			x		
Organizzazioni mantello dell'economia a livello nazionale						
usam	Unione svizzera delle arti e mestieri (usam)			x		
	Unione svizzera degli imprenditori					
Altre organizzazioni interessate						
APC	Associazione del personale della Confederazione (APC)			x		
	Swissgrid AG			x		
Partecipanti non invitati a titolo individuale						
asut	asut – Associazione svizzera delle telecomunicazioni				x	
MPC	Ministero pubblico della Confederazione			x		
X. D.	Xavier Dufour	x		x		