



Termine di referendum: 18 gennaio 2024

Legge federale sulla sicurezza delle informazioni in seno alla Confederazione

(Legge sulla sicurezza delle informazioni, LSIn)

**(Introduzione dell'obbligo di segnalare ciberattacchi
a infrastrutture critiche)**

Modifica del 29 settembre 2023

L'Assemblea federale della Confederazione Svizzera,
visto il messaggio del Consiglio federale del 2 dicembre 2022¹,
decreta:

I

La legge del 18 dicembre 2020² sulla sicurezza delle informazioni è modificata come segue:

Titolo

Legge federale sulla sicurezza delle informazioni (LSIn)

Art. 1 cpv. 1

¹ La presente legge ha lo scopo di:

- a. garantire il trattamento sicuro delle informazioni di competenza della Confederazione nonché l'impiego sicuro dei mezzi informatici della Confederazione;
- b. aumentare la capacità della Svizzera di fronteggiare le cyberminacce.

¹ FF 2023 84

² RS 128; RU 2022 232

Art. 2 cpv. 5, primo periodo

⁵ Alle organizzazioni di diritto pubblico o privato che gestiscono infrastrutture critiche ma che non sono contemplate ai capoversi 1–3 si applicano gli articoli 73a–79. ...

Art. 4 cpv. 1 e 1^{bis}

¹ La legge del 17 dicembre 2004³ sulla trasparenza (LTras) prevale sulla presente legge.

^{1bis} Le informazioni provenienti da terzi di cui il Centro nazionale per la cibersecurity (NCSC) viene a conoscenza nella sua attività di ricezione e analisi di segnalazioni secondo il capitolo 5 non possono essere rese accessibili secondo la LTras. Non sono considerati terzi le autorità, le organizzazioni e le persone menzionate all'articolo 2 capoverso 1 LTras.

Art. 5, frase introduttiva (concerne soltanto il testo francese) e lett. d–g

Ai sensi della presente legge s'intende per:

- d. *ciberincidente*: un evento che si verifica nell'utilizzo di mezzi informatici e che compromette la confidenzialità, la disponibilità o l'integrità delle informazioni o la tracciabilità del loro trattamento;
- e. *ciberattacco*: un ciberincidente provocato intenzionalmente;
- f. *ciberminaccia*: qualsiasi circostanza o evento che ha il potenziale di provocare un ciberincidente;
- g. *vulnerabilità*: una ciberminaccia riconducibile a punti deboli o errori nei mezzi informatici.

Inserire prima del titolo della sezione 2

Art. 10a **Trattamento di dati personali**

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

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

- a. ciò sia utile al fine di garantire la sicurezza delle informazioni;
- b. non sia violato alcun obbligo legale o contrattuale di serbare il segreto;
- c. siano rispettate le disposizioni della legislazione federale sulla protezione dei dati; e

³ RS 152.3

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

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

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

⁵ Se necessario per far fronte a violazioni della sicurezza delle informazioni o per eliminare vulnerabilità, le autorità e organizzazioni assoggettate possono eseguire con i dati personali degni di particolare protezione ai sensi dell'articolo 5 lettera c della legge federale del 25 settembre 2020⁴ sulla protezione dei dati (LPD) di persone che sono o potrebbero essere coinvolte in tali violazioni o vulnerabilità o che sono o potrebbero esserne interessate le operazioni seguenti:

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

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

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

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

Art. 23 cpv. 3

Concerne soltanto il testo francese

Art. 44 cpv. 2

² La restrizione del diritto d'accesso è retta dall'articolo 26 LPD⁵.

⁴ RS 235.1

⁵ RS 235.1

Titolo dopo l'art. 73

Capitolo 5: Misure della Confederazione per la protezione della Svizzera dalle cyberminacce

Sezione 1: Disposizioni generali

Art. 73a Principio

¹ Per proteggere la Svizzera dalle cyberminacce, il NCSC effettua analisi tecniche al fine di valutare e contrastare ciberincidenti e cyberminacce, nonché di identificare ed eliminare vulnerabilità.

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

- a. sensibilizzare e avvisare il pubblico riguardo alle cyberminacce;
- b. avvisare le autorità, le organizzazioni e le persone interessate in caso di cyberminacce imminenti o di ciberattacchi in corso;
- c. pubblicare informazioni sulla cibersicurezza e raccomandazioni per l'adozione di misure preventive e reattive contro i ciberincidenti;
- d. ricevere e trattare le segnalazioni riguardanti ciberincidenti e cyberminacce;
- e. sostenere i gestori di infrastrutture critiche.

Art. 73b Segnalazioni

¹ Il NCSC è il destinatario delle segnalazioni riguardanti ciberincidenti e cyberminacce. Le segnalazioni possono essere anonime.

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

³ Se viene a conoscenza di vulnerabilità, il NCSC informa immediatamente il produttore dell'hardware o del software interessato e gli fissa un congruo termine per eliminarle. Gli indica che un'inosservanza può essere sanzionata secondo il diritto in materia di appalti pubblici (art. 44 cpv. 1 lett. f^{bis} della legge federale del 21 giugno 2019⁶ sugli appalti pubblici) e che il NCSC, allo scadere del termine, può rendere pubblica la vulnerabilità ai sensi dell'articolo 73c capoverso 2.

Art. 73c Pubblicazione di informazioni provenienti da segnalazioni

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

⁶ RS 172.056.1

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

Art. 73d Inoltro di informazioni

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

² Se dalla segnalazione di un ciberincidente o dalla sua analisi emergono informazioni necessarie a individuare tempestivamente e sventare minacce per la sicurezza interna o esterna, a valutare la situazione di minaccia o ad assicurare un servizio di preallerta informativa per la protezione di infrastrutture critiche secondo l'articolo 6 capoversi 1 lettera a, 2 e 5 della legge federale del 25 settembre 2015⁷ sulle attività informative (LAIn), il NCSC inoltra queste informazioni al SIC.

³ I collaboratori del NCSC che nell'ambito di una segnalazione o della sua analisi constatano indizi di un possibile reato lo denunciano unicamente al direttore del NCSC, in deroga all'articolo 22a capoverso 1 della legge del 24 marzo 2000⁸ sul personale federale. Se la gravità del possibile reato lo esige, il direttore del NCSC può sporgere denuncia presso le autorità di perseguimento penale.

⁴ Il NCSC può inoltrare informazioni che rivelano segreti protetti dal diritto penale unicamente secondo quanto disposto dall'articolo 320 del Codice penale⁹.

Titolo prima dell'art. 74

Abrogato

Art. 74 Sostegno ai gestori di infrastrutture critiche

¹ Il NCSC sostiene i gestori di infrastrutture critiche nella protezione contro le cyberminacce.

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

- a. un sistema di comunicazione per lo scambio sicuro delle informazioni;
- b. informazioni tecniche sulle cyberminacce attuali e raccomandazioni per l'adozione di misure preventive e reattive contro i ciberincidenti;
- c. strumenti tecnici e istruzioni per l'individuazione di ciberincidenti che rispondono alle elevate esigenze di protezione delle infrastrutture critiche.

⁷ RS 121

⁸ RS 172.220.1

⁹ RS 311.0

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

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

Titolo dopo l'art. 74

Sezione 2: Obbligo di segnalare ciberattacchi

Art. 74a Principi

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

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

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

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

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

¹ L'obbligo di segnalazione si applica:

- a. alle scuole universitarie secondo l'articolo 2 capoverso 2 della legge federale del 30 settembre 2011¹⁰ sulla promozione e sul coordinamento del settore universitario svizzero;
- b. alle autorità federali, cantonali e comunali nonché alle organizzazioni intercantionali, cantonali e intercomunali; è eccettuato l'Aggruppamento Difesa, laddove l'esercito presta servizio d'appoggio secondo articolo 67 o servizio attivo secondo l'articolo 76 della legge militare del 3 febbraio 1995¹¹;
- c. alle organizzazioni cui sono affidati compiti di diritto pubblico nei settori della sicurezza e del salvataggio, dell'approvvigionamento di acqua potabile, del trattamento delle acque di scarico e dello smaltimento dei rifiuti;

¹⁰ RS 414.20

¹¹ RS 510.10

- d. alle imprese attive nel settore dell'approvvigionamento energetico secondo l'articolo 6 capoverso 1 della legge federale del 30 settembre 2016¹² sull'energia, nonché nel commercio, nella misurazione e nella gestione dell'energia; sono esentati i titolari di licenze conformemente alla legge federale del 21 marzo 2003¹³ sull'energia nucleare, per quanto riguarda i ciberattacchi effettuati contro un impianto nucleare;
- e. alle imprese che sottostanno alla legge dell'8 novembre 1934¹⁴ sulle banche, alla legge del 17 dicembre 2004¹⁵ sulla sorveglianza degli assicuratori o alla legge del 19 giugno 2015¹⁶ sull'infrastruttura finanziaria;
- f. agli stabilimenti che figurano nell'elenco cantonale di cui all'articolo 39 capoverso 1 lettera e della legge federale del 18 marzo 1994¹⁷ sull'assicurazione malattie;
- g. ai laboratori medici che dispongono di un'autorizzazione secondo l'articolo 16 capoverso 1 della legge del 28 settembre 2012¹⁸ sulle epidemie;
- h. alle imprese che dispongono di un'omologazione secondo la legge del 15 dicembre 2000¹⁹ sugli agenti terapeutici per la fabbricazione, l'immissione in commercio e l'importazione di medicinali;
- i. alle organizzazioni che forniscono prestazioni volte a coprire le conseguenze di malattie, infortuni, incapacità al lavoro e al guadagno, vecchiaia, invalidità e grande invalidità;
- j. alla Società svizzera di radiotelevisione;
- k. alle agenzie di stampa d'importanza nazionale;
- l. ai fornitori di servizi postali registrati presso la Commissione delle poste secondo l'articolo 4 capoverso 1 della legge del 17 dicembre 2010²⁰ sulle poste;
- m. alle imprese ferroviarie secondo gli articoli 5 o 8c della legge federale del 20 dicembre 1957²¹ sulle ferrovie e alle imprese che gestiscono impianti di trasporto a fune, linee filoviarie, autobus e battelli e sono titolari di una concessione secondo l'articolo 6 della legge del 20 marzo 2009²² sul trasporto di viaggiatori;
- n. alle imprese dell'aviazione civile che dispongono di un'autorizzazione dell'Ufficio federale dell'aviazione civile e agli aeroporti nazionali conformemente al Piano settoriale dei trasporti, Parte Infrastruttura aeronautica;

12 RS 730.0

13 RS 732.1

14 RS 952.0

15 RS 961.01

16 RS 958.1

17 RS 832.10

18 RS 818.101

19 RS 812.21

20 RS 783.0

21 RS 742.101

22 RS 745.1

- o. alle imprese che trasportano merci sul Reno secondo la legge federale del 23 settembre 1953²³ sulla navigazione marittima sotto bandiera svizzera e alle imprese che gestiscono l'iscrizione, il carico o lo scarico nei porti di Basilea;
- p. alle imprese che riforniscono la popolazione di beni indispensabili di uso quotidiano e il cui dissesto totale o parziale comporterebbe considerevoli difficoltà di approvvigionamento;
- q. ai fornitori di servizi di telecomunicazione registrati presso l'Ufficio federale delle comunicazioni secondo l'articolo 4 capoverso 1 LTC²⁴;
- r. ai gestori di registri e ai centri di registrazione di domini Internet secondo l'articolo 28b LTC;
- s. ai fornitori e ai gestori di servizi e infrastrutture che servono all'esercizio dei diritti politici;
- t. ai fornitori e ai gestori di servizi di nuvole informatiche, motori di ricerca o servizi di sicurezza e fiduciari digitali nonché ai centri di calcolo, sempre che abbiano una sede in Svizzera;
- u. ai produttori di hardware o software i cui prodotti sono utilizzati da infrastrutture critiche, sempre che tali hardware o software abbiano un accesso remoto per la manutenzione o siano impiegati per uno dei seguenti scopi:
 - 1. la gestione e il monitoraggio di sistemi e processi tecnici,
 - 2. la garanzia della sicurezza pubblica.

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

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

Art. 74c Eccezioni all'obbligo di segnalazione

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

Art. 74d Ciberattacchi da segnalare

Un ciberattacco deve essere segnalato se:

- a. compromette il funzionamento dell'infrastruttura critica interessata;
- b. ha comportato una manipolazione o una fuga di informazioni;

²³ RS 747.30

²⁴ RS 784.10

- c. non è stato identificato per un periodo prolungato, in particolare se vi sono indizi secondo cui potrebbe essere stato effettuato per preparare altri ciberattacchi; o
- d. è connesso al reato di estorsione, minaccia o coazione.

Art. 74e Termine e contenuto della segnalazione

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

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

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

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

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

Art. 74f Trasmissione della segnalazione

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

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

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

Art. 74g Violazione dell'obbligo di segnalazione

¹ Se vi sono indizi di una violazione dell'obbligo di segnalazione, il NCSC informa l'autorità o l'organizzazione assoggettata a tale obbligo e le impartisce un congruo termine entro il quale adempierlo.

² Se l'autorità o l'organizzazione assoggettata all'obbligo di segnalazione non adempie il proprio obbligo entro il termine impartito, il NCSC emana una decisione fissando un nuovo termine, sotto la comminatoria della multa di cui all'articolo 74h.

Art. 74h Inosservanza di decisioni del NCSC

¹ Chi, intenzionalmente, non ottempera a una decisione del NCSC passata in giudicato intimatagli sotto la comminatoria prevista dal presente articolo o a una decisione dell'autorità di ricorso, è punito con la multa sino a 100 000 franchi.

² In caso di infrazioni di cui al capoverso 1 commesse nell'azienda è applicabile l'articolo 6 della legge federale del 22 marzo 1974²⁵ sul diritto penale amministrativo (DPA).

³ Se l'importo presumibile della multa non supera i 20 000 franchi e se la determinazione delle persone punibili secondo l'articolo 6 DPA esige provvedimenti d'inchiesta sproporzionati all'entità della pena, l'autorità può prescindere dal perseguimento di dette persone e, in loro vece, condannare l'azienda al pagamento della multa.

⁴ In caso di inosservanza di una decisione del NCSC, il perseguimento e il giudizio competono ai Cantoni.

Titolo prima dell'art. 75

Sezione 3: Protezione dei dati e scambio di informazioni

Art. 75 Trattamento di dati personali

¹ Per l'adempimento dei propri compiti, il NCSC può trattare dati personali, compresi elementi di indirizzo di cui all'articolo 3 lettera f LTC²⁶ e i relativi dati personali degni di particolare protezione, che contengono informazioni su:

- a. opinioni religiose, filosofiche o politiche; il trattamento è ammesso unicamente qualora sia necessario per la valutazione di minacce e pericoli concreti nell'ambito della cibersicurezza;
- b. perseguimenti o sanzioni di carattere amministrativo o penale.

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

Art. 76 Cooperazione a livello nazionale

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

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

²⁵ RS 313.0

²⁶ RS 784.10

Art. 76a Sostegno alle autorità

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

² Concede al SIC l'accesso a informazioni che riguardano l'identità e il modo di operare degli autori di ciberattacchi al fine di individuare tempestivamente e sventare minacce alla sicurezza interna o esterna, valutare la situazione di minaccia e assicurare un servizio di preallerta informativa per la protezione di infrastrutture critiche secondo l'articolo 6 capoversi 1 lettera a, 2 e 5 LAn²⁷.

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

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

Art. 77 Cooperazione a livello internazionale

¹ Il NCSC può scambiare con servizi esteri e internazionali competenti per la cibersicurezza informazioni che permettono di stabilire l'identità e il modo di operare degli autori di ciberattacchi, se detti servizi necessitano di tali informazioni per l'adempimento di compiti che corrispondono a quelli del NCSC. Se lo scambio di informazioni concerne anche dati personali, vanno osservati gli articoli 16 e 17 LPD²⁸.

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

Art. 78

Abrogato

Art. 79 cpv. 1

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

Art. 80

Abrogato

²⁷ RS 121

²⁸ RS 235.1

II

Gli atti normativi qui appresso sono modificati come segue:

1. Legge federale del 21 giugno 2019²⁹ sugli appalti pubblici

Art. 44 cpv. 1 lett. fbis

¹ Il committente può escludere un offerente dalla procedura di aggiudicazione, radiarlo da un elenco o revocare l'aggiudicazione, se constatata che l'offerente, un terzo coinvolto o i rispettivi organi realizzano una delle seguenti fattispecie:

fbis. non eliminano, entro il termine fissato dal Centro nazionale per la cibersicurezza secondo l'articolo 73b capoverso 3 della legge del 18 dicembre 2020³⁰ sulla sicurezza delle informazioni, una vulnerabilità nell'hardware o nel software da loro prodotto;

2. Legge federale del 25 settembre 2020³¹ sulla protezione dei dati

Art. 24 cpv. 5bis

^{5bis} Con il consenso del titolare del trattamento, l'IFPDT può inoltrare la notifica al Centro nazionale per la cibersicurezza ai fini dell'analisi dell'incidente. La comunicazione può contenere dati personali, compresi dati personali degni di particolare protezione su perseguimenti o sanzioni amministrativi e penali concernenti il titolare del trattamento.

3. Legge federale del 21 marzo 2003³² sull'energia nucleare

Art. 102 cpv. 2

² L'Ispektorato federale della sicurezza nucleare inoltra al Centro nazionale per la cibersicurezza le notifiche riguardanti un ciberattacco effettuato contro un impianto nucleare e adempienti le condizioni di cui all'articolo 74d della legge del 18 dicembre 2020³³ sulla sicurezza delle informazioni.

²⁹ RS 172.056.1

³⁰ RS 128; RU 2022 232

³¹ RS 235.1

³² RS 732.1

³³ RS 128; RU 2022 232

4. Legge del 23 marzo 2007³⁴ sull'approvvigionamento elettrico

Art. 8a Protezione contro le cyberminacce

¹ I gestori di rete, i produttori e i gestori di impianti di stoccaggio adottano misure per proteggere adeguatamente i loro impianti contro le cyberminacce.

² Il Consiglio federale può prevedere eccezioni e, se necessario per garantire l'approvvigionamento, estendere l'obbligo di cui al capoverso 1 ad altri fornitori attivi nel settore dell'approvvigionamento elettrico.

5. Legge del 22 giugno 2007³⁵ sulla vigilanza dei mercati finanziari

Art. 39 cpv. 1

¹ La FINMA è autorizzata a trasmettere ad altre autorità svizzere di vigilanza, al Centro nazionale per la cibersicurezza e alla Banca nazionale svizzera le informazioni non accessibili al pubblico di cui essi necessitano per adempiere i loro compiti.

III

¹ La presente legge sottostà a referendum facoltativo.

² Il Consiglio federale ne determina l'entrata in vigore.

Consiglio nazionale, 29 settembre 2023

Consiglio degli Stati, 29 settembre 2023

Il presidente: Martin Candinas

La presidente: Brigitte Häberli-Koller

Il segretario: Pierre-Hervé Freléchoz

La segretaria: Martina Buol

Data della pubblicazione: 10 ottobre 2023

Termine di referendum: 18 gennaio 2024

³⁴ RS 734.7

³⁵ RS 956.1

