

LEGGI ED ALTRI ATTI NORMATIVI

DECRETO LEGISLATIVO 18 maggio 2018, n. 65.

Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 76 e 87, quinto comma, della Costituzione;

Vista la legge 24 dicembre 2012, n. 234, recante norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea;

Vista la legge 25 ottobre 2017, n. 163, recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017;

Vista la direttiva (UE) 1148/2016 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione;

Visto il regolamento (CE) 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;

Vista la direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio;

Vista la raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese;

Visto il Regolamento di esecuzione della Commissione n. 2018/151/UE del 30 gennaio 2018 recante modalità di applicazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio per quanto riguarda l'ulteriore specificazione degli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente;

Visto il decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, recante misure urgenti per il contrasto del terrorismo internazionale;

Visto il decreto legislativo 4 marzo 2014, n. 39, recante attuazione della direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che sostituisce la decisione quadro 2004;

Vista la legge 3 agosto 2007, n. 124, recante sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto;

Visto il decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, recante proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione;

Visto il decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, recante misure urgenti per la crescita del Paese, e, in particolare, l'articolo 19, che ha istituito l'Agenzia per l'Italia digitale (AgID);

Visto il decreto legislativo 7 marzo 2005, n. 82, recante il codice dell'amministrazione digitale e, in particolare, le disposizioni in materia di funzioni dell'AgID e di sicurezza informatica;

Visto il decreto legislativo 11 aprile 2011, n. 61, attuativo della direttiva 2008/114/CE, recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione;

Visto il regolamento adottato con decreto del Presidente del Consiglio dei ministri 6 novembre 2015, n. 5, recante disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva;

Vista la direttiva adottata con decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, pubblicato nella *Gazzetta Ufficiale* n. 87 del 13 aprile 2017;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il codice in materia di protezione dei dati personali;

Visto il decreto legislativo 1° agosto 2003, n. 259, recante il codice delle comunicazioni elettroniche;

Visto il decreto legislativo 23 giugno 2011, n. 118, recante disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli enti locali e dei loro organismi, a norma degli articoli 1 e 2 della legge 5 maggio 2009, n. 42;

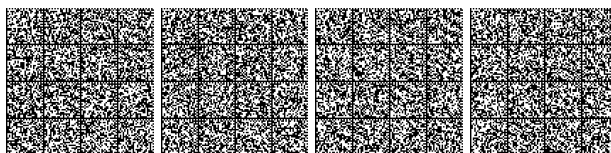
Vista la preliminare deliberazione del Consiglio dei ministri, adottata nella riunione dell'8 febbraio 2018;

Acquisito il parere della Conferenza Unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, reso nella seduta del 19 aprile 2018;

Acquisiti i pareri delle competenti Commissioni della Camera dei deputati e del Senato della Repubblica;

Vista la deliberazione del Consiglio dei ministri, adottata nella riunione del 16 maggio 2018;

Sulla proposta del Presidente del Consiglio dei ministri e del Ministro dello sviluppo economico, di concerto con i Ministri degli affari esteri e della cooperazione internazionale, della giustizia, dell'interno, della difesa, della salute e dell'economia e delle finanze;



EMANA

il seguente decreto legislativo:

Capo I

DISPOSIZIONI GENERALI

Art. 1.

Oggetto e ambito di applicazione

1. Il presente decreto stabilisce misure volte a conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea.

2. Ai fini del comma 1, il presente decreto prevede:

a) l'inclusione nella strategia nazionale di sicurezza cibernetica di previsioni in materia di sicurezza delle reti e dei sistemi informativi rientranti nell'ambito di applicazione del presente decreto;

b) la designazione delle autorità nazionali competenti e del punto di contatto unico, nonché del Gruppo di intervento per la sicurezza informatica in caso di incidenti (CSIRT) in ambito nazionale per lo svolgimento dei compiti di cui all'allegato I;

c) il rispetto di obblighi da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali relativamente all'adozione di misure di sicurezza e di notifica degli incidenti con impatto rilevante;

d) la partecipazione nazionale al gruppo di cooperazione europeo, nell'ottica della collaborazione e dello scambio di informazioni tra Stati membri dell'Unione europea, nonché dell'incremento della fiducia tra di essi;

e) la partecipazione nazionale alla rete CSIRT nell'ottica di assicurare una cooperazione tecnico-operativa rapida ed efficace.

3. Le disposizioni in materia di misure di sicurezza e di notifica degli incidenti di cui al presente decreto non si applicano alle imprese soggette agli obblighi di cui agli articoli 16-bis e 16-ter del decreto legislativo 1° agosto 2003, n. 259, né ai prestatori di servizi fiduciari soggetti agli obblighi di cui all'articolo 19 del regolamento (UE) n. 910/2014.

4. Il presente decreto si applica fatto salvo quanto previsto dal decreto legislativo 11 aprile 2011, n. 61, e dalla direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI, del Consiglio.

5. Fatto salvo quanto previsto dall'articolo 346 del trattato sul funzionamento dell'Unione europea, le informazioni riservate secondo quanto disposto dalla normativa dell'Unione europea e nazionale, in particolare per quanto concerne la riservatezza degli affari, sono scambiate con la Commissione europea e con altre autorità competenti NIS solo nella misura in cui tale scambio sia necessario ai fini dell'applicazione del presente decreto. Le informazioni scambiate sono pertinenti e commisurate

allo scopo. Lo scambio di informazioni ne tutela la riservatezza e protegge la sicurezza e gli interessi commerciali degli operatori di servizi essenziali e dei fornitori di servizi digitali.

6. Il presente decreto lascia impregiudicate le misure adottate per salvaguardare le funzioni essenziali dello Stato, in particolare di tutela della sicurezza nazionale, comprese le misure volte a tutelare le informazioni, nei casi in cui la divulgazione sia ritenuta contraria agli interessi essenziali di sicurezza e di mantenimento dell'ordine pubblico, in particolare a fini di indagine, accertamento e perseguimento di reati.

7. Qualora gli obblighi previsti per gli operatori di servizi essenziali o i fornitori di servizi digitali di assicurare la sicurezza delle loro reti e dei loro sistemi informativi o di notificare gli incidenti siano oggetto di uno specifico atto giuridico dell'Unione europea, si applicano le disposizioni di detto atto giuridico nella misura in cui gli effetti di tali obblighi siano almeno equivalenti a quelli degli obblighi di cui al presente decreto.

Art. 2.

Trattamento dei dati personali

1. Il trattamento dei dati personali in applicazione del presente decreto è effettuato ai sensi del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni.

Art. 3.

Definizioni

1. Ai fini del presente decreto si intende per:

a) autorità competente NIS, l'autorità competente per settore, in materia di sicurezza delle reti e dei sistemi informativi, di cui all'articolo 7, comma 1;

b) CSIRT, gruppo di intervento per la sicurezza informatica in caso di incidente, di cui all'articolo 8;

c) punto di contatto unico, l'organo incaricato a livello nazionale di coordinare le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione europea;

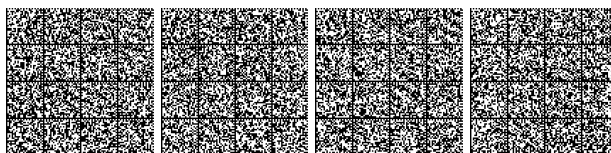
d) autorità di contrasto, l'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n.155;

e) rete e sistema informativo:

1) una rete di comunicazione elettronica ai sensi dell'articolo 1, comma 1, lettera *dd)*, del decreto legislativo 1° agosto 2003, n. 259;

2) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali;

3) i dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione;



f) sicurezza della rete e dei sistemi informativi, la capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi;

g) operatore di servizi essenziali, soggetto pubblico o privato, della tipologia di cui all'allegato II, che soddisfa i criteri di cui all'articolo 4, comma 2;

h) servizio digitale, servizio ai sensi dell'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, di un tipo elencato nell'allegato III;

i) fornitore di servizio digitale, qualsiasi persona giuridica che fornisce un servizio digitale;

l) incidente, ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi;

m) trattamento dell'incidente, tutte le procedure necessarie per l'identificazione, l'analisi e il contenimento di un incidente e l'intervento in caso di incidente;

n) rischio, ogni circostanza o evento ragionevolmente individuabile con potenziali effetti pregiudizievoli per la sicurezza della rete e dei sistemi informativi;

o) rappresentante, la persona fisica o giuridica stabilita nell'Unione europea espressamente designata ad agire per conto di un fornitore di servizi digitali che non è stabilito nell'Unione europea, a cui l'autorità competente NIS o il CSIRT Nazionale può rivolgersi in luogo del fornitore di servizi digitali, per quanto riguarda gli obblighi di quest'ultimo ai sensi del presente decreto;

p) norma, una norma ai sensi dell'articolo 2, primo paragrafo, numero 1), del regolamento (UE) n. 1025/2012;

q) specifica, una specifica tecnica ai sensi dell'articolo 2, primo paragrafo, numero 4), del regolamento (UE) n. 1025/2012;

r) punto di interscambio internet (IXP), una infrastruttura di rete che consente l'interconnessione di più di due sistemi autonomi indipendenti, principalmente al fine di agevolare lo scambio del traffico internet; un IXP fornisce interconnessione soltanto ai sistemi autonomi; un IXP non richiede che il traffico internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo, né altera o interferisce altrimenti con tale traffico;

s) sistema dei nomi di dominio (DNS), è un sistema distribuito e gerarchico di *naming* in una rete che inoltra le richieste dei nomi di dominio;

t) fornitore di servizi DNS, un soggetto che fornisce servizi DNS su internet;

u) registro dei nomi di dominio di primo livello, un soggetto che amministra e opera la registrazione di nomi di dominio internet nell'ambito di uno specifico dominio di primo livello (TLD);

v) mercato online, un servizio digitale che consente ai consumatori ovvero ai professionisti, come definiti rispettivamente all'articolo 141, comma 1, lettere a) e b), del decreto legislativo 6 settembre 2005, n. 206, di con-

cludere contratti di vendita o di servizi online con i professionisti sia sul sito web del mercato online sia sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato on line;

z) motore di ricerca on line, un servizio digitale che consente all'utente di effettuare ricerche, in linea di principio, su tutti i siti web o su siti web in una lingua particolare sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, frase o di altra immissione, e fornisce i link in cui possono essere trovate le informazioni relative al contenuto richiesto;

aa) servizio di *cloud computing*, un servizio digitale che consente l'accesso a un insieme scalabile ed elastico di risorse informatiche condivisibili.

Art. 4.

Identificazione degli operatori di servizi essenziali

1. Entro il 9 novembre 2018, con propri provvedimenti, le autorità competenti NIS identificano per ciascun settore e sottosectore di cui all'allegato II, gli operatori di servizi essenziali con una sede nel territorio nazionale. Gli operatori che prestano attività di assistenza sanitaria sono individuati con decreto del Ministro della salute, di intesa con la Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. Gli operatori che forniscono e distribuiscono acque destinate al consumo umano sono individuati con decreto del Ministro dell'ambiente e della tutela del territorio e del mare, di intesa con la Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano.

2. I criteri per l'identificazione degli operatori di servizi essenziali sono i seguenti:

a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali;

b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi;

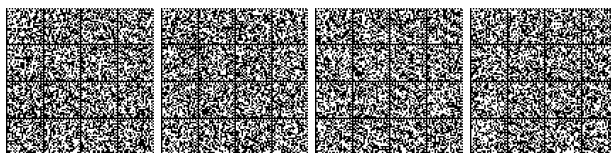
c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

3. Oltre ai criteri indicati nel comma 2, nell'individuazione degli operatori di servizi essenziali si tiene conto dei documenti prodotti al riguardo dal Gruppo di cooperazione di cui all'articolo 10.

4. Ai fini del comma 1, prima dell'adozione dei provvedimenti previsti dalla medesima disposizione, qualora un soggetto fornisca un servizio di cui al comma 2, lettera a), sul territorio nazionale e in altro o altri Stati membri dell'Unione europea, le autorità competenti NIS consultano le autorità competenti degli altri Stati membri.

5. È istituito presso il Ministero dello sviluppo economico un elenco nazionale degli operatori di servizi essenziali.

6. L'elenco degli operatori di servizi essenziali identificati ai sensi del comma 1 è riesaminato con le medesime modalità di cui al comma 1 e, se del caso, aggiornato su base regolare, ed almeno ogni due anni dopo il 9 maggio 2018, a cura delle autorità competenti NIS ed è comunicato al Ministero dello sviluppo economico.



7. Entro il 9 novembre 2018, e in seguito ogni due anni, il punto di contatto unico trasmette alla Commissione europea le informazioni necessarie per la valutazione dell'attuazione del presente decreto, in particolare della coerenza dell'approccio in merito all'identificazione degli operatori di servizi essenziali.

8. Le informazioni di cui al comma 7 comprendono almeno:

- a) le misure nazionali che consentono l'identificazione degli operatori di servizi essenziali;
- b) l'elenco dei servizi di cui al comma 2;
- c) il numero degli operatori di servizi essenziali identificati per ciascun settore di cui all'allegato II ed un'indicazione della loro importanza in relazione a tale settore;
- d) le soglie, ove esistano, per determinare il pertinente livello di fornitura con riferimento al numero di utenti che dipendono da tale servizio di cui all'articolo 5, comma 1, lettera a), o all'importanza di tale particolare operatore di servizi essenziali di cui all'articolo 5, comma 1, lettera f).

Art. 5.

Effetti negativi rilevanti

1. Ai fini della determinazione della rilevanza degli effetti negativi di cui all'articolo 4, comma 2, lettera c), le autorità competenti NIS considerano i seguenti fattori intersettoriali:

- a) il numero di utenti che dipendono dal servizio fornito dal soggetto interessato;
- b) la dipendenza di altri settori di cui all'allegato II dal servizio fornito da tale soggetto;
- c) l'impatto che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza;
- d) la quota di mercato di detto soggetto;
- e) la diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente;
- f) l'importanza del soggetto per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio.

2. Al fine della determinazione degli effetti negativi rilevanti di un incidente sono altresì considerati, ove opportuno, fattori settoriali.

Capo II

CONTESTO STRATEGICO E ISTITUZIONALE

Art. 6.

Strategia nazionale di sicurezza cibernetica

1. Il Presidente del Consiglio dei ministri adotta, sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR), la strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale.

2. Nell'ambito della strategia nazionale di sicurezza cibernetica, sono in particolare indicati, per la sicurezza di reti e sistemi informativi rientranti nell'ambito di applicazione del presente decreto:

- a) gli obiettivi e le priorità in materia di sicurezza delle reti e dei sistemi informativi;
- b) il quadro di governance per conseguire gli obiettivi e le priorità, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti;
- c) le misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato;
- d) i programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi;
- e) i piani di ricerca e sviluppo;
- f) un piano di valutazione dei rischi;
- g) l'elenco dei vari attori coinvolti nell'attuazione.

3. Con la procedura di cui al comma 1 sono adottate linee di indirizzo per l'attuazione della strategia nazionale di sicurezza cibernetica.

4. La Presidenza del Consiglio dei ministri trasmette la strategia nazionale in materia di sicurezza cibernetica alla Commissione europea entro tre mesi dalla sua adozione. Può essere esclusa la trasmissione di elementi della strategia riguardanti la sicurezza nazionale.

Art. 7.

Autorità nazionali competenti e punto di contatto unico

1. Sono designate quali Autorità competenti NIS per i settori e sottosectori di cui all'allegato II e per i servizi di cui all'allegato III:

- a) il Ministero dello sviluppo economico per il settore energia, sottosectori energia elettrica, gas e petrolio e per il settore infrastrutture digitali, sottosectori IXP, DNS, TLD, nonché per i servizi digitali;
- b) il Ministero delle infrastrutture e dei trasporti per il settore trasporti, sottosectori aereo, ferroviario, per vie d'acqua e su strada;
- c) il Ministero dell'economia e delle finanze per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob, secondo modalità di collaborazione e di scambio di informazioni stabilite con decreto del Ministro dell'economia e delle finanze;
- d) il Ministero della salute per l'attività di assistenza sanitaria, come definita dall'articolo 3, comma 1, lettera a), del decreto legislativo 4 marzo 2014, n. 38, prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità sanitarie territorialmente competenti, per le attività di assistenza sanitaria prestata dagli operatori autorizzati e accreditati delle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza;
- e) il Ministero dell'ambiente e della tutela del territorio e del mare e le Regioni e le Province autonome di



Trento e di Bolzano, direttamente o per il tramite delle Autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.

2. Le Autorità competenti NIS sono responsabili dell'attuazione del presente decreto con riguardo ai settori di cui all'allegato II e ai servizi di cui all'allegato III e vigilano sull'applicazione del presente decreto a livello nazionale esercitando altresì le relative potestà ispettive e sanzionatorie.

3. Il Dipartimento delle informazioni per la sicurezza (DIS) è designato quale punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi.

4. Il punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità competenti NIS con le autorità competenti degli altri Stati membri, nonché con il gruppo di cooperazione di cui all'articolo 10 e la rete di CSIRT di cui all'articolo 11.

5. Il punto di contatto unico collabora nel gruppo di cooperazione in modo effettivo, efficiente e sicuro con i rappresentanti designati dagli altri Stati.

6. Le autorità competenti NIS e il punto di contatto unico consultano, conformemente alla normativa vigente, l'autorità di contrasto ed il Garante per la protezione dei dati personali e collaborano con essi.

7. La Presidenza del Consiglio dei ministri comunica tempestivamente alla Commissione europea la designazione del punto di contatto unico e quella delle autorità competenti NIS, i relativi compiti e qualsiasi ulteriore modifica. Alle designazioni sono assicurate idonee forme di pubblicità.

8. Agli oneri derivanti dal presente articolo pari a 1.300.000 euro a decorrere dal 2018, si provvede ai sensi dell'articolo 22.

Art. 8.

Gruppi di intervento per la sicurezza informatica in caso di incidente - CSIRT

1. È istituito, presso la Presidenza del Consiglio dei ministri, il CSIRT italiano, che svolge i compiti e le funzioni del *Computer Emergency Response Team* (CERT) nazionale, di cui all'articolo 16-bis del decreto legislativo 1° agosto 2003, n. 259, e del CERT-PA, già operante presso l'Agenzia per l'Italia digitale ai sensi dell'articolo 51 del decreto legislativo 7 marzo 2005, n. 82.

2. L'organizzazione e il funzionamento del CSIRT italiano sono disciplinati con decreto del Presidente del Consiglio dei ministri ai sensi dell'articolo 7 del decreto legislativo 30 luglio 1999, n. 303, da adottare entro il 9 novembre 2018. Per lo svolgimento delle funzioni del CSIRT italiano, la Presidenza del Consiglio dei ministri si avvale di un contingente massimo di trenta unità di personale, di cui quindici scelti tra dipendenti di altre amministrazioni pubbliche, in posizione di comando o fuori ruolo, per i quali si applica l'articolo 17, comma 14, della legge 15 maggio 1997, n. 127, e quindici da assumere, nel limite della dotazione organica vigente, in aggiunta alle ordinarie facoltà assunzionali della Presidenza del Consiglio dei ministri, nel limite di spesa annuo di 1.300.000 di

euro a decorrere dal 2018. Ai relativi oneri si provvede ai sensi dell'articolo 22.

3. Nelle more dell'adozione del decreto di cui al comma 2, le funzioni di CSIRT italiano sono svolte dal CERT nazionale unitamente al CERT-PA in collaborazione tra loro.

4. Il CSIRT italiano assicura la conformità ai requisiti di cui all'allegato I, punto 1, svolge i compiti di cui all'allegato I, punto 2, si occupa dei settori di cui all'allegato II e dei servizi di cui all'allegato III e dispone di un'infrastruttura di informazione e comunicazione appropriata, sicura e resiliente a livello nazionale.

5. Il CSIRT italiano definisce le procedure per la prevenzione e la gestione degli incidenti informatici.

6. Il CSIRT italiano garantisce la collaborazione effettiva, efficiente e sicura, nella rete di CSIRT di cui all'articolo 11.

7. La Presidenza del Consiglio dei ministri comunica alla Commissione europea il mandato del CSIRT italiano e le modalità di trattamento degli incidenti a questo affidati.

8. Il CSIRT italiano, per lo svolgimento delle proprie funzioni, può avvalersi anche dell'Agenzia per l'Italia digitale.

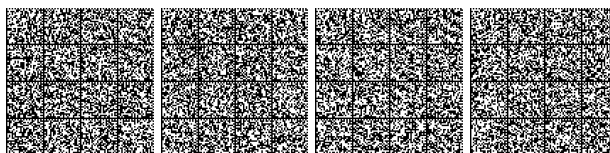
9. Le funzioni svolte dal Ministero dello sviluppo economico in qualità di CERT nazionale ai sensi dell'articolo 16-bis, del decreto legislativo 1° agosto 2003, n. 259, nonché quelle svolte da Agenzia per l'Italia digitale in qualità di CERT-PA, ai sensi dell'articolo 51 del decreto legislativo 7 marzo 2005, n. 82, sono trasferite al CSIRT italiano a far data dalla entrata in vigore del decreto di cui al comma 2.

10. Per le spese di funzionamento del CSIRT italiano è autorizzata la spesa di 2.700.000 euro per l'anno 2018, di cui 2.000.000 per le spese di investimenti, e di 700.000 annui a decorrere dall'anno 2019. A tali oneri si provvede ai sensi dell'articolo 22.

Art. 9.

Cooperazione a livello nazionale

1. Le autorità competenti NIS, il punto di contatto unico e il CSIRT italiano collaborano per l'adempimento degli obblighi di cui al presente decreto. A tal fine è istituito, presso la Presidenza del Consiglio dei ministri, un Comitato tecnico di raccordo, composto da rappresentanti delle amministrazioni statali competenti ai sensi dell'articolo 7, comma 1, e da rappresentanti delle Regioni e Province autonome in numero non superiore a due, designati dalle Regioni e Province autonome in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. L'organizzazione del Comitato è definita con decreto del Presidente del Consiglio dei ministri, da adottare su proposta dei Ministri per la semplificazione e la pubblica amministrazione e dello sviluppo economico, sentita la Conferenza unificata. Per la partecipazione al Comitato tecnico di raccordo non sono previsti gettoni di presenza, compensi o rimborsi spese.



2. Gli operatori di servizi essenziali e i fornitori di servizi digitali inviano le notifiche relative ad incidenti al CSIRT italiano.

3. Il CSIRT italiano informa le autorità competenti NIS e il punto di contatto unico in merito alle notifiche di incidenti trasmesse ai sensi del presente decreto.

Capo III

COOPERAZIONE

Art. 10.

Gruppo di cooperazione

1. Il punto di contatto unico partecipa alle attività del gruppo di cooperazione composto da rappresentanti degli Stati membri, della Commissione europea e dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e, in particolare, contribuisce a:

a) condividere buone pratiche sullo scambio di informazioni relative alla notifica di incidenti di cui all'articolo 12 e all'articolo 14;

b) scambiare migliori pratiche con gli Stati membri e, in collaborazione con l'ENISA, fornire supporto per la creazione di capacità in materia di sicurezza delle reti e dei sistemi informativi;

c) discutere le capacità e lo stato di preparazione degli Stati membri e valutare, su base volontaria, le strategie nazionali in materia di sicurezza delle reti e dei sistemi informativi e l'efficacia dei CSIRT e individuare le migliori pratiche;

d) scambiare informazioni e migliori pratiche in materia di sensibilizzazione e formazione;

e) scambiare informazioni e migliori pratiche in materia di ricerca e sviluppo riguardo alla sicurezza delle reti e dei sistemi informativi;

f) scambiare, ove opportuno, esperienze in materia di sicurezza delle reti e dei sistemi informativi con le istituzioni, gli organi e gli organismi pertinenti dell'Unione europea;

g) discutere le norme e le specifiche di cui all'articolo 17 con i rappresentanti delle pertinenti organizzazioni di normazione europee;

h) fornire informazioni in relazione ai rischi e agli incidenti;

i) esaminare, su base annuale, le relazioni sintetiche di cui al comma 4;

l) discutere il lavoro svolto riguardo a esercitazioni in materia di sicurezza delle reti e dei sistemi informativi, programmi di istruzione e formazione, comprese le attività svolte dall'ENISA;

m) con l'assistenza dell'ENISA, scambiare migliori pratiche connesse all'identificazione degli operatori di servizi essenziali da parte degli Stati membri, anche in relazione alle dipendenze transfrontaliere riguardo a rischi e incidenti;

n) discutere modalità per la comunicazione di notifiche di incidenti di cui agli articoli 12 e 14.

2. Le autorità competenti NIS, attraverso il punto di contatto unico, assicurano la partecipazione al gruppo di cooperazione al fine di elaborare ed adottare orientamenti sulle circostanze in cui gli operatori di servizi essenziali sono tenuti a notificare gli incidenti, compresi i parametri di cui all'articolo 12, comma 8.

3. Il punto di contatto unico, ove necessario, chiede alle autorità competenti NIS interessate, nonché al CSIRT, la partecipazione al gruppo di cooperazione.

4. Entro il 9 agosto 2018 e in seguito ogni anno, il punto di contatto unico trasmette una relazione sintetica al gruppo di cooperazione in merito alle notifiche ricevute, compresi il numero di notifiche e la natura degli incidenti notificati e alle azioni intraprese ai sensi degli articoli 12 e 14.

Art. 11.

Rete di CSIRT

1. Il CSIRT italiano partecipa alla rete di CSIRT, composta da rappresentanti dei CSIRT degli Stati membri e del CERT-UE.

2. Il CSIRT italiano, ai fini del comma 1, provvede a:

a) scambiare informazioni sui servizi, sulle operazioni e sulle capacità di cooperazione dei CSIRT;

b) su richiesta del rappresentante di un CSIRT di uno Stato membro potenzialmente interessato da un incidente, scambiare e discutere informazioni non sensibili sul piano commerciale connesse a tale incidente e i rischi associati, ad eccezione dei casi in cui lo scambio di informazioni potrebbe compromettere l'indagine sull'incidente;

c) scambiare e mettere a disposizione su base volontaria informazioni non riservate su singoli incidenti;

d) su richiesta di un rappresentante di un CSIRT di un altro Stato membro, discutere e, ove possibile, individuare un intervento coordinato per un incidente rilevato nella giurisdizione di quello stesso Stato membro;

e) fornire sostegno agli altri Stati membri nel far fronte a incidenti transfrontalieri sulla base dell'assistenza reciproca volontaria;

f) discutere, esaminare e individuare ulteriori forme di cooperazione operativa, anche in relazione a:

1) categorie di rischi e di incidenti;

2) preallarmi;

3) assistenza reciproca;

4) principi e modalità di coordinamento, quando gli Stati membri intervengono in relazione a rischi e incidenti transfrontalieri;

g) informare il gruppo di cooperazione in merito alle proprie attività e a ulteriori forme di cooperazione operativa discusse sulla scorta della lettera f) e chiedere orientamenti in merito;

h) discutere gli insegnamenti appresi dalle esercitazioni in materia di sicurezza delle reti e dei sistemi informativi, comprese quelle organizzate dall'ENISA;

i) formulare orientamenti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni del presente articolo in materia di cooperazione operativa.



*Capo IV*SICUREZZA DELLA RETE E DEI SISTEMI INFORMATIVI
DEGLI OPERATORI DI SERVIZI ESSENZIALI

Art. 12.

Obblighi in materia di sicurezza e notifica degli incidenti

1. Gli operatori di servizi essenziali adottano misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano nelle loro operazioni. Tenuto conto delle conoscenze più aggiornate in materia, dette misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente.

2. Gli operatori di servizi essenziali adottano misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali, al fine di assicurare la continuità di tali servizi.

3. Nell'adozione delle misure di cui ai commi 1 e 2, gli operatori di servizi essenziali tengono conto delle linee guida predisposte dal gruppo di cooperazione di cui all'articolo 10, nonché delle linee guida di cui al comma 7.

4. Fatto salvo quanto previsto dai commi 1, 2 e 3, le autorità competenti NIS possono, se necessario, definire specifiche misure, sentiti gli operatori di servizi essenziali.

5. Gli operatori di servizi essenziali notificano al CSIRT italiano e, per conoscenza, all'autorità competente NIS, senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti.

6. Il CSIRT italiano inoltra tempestivamente le notifiche all'organo istituito presso il Dipartimento informazioni per la sicurezza incaricato, ai sensi delle direttive del Presidente del Consiglio dei ministri adottate sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR), delle attività di prevenzione e preparazione ad eventuali situazioni di crisi e di attivazione delle procedure di allertamento.

7. Le notifiche includono le informazioni che consentono al CSIRT italiano di determinare un eventuale impatto transfrontaliero dell'incidente. La notifica non espone la parte che la effettua a una maggiore responsabilità rispetto a quella derivante dall'incidente. Le autorità competenti NIS possono predisporre linee guida per la notifica degli incidenti.

8. Per determinare la rilevanza dell'impatto di un incidente si tiene conto in particolare dei seguenti parametri:

- a) il numero di utenti interessati dalla perturbazione del servizio essenziale;
- b) la durata dell'incidente;
- c) la diffusione geografica relativamente all'area interessata dall'incidente.

9. Sulla base delle informazioni fornite nella notifica da parte dell'operatore di servizi essenziali, il CSIRT italiano informa gli eventuali altri Stati membri interessati

in cui l'incidente ha un impatto rilevante sulla continuità dei servizi essenziali.

10. Ai fini del comma 9, il CSIRT italiano preserva, conformemente al diritto dell'Unione europea e alla legislazione nazionale, la sicurezza e gli interessi commerciali dell'operatore di servizi essenziali, nonché la riservatezza delle informazioni fornite nella notifica secondo quanto previsto dall'articolo 1, comma 5.

11. Ove le circostanze lo consentano, il CSIRT italiano fornisce all'operatore di servizi essenziali, che effettua la notifica, le pertinenti informazioni relative al seguito della notifica stessa, nonché le informazioni che possono facilitare un trattamento efficace dell'incidente.

12. Su richiesta dell'autorità competente NIS o del CSIRT italiano, il punto di contatto unico trasmette, previa verifica dei presupposti, le notifiche ai punti di contatto unici degli altri Stati membri interessati.

13. Previa valutazione da parte dell'organo di cui al comma 6, l'autorità competente NIS, d'intesa con il CSIRT italiano, dopo aver consultato l'operatore dei servizi essenziali notificante, può informare il pubblico in merito ai singoli incidenti, qualora ne sia necessaria la sensibilizzazione per evitare un incidente o gestire un incidente in corso.

14. Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Gli operatori di servizi essenziali provvedono agli adempimenti previsti dal presente articolo a valere sulle risorse finanziarie disponibili sui propri bilanci.

Art. 13.

Attuazione e controllo

1. Le autorità competenti NIS valutano il rispetto da parte degli operatori di servizi essenziali degli obblighi previsti dall'articolo 12, nonché i relativi effetti sulla sicurezza della rete e dei sistemi informativi.

2. Ai fini del comma 1, gli operatori di servizi essenziali sono tenuti a fornire all'autorità competente NIS:

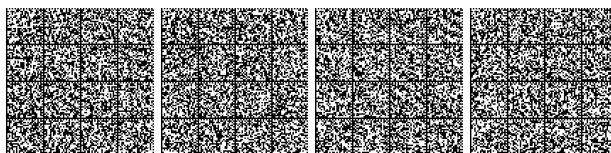
a) le informazioni necessarie per valutare la sicurezza della loro rete e dei loro sistemi informativi, compresi i documenti relativi alle politiche di sicurezza;

b) la prova dell'effettiva attuazione delle politiche di sicurezza, come i risultati di un audit sulla sicurezza svolto dall'autorità competente NIS o da un revisore abilitato e, in quest'ultimo caso, metterne a disposizione dell'autorità competente NIS i risultati, inclusi gli elementi di prova.

3. Quando richiede le informazioni o le prove di cui al comma 2, l'autorità competente NIS indica lo scopo delle richieste specificando il tipo di informazioni da fornire.

4. A seguito della valutazione delle informazioni o dei risultati degli audit sulla sicurezza di cui al comma 2, l'autorità competente NIS può emanare istruzioni vincolanti per gli operatori di servizi essenziali al fine di porre rimedio alle carenze individuate.

5. Nei casi di incidenti che comportano violazioni di dati personali, l'autorità competente NIS opera in stretta cooperazione con il Garante per la protezione dei dati personali.



*Capo V*SICUREZZA DELLA RETE E DEI SISTEMI INFORMATIVI
DEI FORNITORI DI SERVIZI DIGITALI

Art. 14.

Obblighi in materia di sicurezza e notifica degli incidenti

1. I fornitori di servizi digitali identificano e adottano misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi relativi alla sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dell'offerta di servizi di cui all'allegato III all'interno dell'Unione europea.

2. Tenuto conto delle conoscenze più aggiornate in materia, tali misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente e tengono conto dei seguenti elementi:

- a) la sicurezza dei sistemi e degli impianti;
- b) trattamento degli incidenti;
- c) gestione della continuità operativa;
- d) monitoraggio, audit e test;
- e) conformità con le norme internazionali.

3. I fornitori di servizi digitali adottano misure per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi del fornitore di servizi digitali sui servizi di cui all'allegato III offerti all'interno dell'Unione europea, al fine di assicurare la continuità di tali servizi.

4. I fornitori di servizi digitali notificano al CSIRT italiano e, per conoscenza, all'autorità competente NIS, senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla fornitura di un servizio di cui all'allegato III che essi offrono all'interno dell'Unione europea.

5. Le notifiche includono le informazioni che consentono al CSIRT italiano di determinare la rilevanza di un eventuale impatto transfrontaliero. La notifica non espone la parte che la effettua a una maggiore responsabilità rispetto a quella derivante dall'incidente.

6. Il CSIRT italiano inoltra tempestivamente le notifiche all'organo di cui all'articolo 12, comma 6.

7. Al fine di determinare la rilevanza dell'impatto di un incidente, sono tenuti in considerazione, in particolare, i seguenti parametri:

- a) il numero di utenti interessati dall'incidente, in particolare gli utenti che dipendono dal servizio digitale per la fornitura dei propri servizi;
- b) la durata dell'incidente;
- c) la diffusione geografica relativamente all'area interessata dall'incidente;
- d) la portata della perturbazione del funzionamento del servizio;
- e) la portata dell'impatto sulle attività economiche e sociali.

8. L'obbligo di notificare un incidente si applica soltanto qualora il fornitore di servizi digitali abbia accesso alle informazioni necessarie per valutare l'impatto di un incidente con riferimento ai parametri di cui al comma 7.

9. Qualora un operatore di servizi essenziali dipenda da una terza parte fornitrice di servizi digitali per la fornitura di un servizio che è indispensabile per il mantenimento di attività economiche e sociali fondamentali, l'operatore stesso notifica qualsiasi impatto rilevante per la continuità di servizi essenziali dovuto ad un incidente a carico di tale operatore.

10. Qualora l'incidente di cui al comma 4 riguardi due o più Stati membri, il CSIRT italiano informa gli altri Stati membri coinvolti.

11. Ai fini del comma 9, il CSIRT italiano tutela, nel rispetto del diritto dell'Unione europea e della legislazione nazionale, la sicurezza e gli interessi commerciali del fornitore del servizio digitale nonché la riservatezza delle informazioni fornite.

12. Previa valutazione da parte dell'organo di cui all'articolo 12, comma 6, l'autorità competente NIS, d'intesa con il CSIRT italiano, dopo aver consultato il fornitore di servizi digitali interessato e, se del caso, le autorità competenti o i CSIRT degli altri Stati membri interessati, può informare il pubblico riguardo ai singoli incidenti o chiedere al fornitore di servizi digitali di provvedervi, qualora ne sia necessaria la sensibilizzazione per evitare un incidente o gestirne uno in corso, o qualora sussista comunque un interesse pubblico alla divulgazione dell'incidente.

13. I fornitori di servizi digitali applicano le disposizioni di attuazione degli atti di esecuzione della Commissione europea che specificano ulteriormente le misure tecnico-organizzative di cui al comma 1 e i parametri, ivi compresi formati e procedure, relativi agli obblighi di notifica di cui al comma 4.

14. Fatto salvo quanto previsto dall'articolo 1, comma 7, non sono imposti ulteriori obblighi in materia di sicurezza o di notifica ai fornitori di servizi digitali.

15. Il presente capo non si applica alle microimprese e alle piccole imprese quali definite nella raccomandazione della Commissione europea del 6 maggio 2003, n. 2003/361/CE.

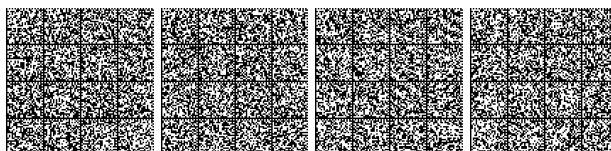
Art. 15.

Attuazione e controllo

1. Nel caso in cui sia dimostrato il mancato rispetto degli obblighi di cui all'articolo 14 da parte dei fornitori di servizi digitali, l'autorità competente NIS può adottare misure di vigilanza *ex post* adeguate alla natura dei servizi e delle operazioni. La dimostrazione del mancato rispetto degli obblighi può essere prodotta dall'autorità competente di un altro Stato membro in cui è fornito il servizio.

2. Ai fini del comma 1, i fornitori di servizi digitali sono tenuti a:

- a) fornire le informazioni necessarie per valutare la sicurezza della loro rete e dei loro sistemi informativi, compresi i documenti relativi alle politiche di sicurezza;



b) porre rimedio ad ogni mancato adempimento degli obblighi di cui all'articolo 14.

3. Se un fornitore di servizi digitali ha lo stabilimento principale o un rappresentante in uno Stato membro, ma la sua rete o i suoi sistemi informativi sono ubicati in uno o più altri Stati membri, l'autorità competente dello Stato membro dello stabilimento principale o del rappresentante e le autorità competenti dei suddetti altri Stati membri cooperano e si assistono reciprocamente in funzione delle necessità. Tale assistenza e cooperazione può comprendere scambi di informazioni tra le autorità competenti interessate e richieste di adottare le misure di vigilanza di cui al comma 1.

Art. 16.

Giurisdizione e territorialità

1. Ai fini del presente decreto, un fornitore di servizi digitali è considerato soggetto alla giurisdizione dello Stato membro in cui ha lo stabilimento principale. Un fornitore di servizi digitali è comunque considerato avere il proprio stabilimento principale in uno Stato membro quando ha la sua sede sociale in tale Stato membro.

2. Un fornitore di servizi digitali che non è stabilito nell'Unione europea, ma offre servizi di cui all'allegato III all'interno dell'Unione europea, designa un rappresentante nell'Unione europea.

3. Il rappresentante è stabilito in uno di quegli Stati membri in cui sono offerti i servizi. Il fornitore di servizi digitali è considerato soggetto alla giurisdizione dello Stato membro in cui è stabilito il suo rappresentante.

4. La designazione di un rappresentante da parte di un fornitore di servizi digitali fa salve le azioni legali che potrebbero essere avviate nei confronti del fornitore stesso di servizi digitali.

Capo VI

NORMAZIONE E NOTIFICA VOLONTARIA

Art. 17.

Normazione

1. Ai fini dell'attuazione armonizzata dell'articolo 12, commi 1 e 2, e dell'articolo 14, commi 1, 2 e 3, le autorità competenti NIS promuovono l'adozione di norme e specifiche europee o accettate a livello internazionale relative alla sicurezza della rete e dei sistemi informativi, senza imporre o creare discriminazioni a favore dell'uso di un particolare tipo di tecnologia.

2. Le autorità competenti NIS tengono conto dei pareri e delle linee guida predisposti dall'ENISA, in collaborazione con gli Stati membri, riguardanti i settori tecnici da prendere in considerazione in relazione al comma 1, nonché le norme già esistenti, comprese le norme nazionali, che potrebbero essere applicate a tali settori.

Art. 18.

Notifica volontaria

1. I soggetti che non sono stati identificati come operatori di servizi essenziali e non sono fornitori di servizi digitali possono notificare, su base volontaria, gli incidenti aventi un impatto rilevante sulla continuità dei servizi da loro prestati.

2. Nel trattamento delle notifiche, il CSIRT italiano applica la procedura di cui all'articolo 12.

3. Le notifiche obbligatorie sono trattate prioritariamente rispetto alle notifiche volontarie.

4. Le notifiche volontarie sono trattate soltanto qualora tale trattamento non costituisca un onere sproporzionato o eccessivo.

5. La notifica volontaria non può avere l'effetto di imporre al soggetto notificante alcun obbligo a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica.

Capo VII

DISPOSIZIONI FINALI

Art. 19.

Poteri ispettivi

1. L'attività di ispezione e verifica necessarie per le misure previste dagli articoli 12, 13, 14 e 15, fatte salve le attribuzioni e le competenze degli organi preposti alla tutela dell'ordine e della sicurezza pubblica, sono svolte dalle autorità competenti NIS.

2. Con successivo Accordo tra Governo, Regioni e Province autonome di Trento e di Bolzano sono definiti i criteri uniformi in ambito nazionale per lo svolgimento delle attività di ispezione e verifica, necessarie per le misure previste dagli articoli 12, 13, 14 e 15, che riguardano le reti e i sistemi informativi utilizzati dagli operatori che prestano attività di assistenza sanitaria, nonché in merito al settore fornitura e distribuzione di acqua potabile.

Art. 20.

Autorità competente e regime dell'accertamento e dell'irrogazione delle sanzioni amministrative

1. Le autorità competenti NIS di cui all'articolo 7, comma 1, lettere a), b), c), d) ed e), per i rispettivi settori e sottosectori di riferimento di cui all'allegato II e per i servizi di cui all'allegato III, sono competenti per l'accertamento delle violazioni e per l'irrogazione delle sanzioni amministrative previste dal presente decreto.

2. Ai fini dell'accertamento e dell'irrogazione delle sanzioni amministrative di cui al comma 1, si osservano le disposizioni contenute nel capo I, sezioni I e II, della legge 24 novembre 1981, n. 689.



Art. 21.

Sanzioni amministrative

1. Salvo che il fatto costituisca reato, l'operatore di servizi essenziali che non adotta le misure tecniche e organizzative adeguate e proporzionate per la gestione del rischio per la sicurezza della rete e dei sistemi informativi, ai sensi dell'articolo 12, comma 1, è soggetto ad una sanzione amministrativa pecuniaria da 12.000 euro a 120.000 euro. La sanzione è ridotta di un terzo se lo stesso fatto è commesso da un fornitore di servizio digitale, in violazione degli obblighi di cui all'articolo 14, comma 1.

2. Salvo che il fatto costituisca reato, l'operatore di servizi essenziali che non adotta le misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali, ai sensi dell'articolo 12, comma 2, è soggetto ad una sanzione amministrativa pecuniaria da 12.000 euro a 120.000 euro. La sanzione è ridotta di un terzo se lo stesso fatto è commesso da un fornitore di servizio digitale, in violazione degli obblighi di cui all'articolo 14, comma 3.

3. Salvo che il fatto costituisca reato, l'operatore di servizio essenziale che non notifica al CSIRT italiano gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti, ai sensi dell'articolo 12, comma 5, è soggetto ad una sanzione amministrativa pecuniaria da 25.000 euro a 125.000 euro.

4. Salvo che il fatto costituisca reato, l'operatore di servizio essenziale che non ottempera agli obblighi, ai sensi dell'articolo 13, comma 2, è soggetto ad una sanzione amministrativa pecuniaria da 12.000 euro a 120.000 euro.

5. Salvo che il fatto costituisca reato, l'operatore di servizio essenziale che non osserva le istruzioni, ai sensi dell'articolo 13, comma 4, è soggetto ad una sanzione amministrativa pecuniaria da 15.000 euro a 150.000 euro.

6. Salvo che il fatto costituisca reato, il fornitore di servizio digitale che non notifica al CSIRT italiano gli incidenti aventi un impatto rilevante sulla fornitura di un servizio fornito, ai sensi dell'articolo 14, comma 4, è soggetto ad una sanzione amministrativa pecuniaria da 25.000 euro a 125.000 euro.

7. Salvo che il fatto costituisca reato, l'operatore di servizi essenziali dipendente da terze parti che fornisce servizi digitali per la fornitura di un servizio che è indispensabile per il mantenimento di attività economiche e sociali fondamentali, che ometta la notifica, ai sensi dell'articolo 14, comma 9, è soggetto ad una sanzione amministrativa pecuniaria da 12.000 euro a 120.000 euro.

8. Salvo che il fatto costituisca reato, il fornitore di servizi digitali che non osserva gli obblighi ai sensi dell'articolo 15, comma 2, è soggetto ad una sanzione amministrativa pecuniaria da 12.000 euro a 120.000 euro.

9. Si ha reiterazione delle violazioni di cui al presente articolo nei casi regolati dall'articolo 8-bis della legge 24 novembre del 1981, n. 689. La reiterazione determina l'aumento fino al triplo della sanzione prevista.

Art. 22.

Disposizioni finanziarie

1. Agli oneri derivanti dagli articoli 7 e 8, pari a 5.300.000 euro per l'anno 2018 e 3.300.000 euro annui a decorrere dall'anno 2019, si provvede mediante corrispondente riduzione del Fondo per il recepimento della normativa europea di cui all'articolo 41-bis della legge 24 dicembre 2012, n. 234.

2. Le spese ICT sostenute dalle pubbliche amministrazioni ai sensi degli articoli 7, 8 e 12 del presente decreto e più in generale le spese ICT sostenute per l'adeguamento dei sistemi informativi al presente decreto sono coerenti con il Piano triennale per l'informatica nella pubblica amministrazione ai sensi dei commi da 512 a 520, dell'articolo 1, della legge 28 dicembre 2015, n. 208.

3. Dall'attuazione del presente decreto, ad esclusione degli articoli 7 e 8, non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e le amministrazioni pubbliche provvedono con le risorse umane, strumentali e finanziarie previste a legislazione vigente.

4. Il Ministro dell'economia e delle finanze è autorizzato ad apportare le occorrenti variazioni di bilancio negli stati di previsione interessati.



Il presente decreto munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addì, 18 maggio 2018

MATTARELLA

GENTILONI SILVERI, *Presidente del Consiglio dei ministri*
CALENDA, *Ministro dello sviluppo economico*
ALFANO, *Ministro degli affari esteri e della cooperazione internazionale*
ORLANDO, *Ministro della giustizia*
MINNITI, *Ministro dell'interno*
PINOTTI, *Ministro della difesa*
LORENZIN, *Ministro della salute*
PADOAN, *Ministro dell'economia e delle finanze*

Visto, il Guardasigilli: ORLANDO

ALLEGATO I

(di cui all'art. 8)

REQUISITI E COMPITI DEI GRUPPI DI INTERVENTO PER LA SICUREZZA INFORMATICA IN CASO DI INCIDENTE (CSIRT)

I requisiti e i compiti del CSIRT sono adeguatamente e chiaramente definiti ai sensi del presente decreto e del decreto del Presidente del Consiglio dei ministri di cui all'art. 8, comma 2. Essi includono quanto segue:

1. Requisiti per il CSIRT

a) Il CSIRT garantisce un alto livello di disponibilità dei propri servizi di comunicazione, evitando singoli punti di guasto, e dispone di vari mezzi che permettono allo stesso di essere contattato e di contattare altri in qualsiasi momento. Inoltre, i canali di comunicazione sono chiaramente specificati e ben noti alla loro base di utenti e ai partner con cui collaborano.

b) I locali del CSIRT e i sistemi informativi di supporto sono ubicati in siti sicuri.

c) Continuità operativa:

i. il CSIRT è dotato di un sistema adeguato di gestione e inoltro delle richieste in modo da facilitare i passaggi;

ii. il CSIRT dispone di personale sufficiente per garantirne l'operatività 24 ore su 24;

iii. il CSIRT opera in base a un'infrastruttura di cui è garantita la continuità. A tal fine è necessario che siano disponibili sistemi ridondanti e spazi di lavoro di backup.

d) Il CSIRT ha la possibilità, se lo desidera, di partecipare a reti di cooperazione internazionale.

2. Compiti del CSIRT

a) I compiti del CSIRT comprendono almeno:

i. monitoraggio degli incidenti a livello nazionale;

ii. emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti;

iii. intervento in caso di incidente;

iv. analisi dinamica dei rischi e degli incidenti, nonché sensibilizzazione situazionale;

v. partecipazione alla rete dei CSIRT;

b) il CSIRT stabilisce relazioni di cooperazione con il settore privato;

c) per facilitare la cooperazione, il CSIRT promuove l'adozione e l'uso di prassi comuni o standardizzate nei seguenti settori:

i. procedure di trattamento degli incidenti e dei rischi;

ii. sistemi di classificazione degli incidenti, dei rischi e delle informazioni.



ALLEGATO II

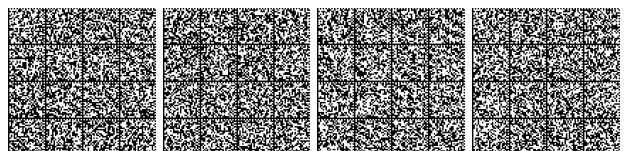
(di cui art. 3, comma 1, lettera g)

OPERATORI DI SERVIZI ESSENZIALI

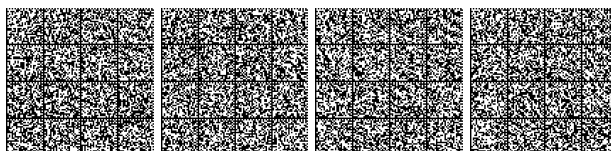
Settore	Sottosettore	Tipo di soggetto
1. Energia	a) Energia elettrica	Impresa elettrica quale definita all'articolo 2, comma 25-terdecies, del decreto legislativo 16 marzo 1999, 79, che esercita attività di «fornitura» quale all'articolo 2, comma 25-sexies, di tale decreto legislativo
		Gestori del sistema di distribuzione quali definiti all'articolo 2, comma 25-ter, del decreto legislativo 16 marzo 1999, 79
		Gestori del sistema di trasmissione quali definiti all'articolo 2, comma 25-bis, del decreto legislativo 16 marzo 1999, 79
	b) Petrolio	Gestori di oleodotti
		Gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio
	c) Gas	Imprese fornitrici quali definite all'articolo 2, comma 1, lettera kk-septies), del decreto legislativo 23 maggio 2000, n. 164
		Gestori del sistema di distribuzione quali definiti all'articolo 2, comma 1, lettera kk-sexies), del decreto legislativo 23 maggio 2000, n. 164
		Gestori del sistema di trasmissione quali definiti all'articolo 2, comma 1, lettera kk-quater), del decreto legislativo 23 maggio 2000, n. 164
		Gestori dell'impianto di stoccaggio quali definiti all'articolo 2, comma 1, lettera kk-nonies), del decreto legislativo 23 maggio 2000, n. 164
		Gestori del sistema GNL quali definiti all'articolo 2, comma 1, lettera kk-decies), del decreto legislativo 23 maggio 2000, n. 164
		Imprese di gas naturale quale quali definite all'articolo 2, comma 1, lettera t), del decreto legislativo 23 maggio 2000, n. 164
		Gestori di impianti di raffinazione e trattamento di gas naturale



2. Trasporti	a) Trasporto aereo	Vettori aerei quali definiti all'articolo 3, primo paragrafo, numero 4), del regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio
		Gestori aeroportuali quali definiti all'articolo 72, comma 1, lettera b), del decreto-legge 24 gennaio 2012, n. 1, convertito, con modificazioni, dalla legge 24 marzo 2012, n. 27, aeroporti quali definiti all'articolo 72, comma 1, lettera a), di tale decreto-legge, compresi gli aeroporti centrali di cui all'allegato II, punto 2, del regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio, e soggetti che gestiscono impianti annessi situati in aeroporti
		Operatori attivi nel controllo della gestione del traffico che forniscono servizi di controllo del traffico aereo quale definito all'articolo 2, primo paragrafo, numero 1), del regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio
	b) Trasporto ferroviario	Gestori dell'infrastruttura quali definiti all'articolo 3, comma 1, lettera b), del decreto legislativo 15 luglio 2015, n. 112
		Imprese ferroviarie quali definite all'articolo 3, comma 1, lettera a), del decreto legislativo 15 luglio 2015, n. 112, compresi gli operatori degli impianti di servizio quali definiti all'articolo 3, comma 1, lettera n), del decreto legislativo 15 luglio 2015, n. 112,
c) Trasporto per vie d'acqua		compagnie di navigazione per il trasporto per vie d'acqua interne, marittimo e costiero di passeggeri e merci quali definite nell'allegato I del regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio, escluse le singole navi gestite da tale compagnia
		organi di gestione dei porti quali definiti all'articolo 2, comma 1, lettera a), del decreto legislativo 6 novembre 2007, n. 203, compresi i relativi impianti portuali quali definiti all'articolo 2, primo paragrafo, numero 11), del regolamento (CE) n. 725/2004, e soggetti che gestiscono opere e attrezzature all'interno di porti
		Gestori di servizi di assistenza al traffico marittimo quali definiti all'articolo 2, comma 1, lettera p), del decreto legislativo 19 agosto 2005, n. 196
d) Trasporto su strada		Autorità stradali quali definite all'articolo 2, punto 12, del regolamento delegato (UE) 2015/962 della Commissione responsabili del controllo della gestione del traffico



		Gestori di sistemi di trasporto intelligenti quali definiti all'articolo 1, comma 1, lettera a), del decreto del Ministro delle infrastrutture e dei trasporti 1 febbraio 2013
3. Settore bancario		Enti creditizi quali definiti all'articolo 4, paragrafo 1, numero 1), del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio
4. Infrastrutture dei mercati finanziari		Gestori delle sedi di negoziazione quali definite all'articolo 1, comma 5- <i>octies</i> , lettera c), del decreto legislativo 24 febbraio 1998, n. 58
		Controparte centrale quale definita all'articolo 2, primo paragrafo, numero 1), del regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio
5. Settore sanitario	Istituti sanitari (compresi ospedali e cliniche private)	Prestatori di assistenza sanitaria quali definiti all'articolo 3, comma 1, lettera h), del decreto legislativo 4 marzo 2014, n. 38
6. Fornitura e distribuzione di acqua potabile		Fornitori e distributori di acque destinate al consumo umano, quali definite all'articolo 2, comma 1, lettera a), del decreto legislativo 2 febbraio 2001, n. 31, ma esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano è solo una parte della loro attività generale di distribuzione di altri prodotti e beni che non sono considerati servizi essenziali
7. Infrastrutture digitali		IXP DNS TLD



ALLEGATO III

(di cui all'art. 3, comma 1, lettera h)

TIPI DI SERVIZI DIGITALI

1. Mercato online
2. Motore di ricerca online
3. Servizi di cloud computing

NOTE

AVVERTENZA:

— Il testo delle note qui pubblicato è stato redatto dall'amministrazione competente per materia ai sensi dell'art. 10, comma 3 del testo unico delle disposizioni sulla promulgazione delle leggi, sull'emanazione dei decreti del Presidente della Repubblica e sulle pubblicazioni ufficiali della Repubblica italiana, approvato con decreto del Presidente della Repubblica 28 dicembre 1985, n. 1092, al solo fine di facilitare la lettura delle disposizioni di legge modificate o alle quali è operato il rinvio. Restano invariati il valore e l'efficacia degli atti legislativi qui trascritti.

— Per gli atti dell'Unione europea vengono forniti gli estremi di pubblicazione nella Gazzetta Ufficiale dell'Unione Europea (G.U.U.E.).

Note alle premesse:

— L'art. 76 della Costituzione stabilisce che l'esercizio della funzione legislativa non può essere delegato al Governo se non con determinazione di principi e criteri direttivi e soltanto per tempo limitato e per oggetti definiti.

— L'art. 87 della Costituzione conferisce, tra l'altro, al Presidente della Repubblica il potere di promulgare le leggi e di emanare i decreti aventi valore di legge ed i regolamenti.

— La legge 24 dicembre 2012, n. 234, recante: «Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea», è pubblicata nella Gazzetta Ufficiale 4 gennaio 2013, n. 3.

— La legge 25 ottobre 2017, n. 163, recante: «Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - legge di delegazione europea 2016-2017», è pubblicata nella Gazzetta Ufficiale 6 novembre 2017, n. 259.

— La direttiva (UE) 1148/2016 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, è pubblicata nella G.U.U.E. 19 luglio 2016, n. L 194.

— Il regolamento (CE) 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, è pubblicato nella G.U.C.E. 28 agosto 2014, n. L 257.

— La direttiva (UE) 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio, è pubblicata nella G.U.U.E. 14 agosto 2013, n. L 218.

— La raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese, è pubblicata nella G.U.C.E. 20 maggio 2003, n. L 124.

— Il regolamento di esecuzione (UE) 2018/151 della Commissione, del 30 gennaio 2018, recante modalità di applicazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, per quanto riguarda l'ulteriore specificazione degli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente, è pubblicato nella G.U.U.E. 31 gennaio 2018, n. L 26.

— Il decreto-legge 27 luglio 2005, n. 144, recante: «Misure urgenti per il contrasto del terrorismo internazionale», pubblicato nella Gazzetta Ufficiale 27 luglio 2005, n. 173, è convertito, con modificazioni,

dalla legge. 31 luglio 2005, n. 155, pubblicata nella Gazzetta Ufficiale 1° agosto 2005, n. 177.

— Il decreto legislativo 4 marzo 2014, n. 39, recante: «Attuazione della direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che sostituisce la decisione quadro 2004/68/GAI», è pubblicato nella Gazzetta Ufficiale 22 marzo 2014, n. 68.

— La legge 3 agosto 2007, n. 124, recante: «Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto», è pubblicata nella Gazzetta Ufficiale 13 agosto 2007, n. 187.

— Il decreto-legge 30 ottobre 2015, n. 174, recante: «Proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione», pubblicato nella Gazzetta Ufficiale 30 ottobre 2015, n. 253, è convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, pubblicata nella Gazzetta Ufficiale 16 dicembre 2015, n. 292.

— Il decreto-legge 22 giugno 2012, n. 83, recante: «Misure urgenti per la crescita del Paese», pubblicato nella Gazzetta Ufficiale 26 giugno 2012, n. 147, S.O., è convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, pubblicata nella Gazzetta Ufficiale 11 agosto 2012, n. 187, S.O.

— Il decreto legislativo 7 marzo 2005, n. 82, recante: «Codice dell'amministrazione digitale», è pubblicato nella Gazzetta Ufficiale 16 maggio 2005, n. 112, S.O.

— Il decreto legislativo 11 aprile 2011, n. 61, recante: «Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione», è pubblicato nella Gazzetta Ufficiale 4 maggio 2011, n. 102.

— Il decreto del Presidente del Consiglio dei ministri 6 novembre 2015, recante: «Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva», è pubblicato nella Gazzetta Ufficiale 5 dicembre 2015, n. 284, S.O.

— Il decreto del Presidente del Consiglio dei ministri 17 febbraio 2017: (Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali), è pubblicato nella Gazzetta Ufficiale 13 aprile 2017, n. 87.

— Il decreto legislativo 30 giugno 2003, n. 196, recante: «Codice in materia di protezione dei dati personali», è pubblicato nella Gazzetta Ufficiale 29 luglio 2003, n. 174, S.O.

— Il decreto legislativo 1° agosto 2003, n. 259, recante: «Codice delle comunicazioni elettroniche», è pubblicato nella Gazzetta Ufficiale 15 settembre 2003, n. 214, S.O.

— Il decreto legislativo 23 giugno 2011, n. 118, recante: «Disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli enti locali e dei loro organismi, a norma degli articoli 1 e 2 della legge 5 maggio 2009, n. 42», è pubblicato nella Gazzetta Ufficiale 26 luglio 2011, n. 172.

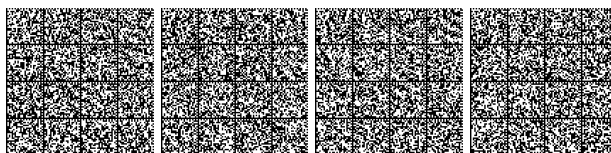
Note all'art. 1:

— Si riporta il testo degli articoli 16-bis e 16-ter del decreto legislativo 1° agosto 2003, n. 259, recante: «Codice delle comunicazioni elettroniche»:

«Art. 16-bis (Sicurezza e integrità). — 1. Fatte salve le competenze dell'Autorità previste dall'art. 1, comma 6, lettera a), numero 3), della legge 31 luglio 1997, n. 249, il Ministero, sentite le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico e tenuto conto delle misure tecniche di attuazione eventualmente adottate dalla Commissione europea, ai sensi dell'art. 13-bis, comma 4, della direttiva 2002/21/CE, individua:

a) adeguate misure di natura tecnica e organizzativa per assicurare la sicurezza delle reti e dei servizi di comunicazione elettronica accessibili al pubblico, nonché per garantire l'integrità delle reti. Tali misure sono anche finalizzate a prevenire e limitare le conseguenze per gli utenti e le reti interconnesse degli incidenti che pregiudicano la sicurezza;

b) i casi in cui le violazioni della sicurezza o perdita dell'integrità siano da considerarsi significative ai fini del corretto funzionamento delle reti o dei servizi.



2. Le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico:

a) adottano le misure individuate dal Ministero di cui al comma 1, lettera a), al fine di conseguire un livello di sicurezza delle reti adeguato al rischio esistente, e di garantire la continuità della fornitura dei servizi su tali reti;

b) comunicano al Ministero ogni significativa violazione della sicurezza o perdita dell'integrità secondo quanto previsto al comma 1, lettera b).

3. Nei casi di cui al comma 2, lettera b), il Ministero informa le altre autorità nazionali eventualmente interessate per le relative iniziative di competenza, e, se del caso, informa le autorità degli altri Stati membri nonché l'ENISA.

4. Il Ministero, anche su impulso dell'Autorità, può informare il pubblico o imporre all'impresa di farlo, ove accerti che la divulgazione della violazione di cui al comma 2, lettera b), sia nell'interesse pubblico. Anche a tal fine, presso il Ministero è individuato il Computer Emergency Response Team (CERT) nazionale, avvalendosi delle risorse umane, strumentali e finanziarie e disponibili, con compiti di assistenza tecnica in caso di segnalazioni da parte di utenti e di diffusione di informazioni anche riguardanti le contromisure adeguate per i tipi più comuni di incidente.

5. Il Ministero trasmette ogni anno alla Commissione europea e all'ENISA una relazione sintetica delle notifiche ricevute e delle azioni adottate conformemente al presente articolo.»

«Art. 16-ter (Attuazione e controllo). – 1. Le misure adottate ai fini dell'attuazione del presente articolo e dell'art. 16-bis sono approvate con decreto del Ministro dello sviluppo economico.

2. Ai fini del controllo del rispetto dell'art. 16-bis le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico sono tenute a:

a) fornire al Ministero, e se necessario all'Autorità, le informazioni necessarie per valutare la sicurezza e l'integrità dei loro servizi e delle loro reti, in particolare i documenti relativi alle politiche di sicurezza; nonché;

b) sottostare a una verifica della sicurezza effettuata dal Ministero, anche su impulso dell'Autorità, in collaborazione con gli Ispettorati territoriali del Ministero dello sviluppo economico, o da un organismo qualificato indipendente designato dal Ministero. L'impresa si assume l'onere finanziario della verifica.

3. Il Ministero e l'Autorità hanno la facoltà di indagare i casi di mancata conformità nonché i loro effetti sulla sicurezza e l'integrità delle reti.

4. Nel caso in cui il Ministero riscontri, anche su indicazione dell'Autorità, il mancato rispetto degli articoli 16-bis e 16-ter ovvero delle disposizioni attuative previste dal comma 1 da parte delle imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, si applicano le sanzioni di cui all'art. 98, commi da 4 a 12.»

— Per i riferimenti normativi del decreto legislativo 11 aprile 2011, n. 61, si veda nelle note alle premesse.

— Per i riferimenti normativi della direttiva 2013/40/UE, si veda nelle note alle premesse.

— La decisione quadro 2005/222/GAI del Consiglio, del 24 febbraio 2005, relativa agli attacchi contro i sistemi di informazione, è pubblicata nella G.U.U.E. 16 marzo 2005, n. L 69.

— Si riporta il testo dell'art. 346 del Trattato sul funzionamento dell'Unione europea (versione consolidata), pubblicato nella G.U.U.E. 26 ottobre 2012, n. C 326:

«Art. 346 (ex art. 296 del TCE). – 1. Le disposizioni dei trattati non ostano alle norme seguenti:

a) nessuno Stato membro è tenuto a fornire informazioni la cui divulgazione sia dallo stesso considerata contraria agli interessi essenziali della propria sicurezza;

b) ogni Stato membro può adottare le misure che ritenga necessarie alla tutela degli interessi essenziali della propria sicurezza e che si riferiscano alla produzione o al commercio di armi, munizioni e materiale bellico; tali misure non devono alterare le condizioni di concorrenza nel mercato interno per quanto riguarda i prodotti che non siano destinati a fini specificamente militari.

2. Il Consiglio, deliberando all'unanimità su proposta della Commissione, può apportare modificazioni all'elenco, stabilito il 15 aprile 1958, dei prodotti cui si applicano le disposizioni del paragrafo 1, lettera b).»

Note all'art. 2:

— Per i riferimenti normativi del decreto legislativo 30 giugno 2003, n. 196, si veda nelle note alle premesse.

Note all'art. 3:

— Si riporta il testo dell'art. 7-bis del decreto-legge 27 luglio 2005, n. 144, recante «Misure urgenti per il contrasto del terrorismo internazionale», pubblicato nella *Gazzetta Ufficiale* 27 luglio 2005, n. 173, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, pubblicata nella *Gazzetta Ufficiale* 1° agosto 2005, n. 177:

«Art. 7-bis (Sicurezza telematica). – 1. Ferme restando le competenze dei Servizi informativi e di sicurezza, di cui agli articoli 4 e 6 della legge 24 ottobre 1977, n. 801, l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione assicura i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'interno, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate.

2. Per le finalità di cui al comma 1 e per la prevenzione e repressione delle attività terroristiche o di agevolazione del terrorismo condotte con i mezzi informatici, gli ufficiali di polizia giudiziaria appartenenti all'organo di cui al comma 1 possono svolgere le attività di cui all'art. 4, commi 1 e 2, del decreto-legge 18 ottobre 2001, n. 374, convertito, con modificazioni, dalla legge 15 dicembre 2001, n. 438, e quelle di cui all'art. 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, anche a richiesta o in collaborazione con gli organi di polizia giudiziaria ivi indicati.»

— Si riporta il testo dell'art. 1, comma 1, lettera dd), del decreto legislativo 1° agosto 2003, n. 259, recante «Codice delle comunicazioni elettroniche»:

«Art. 1 (Definizioni). – 1. Ai fini del presente Codice si intende per: a) cc) (Omissis);

dd) reti di comunicazione elettronica: i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa Internet), le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

(Omissis)».

— La direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (codificazione), è pubblicata nella G.U.U.E. 17 settembre 2015, n. L 241.

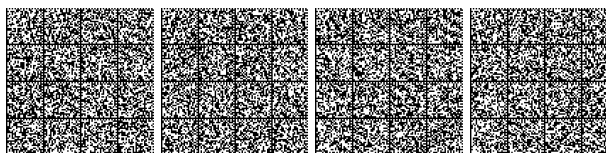
— Il regolamento (UE) 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio, nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio, è pubblicato nella G.U.U.E. 14 novembre 2012, n. L 316.

— Si riporta il testo dell'art. 141, comma 1, lettere a) e b), del decreto legislativo 6 settembre 2005, n. 206, recante il Codice di consumo:

«Art. 141. (Disposizioni generali: definizioni ed ambito di applicazione) – 1. Ai fini del presente titolo, si intende per:

a) «consumatore»: la persona fisica, di cui all'art. 3, comma 1, lettera a);

b) «professionista»: il soggetto, di cui all'art. 3, comma 1, lettera c); (Omissis)».



Note all'art. 7:

— Si riporta il testo dell'art. 3, comma 1, lettera *a*), del decreto legislativo 4 marzo 2014, n. 38, recante: «Attuazione della direttiva 2011/24/UE concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera, nonché della direttiva 2012/52/UE, comportante misure destinate ad agevolare il riconoscimento delle ricette mediche emesse in un altro stato membro»:

«Art. 3 (*Definizioni*). – 1. Ai fini del presente decreto, si applicano le seguenti definizioni:

a) «assistenza sanitaria»: i servizi prestati da professionisti sanitari a pazienti, al fine di valutare, mantenere o ristabilire il loro stato di salute, ivi compresa la prescrizione, la somministrazione e la fornitura di medicinali e dispositivi medici;

(*Omissis*)».

Note all'art. 8:

— Per il testo dell'art. 16-*bis* del citato decreto legislativo 1° agosto 2003, n. 259, si veda nelle note all'art. 1.

— Si riporta il testo dell'art. 51 del decreto legislativo 7 marzo 2005, n. 82, recante: «Codice dell'amministrazione digitale»:

«Art. 51 (*Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni*). – 1. Con le Linee guida sono individuate le soluzioni tecniche idonee a garantire la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati e la continuità operativa dei sistemi e delle infrastrutture.

1-*bis*. AgID attua, per quanto di competenza e in raccordo con le altre autorità competenti in materia, il Quadro strategico nazionale per la sicurezza dello spazio cibernetico e il Piano nazionale per la sicurezza cibernetica e la sicurezza informatica. AgID, in tale ambito:

a) coordina, tramite il Computer Emergency Response Team Pubblica Amministrazione (CERT-PA) istituito nel suo ambito, le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;

b) promuove intese con le analoghe strutture internazionali;

c) segnala al Ministro per la semplificazione e la pubblica amministrazione il mancato rispetto delle regole tecniche di cui al comma 1 da parte delle pubbliche amministrazioni.

2. I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.

2-*bis*. (abrogato).

2-*ter*. I soggetti di cui all'art. 2, comma 2, aderiscono ogni anno ai programmi di sicurezza preventiva coordinati e promossi da AgID secondo le procedure dettate dalla medesima AgID con le Linee guida.

2-*quater*. I soggetti di cui art. 2, comma 2, predispongono, nel rispetto delle Linee guida adottate dall'AgID, piani di emergenza in grado di assicurare la continuità operativa delle operazioni indispensabili per i servizi erogati e il ritorno alla normale operatività. Onde garantire quanto previsto, è possibile il ricorso all'art. 15 della legge 7 agosto 1990, n. 241, per l'erogazione di servizi applicativi, infrastrutturali e di dati, con ristoro dei soli costi di funzionamento. Per le Amministrazioni dello Stato coinvolte si provvede mediante rimodulazione degli stanziamenti dei pertinenti capitoli di spesa o mediante riassegnazione alla spesa degli importi versati a tale titolo ad apposito capitolo di entrata del bilancio statale.».

— Si riporta il testo dell'art. 7 del decreto legislativo 30 luglio 1999, n. 303, recante: «Ordinamento della Presidenza del Consiglio dei ministri, a norma dell'art. 11 della legge 15 marzo 1997, n. 59»:

«Art. 7 (*Autonomia organizzativa*). – 1. Per lo svolgimento delle funzioni istituzionali di cui all'art. 2, e per i compiti di organizzazione e gestione delle occorrenti risorse umane e strumentali, il Presidente individua con propri decreti le aree funzionali omogenee da affidare alle strutture in cui si articola il Segretariato generale.

2. Con propri decreti, il Presidente determina le strutture della cui attività si avvalgono i Ministri o Sottosegretari da lui delegati.

3. I decreti di cui ai commi 1 e 2 indicano il numero massimo degli uffici in cui si articola ogni Dipartimento e dei servizi in cui si articola ciascun ufficio. Alla organizzazione interna delle strutture medesime provvedono, nell'ambito delle rispettive competenze, il Segretario generale ovvero il Ministro o Sottosegretario delegato.

4. Per lo svolgimento di particolari compiti per il raggiungimento di risultati determinati o per la realizzazione di specifici programmi, il

Presidente istituisce, con proprio decreto, apposite strutture di missione, la cui durata temporanea, comunque non superiore a quella del Governo che le ha istituite, è specificata dall'atto istitutivo. Entro trenta giorni dalla data di entrata in vigore della presente disposizione, il Presidente può ridefinire le finalità delle strutture di missione già operanti: in tale caso si applica l'art. 18, comma 3, della legge 23 agosto 1988, n. 400, e successive modificazioni. Sentiti il Comitato nazionale per la bioetica e gli altri organi collegiali che operano presso la Presidenza, il Presidente, con propri decreti, ne disciplina le strutture di supporto.

4-*bis*. Per le attribuzioni che implicano l'azione unitaria di più dipartimenti o uffici a questi equiparabili, il Presidente può istituire con proprio decreto apposite unità di coordinamento interdipartimentale, il cui responsabile è nominato ai sensi dell'art. 18, comma 3, della legge 23 agosto 1988, n. 400. Dall'attuazione del presente comma non devono in ogni caso derivare nuovi o maggiori oneri per il bilancio dello Stato.

5. Il Segretario generale è responsabile del funzionamento del Segretariato generale e della gestione delle risorse umane e strumentali della Presidenza. Il Segretario generale può essere coadiuvato da uno o più Vicesegretari generali. Per le strutture affidate a Ministri o Sottosegretari, le responsabilità di gestione competono ai funzionari preposti alle strutture medesime, ovvero, nelle more della preposizione, a dirigenti temporaneamente delegati dal Segretario generale, su indicazione del Ministro o Sottosegretario competente.

6. Le disposizioni che disciplinano i poteri e le responsabilità dirigenziali nelle pubbliche amministrazioni, con particolare riferimento alla valutazione dei risultati, si applicano alla Presidenza nei limiti e con le modalità da definirsi con decreto del Presidente, sentite le organizzazioni sindacali, tenuto conto della peculiarità dei compiti della Presidenza. Il Segretario generale e, per le strutture ad essi affidate, i Ministri o Sottosegretari delegati, indicano i parametri organizzativi e funzionali, nonché gli obiettivi di gestione e di risultato cui sono tenuti i dirigenti generali preposti alle strutture individuate dal Presidente.

7. Il Presidente, con propri decreti, individua gli uffici di diretta collaborazione propri e, sulla base delle relative proposte, quelli dei Ministri senza portafoglio o sottosegretari della Presidenza, e ne determina la composizione.

8. La razionalità dell'ordinamento e dell'organizzazione della Presidenza è sottoposta a periodica verifica triennale, anche mediante ricorso a strutture specializzate pubbliche o private. Il Presidente informa le Camere dei risultati della verifica. In sede di prima applicazione del presente decreto, la verifica è effettuata dopo due anni.».

— Si riporta il testo dell'art. 17, comma 14, della legge 15 maggio 1997, n. 127, recante: «Misure urgenti per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e di controllo»:

«Art. 17 (*Ulteriori disposizioni in materia di semplificazione dell'attività amministrativa e di snellimento dei procedimenti di decisione e di controllo*). – 1-13 (*Omissis*).

14. Nel caso in cui disposizioni di legge o regolamentari dispongano l'utilizzazione presso le amministrazioni pubbliche di un contingente di personale in posizione di fuori ruolo o di comando, le amministrazioni di appartenenza sono tenute ad adottare il provvedimento di fuori ruolo o di comando entro quindici giorni dalla richiesta.

(*Omissis*)».

Note all'art. 14:

— Per i riferimenti normativi della raccomandazione 2003/361/CE della Commissione, si veda nelle note alle premesse.

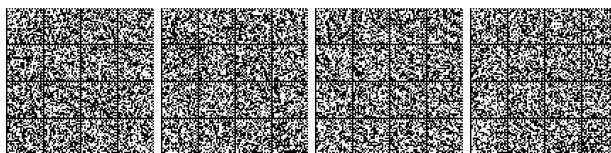
Note all'art. 20:

— La legge 24 novembre 1981, n. 689, recante: «Modifiche al sistema penale», è pubblicata nella *Gazzetta Ufficiale* 30 novembre 1981, n. 329, S.O.

Note all'art. 22:

— Si riporta il testo dell'art. 41-*bis* della legge 24 dicembre 2012, n. 234, recante: «Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea»:

«Art. 41-*bis* (*Fondo per il recepimento della normativa europea*). – 1. Al fine di consentire il tempestivo adeguamento dell'ordinamento interno agli obblighi imposti dalla normativa europea, nei soli limiti oc-



correnti per l'adempimento degli obblighi medesimi e in quanto non sia possibile farvi fronte con i fondi già assegnati alle competenti amministrazioni, è autorizzata la spesa di 10 milioni di euro per l'anno 2015 e di 50 milioni di euro annui a decorrere dall'anno 2016.

2. Per le finalità di cui al comma 1 è istituito nello stato di previsione del Ministero dell'economia e delle finanze un fondo, con una dotazione di 10 milioni di euro per l'anno 2015 e di 50 milioni di euro annui a decorrere dall'anno 2016, destinato alle sole spese derivanti dagli adempimenti di cui al medesimo comma 1.

3. All'onere derivante dall'attuazione del presente articolo, pari a 10 milioni di euro per l'anno 2015 e a 50 milioni di euro annui a decorrere dall'anno 2016, si provvede, quanto a 10 milioni di euro per l'anno 2015, mediante versamento all'entrata del bilancio dello Stato, per un

corrispondente importo, delle somme del fondo di cui all'art. 5, comma 1, della legge 16 aprile 1987, n. 183, e, quanto a 50 milioni di euro annui a decorrere dall'anno 2016, mediante corrispondente riduzione delle proiezioni dello stanziamento del fondo speciale di parte corrente iscritto, ai fini del bilancio triennale 2015-2017, nell'ambito del programma "Fondi di riserva e speciali" della missione "Fondi da ripartire" dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2015, allo scopo parzialmente utilizzando l'accantonamento relativo al medesimo Ministero.

4. Il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.»

18G00092

DECRETI PRESIDENZIALI

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 aprile 2018.

Autorizzazione al Ministero dell'interno, ex Agenzia autonoma per la gestione dell'albo dei segretari comunali e provinciali (AGES), ad avviare procedure concorsuali relative al corso-concorso COA6 e a procedere alle relative assunzioni per n. 224 unità di segretari comunali e provinciali.

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Visto il decreto legislativo 30 marzo 2001, n. 165, nonché il decreto legislativo 25 maggio 2017, n. 75;

Visto l'art. 3, comma 3 del decreto-legge 24 giugno 2014, n. 90, convertito, con modificazioni, dalla legge 11 agosto 2014, n. 114, secondo cui le assunzioni a tempo indeterminato delle amministrazioni dello Stato, anche ad ordinamento autonomo, delle agenzie e degli enti pubblici non economici ivi compresi quelli di cui all'art. 70, comma 4 del decreto legislativo 30 marzo 2001, n. 165, di cui ai commi 1 e 2, sono autorizzate con il decreto e le procedure di cui all'art. 35, comma 4 del decreto legislativo 30 marzo 2001, n. 165, previa richiesta delle amministrazioni interessate, predisposta sulla base della programmazione del fabbisogno, corredata da analitica dimostrazione delle cessazioni avvenute nell'anno precedente e delle conseguenti economie e dall'individuazione delle unità da assumere e dei correlati oneri. A decorrere dall'anno 2014 è consentito il cumulo delle risorse destinate alle assunzioni per un arco temporale non superiore a tre anni, nel rispetto della programmazione del fabbisogno e di quella finanziaria e contabile;

Visto l'art. 14, comma 6 del decreto-legge 6 luglio 2012, n. 95, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 135, il quale dispone che, a decorrere dal 2012, le assunzioni dei segretari comunali e provinciali sono autorizzate con le modalità di cui all'art. 66, comma 10 del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, per un numero di unità non superiore all'80 per

cento di quelle cessate dal servizio nel corso dell'anno precedente;

Visto l'art. 66, comma 10 del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge del 6 agosto 2008, n. 133, e successive modificazioni e integrazioni, il quale dispone, tra l'altro, che le assunzioni delle amministrazioni dello Stato, anche ad ordinamento autonomo, sono autorizzate secondo le modalità di cui all'art. 35, comma 4 del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni;

Visto il predetto decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni e integrazioni, e in particolare l'art. 35, comma 4, secondo cui con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, sono autorizzati l'avvio delle procedure concorsuali e le relative assunzioni del personale delle amministrazioni dello Stato, anche ad ordinamento autonomo, delle agenzie e degli enti pubblici non economici;

Visto l'art. 97 del decreto legislativo 18 agosto 2000, n. 267, che stabilisce l'obbligatorietà, per ogni comune ed ogni provincia, di avere un segretario titolare dipendente dall'Agenzia autonoma per la gestione dell'albo dei segretari comunali e provinciali, iscritto all'apposito albo previsto dal successivo art. 98 dello stesso decreto;

Visto il decreto del Presidente della Repubblica del 4 dicembre 1997, n. 465, regolamento recante disposizioni in materia di ordinamento dei segretari comunali e provinciali, a norma dell'art. 17, comma 78, della legge 15 maggio 1997, n. 127, ed in particolare l'art. 13, comma 6, che dispone che al corso è ammesso un numero di candidati pari a quello predeterminato ai sensi del comma 3 del medesimo articolo, maggiorato di una percentuale del 30%;

Visto l'art. 7, comma 31-ter del decreto-legge 31 maggio 2010, n. 78, convertito, con modificazioni dalla legge 30 luglio 2010, n. 122, che, nel sopprimere l'Agenzia autonoma per la gestione dell'albo dei segretari comunali e provinciali, istituita dall'art. 102 del decreto legislativo 18 agosto 2000, n. 267, stabilisce che il Ministero dell'in-

