

DECRETO LEGISLATIVO 1° ottobre 2026, n. 191.

Norme di adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2025/37 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti.

IL PRESIDENTE DELLA REPUBBLICA

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

Vista la legge 23 agosto 1988, n. 400, recante «Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri» e, in particolare, l'articolo 14;

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» e, in particolare, gli articoli 31 e 32;

Vista la legge 17 marzo 2026, n. 36, recante «Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2025» e, in particolare, l'articolo 16;

Visto il regolamento (UE) 2025/37 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti;

Visto il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013;

Visto il decreto legislativo 7 marzo 2005, n. 82, recante «Codice dell'amministrazione digitale»;

Visto il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale»;

Visto il decreto legislativo 3 agosto 2022, n. 123, recante «Norme di adeguamento della normativa nazionale alle disposizioni del Titolo III «Quadro di certificazione della cybersicurezza» del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»);

Vista la legge 28 giugno 2024, n. 90, recante «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici»;

Visto il decreto legislativo 4 settembre 2024, n. 138, recante «Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che Abroga la direttiva (UE) 2016/1148»;

Sentita l'Agenzia per la cybersicurezza nazionale;

Vista la preliminare deliberazione del Consiglio dei ministri, adottata nella riunione del 2 luglio 2026;

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 settembre 2026;

Sulla proposta del Presidente del Consiglio dei ministri e del Ministro per gli affari europei, il PNRR e le politiche di coesione, di concerto con i Ministri degli affari esteri e della cooperazione internazionale, della giustizia, dell'economia e delle finanze, delle imprese e del made in Italy, dell'interno e della difesa;

EMANA

il seguente decreto legislativo:

Art. 1.

Modifiche al decreto legislativo 3 agosto 2022, n. 123

1. Al decreto legislativo 3 agosto 2022, n. 123, sono apportate le seguenti modificazioni:

a) all'articolo 3, comma 1:

1) dopo la lettera a) è inserita la seguente:

«a-bis) “servizio di sicurezza gestito”: un servizio prestato a un terzo consistente nello svolgimento di attività o nella fornitura di assistenza per tali attività, legate alla gestione dei rischi in materia di cybersicurezza, ad esempio servizi di gestione degli incidenti, test di penetrazione, audit di sicurezza e consulenza, tra cui consulenza specialistica, relativa all'assistenza tecnica»;

2) alla lettera d), le parole: «prodotto TIC o di un servizio TIC» sono sostituite dalle seguenti: «prodotto TIC, di un servizio TIC o di un servizio di sicurezza gestito»;

3) alla lettera f), le parole: «prodotto TIC o servizio TIC» sono sostituite dalle seguenti: «prodotto TIC, di un servizio TIC o di un servizio di sicurezza gestito»;

4) alla lettera g), dopo le parole: «ad essi collegati» sono inserite le seguenti: «nonché i servizi di sicurezza gestiti»;

5) alla lettera u), le parole: «prodotti TIC o fornitore di servizi TIC» sono sostituite dalle seguenti: «prodotti TIC, un fornitore di servizi TIC o un fornitore di servizi di sicurezza gestiti»;

6) alla lettera z), le parole: «servizio TIC o processo TIC» sono sostituite dalle seguenti: «servizio TIC, processo TIC o servizio di sicurezza gestito»;

b) all'articolo 5:

1) al comma 4, lettera b), le parole: «servizio TIC o processo TIC che ha comportato un concreto e dimostrato pregiudizio ad un servizio essenziale ai sensi dell'allegato II del decreto legislativo 18 maggio 2018, n. 65, o a un servizio di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera fff), del decreto legislativo 1° agosto 2003, n. 259,» sono sostituite dalle seguenti: «servizio TIC, processo TIC o servizio di sicurezza gestito che ha



comportato un concreto e dimostrato pregiudizio a un soggetto essenziale di cui all'articolo 6, commi 1 e 2, del decreto legislativo 4 settembre 2024, n. 138»;

2) al comma 5, secondo periodo, dopo le parole: «revoca del certificato» sono inserite le seguenti: «, dandone contestuale notifica all'Agenzia»;

3) al comma 6, primo periodo, dopo la parola: «entro» sono inserite le seguenti: «i termini stabiliti dall'Agenzia e comunque non oltre»;

4) al comma 9, le parole: «commi 3, 8 e 9» sono sostituite dalle seguenti: «commi 3 e 8»;

c) all'articolo 6, comma 1, dopo le parole: «affidabilità elevato» sono inserite le seguenti: «, sostanziale e di base» e le parole: «vigilanza nazionale» sono sostituite dalla seguente: «certificazione»;

d) all'articolo 7:

1) al comma 1, le parole: «servizi TIC o processi TIC» sono sostituite dalle seguenti: «servizi TIC, processi TIC o servizi di sicurezza gestiti»;

2) al comma 2, il primo periodo è sostituito dal seguente: «Il fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti rende disponibile all'Agenzia, per il periodo stabilito nel corrispondente sistema europeo di certificazione della cybersicurezza ai sensi dell'articolo 54, paragrafo 1, lettera q), del Regolamento, la dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti relative alla conformità dei prodotti TIC, servizi TIC o servizi di sicurezza gestiti al sistema.»;

e) all'articolo 9, comma 3, le parole: «servizi TIC o processi TIC» sono sostituite dalle seguenti: «servizi TIC, processi TIC o servizi di sicurezza gestiti»;

f) all'articolo 10:

1) al comma 1, secondo periodo, le parole: «, in quanto compatibile, la disciplina della legge 24 novembre 1981, n. 689» sono sostituite dalle seguenti: «l'articolo 17, comma 4-*quater*, del decreto-legge n. 82 del 2021»;

2) al comma 4, primo periodo, le parole: «o servizio TIC» sono sostituite dalle seguenti: «, un servizio TIC o un servizio di sicurezza gestito»;

3) al comma 5, le parole: «o di un servizio TIC» sono sostituite dalle seguenti: «, di un servizio TIC o di un servizio di sicurezza gestito»;

4) al comma 8:

4.1) al primo periodo, le parole: «servizi TIC o processi TIC» sono sostituite dalle seguenti: «servizi TIC, processi TIC o servizi di sicurezza gestiti»;

4.2) al secondo periodo, le parole: «servizio TIC o processo TIC» sono sostituite dalle seguenti: «servizio TIC, processo TIC o servizio di sicurezza gestito»;

5) al comma 16, le parole: «servizio TIC o ad un processo TIC» sono sostituite dalle seguenti: «servizio TIC, ad un processo TIC o a un servizio di sicurezza gestito» e le parole: «essenziale ai sensi dell'allegato II del decreto legislativo 18 maggio 2018, n. 65, o di un servizio di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera fff), del decreto legislativo 1° agosto

2003, n. 259» sono sostituite dalle seguenti: «erogato da un soggetto essenziale di cui all'articolo 6, commi 1 e 2, del decreto legislativo 4 settembre 2024, n. 138»;

g) all'articolo 13:

1) al comma 1, le parole: «per incrementare la dotazione degli appositi capitoli dell'Agenzia» sono sostituite dalle seguenti: «di cui all'articolo 18 del decreto-legge n. 82 del 2021»;

2) al comma 3, le parole: «per incrementare la dotazione dei capitoli del bilancio dell'Agenzia» sono sostituite dalle seguenti: «di cui all'articolo 18 del decreto-legge n. 82 del 2021, e» e le parole: «servizi TIC e processi TIC» sono sostituite dalle seguenti: «servizi TIC, processi TIC e servizi di sicurezza gestiti».

Art. 2.

Modifiche all'articolo 35 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82

1. All'articolo 35 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, sono apportate le seguenti modificazioni:

a) al comma 4, le parole: «dello schema nazionale di cui al comma 5» sono sostituite dalle seguenti: «dell'articolo 30 del regolamento eIDAS»;

b) al comma 5:

1) al primo periodo, le parole da: «in base allo schema nazionale» fino a: «delle attività produttive e dell'economia e delle finanze» sono sostituite dalle seguenti: «(OCSI)»;

2) il secondo e il terzo periodo sono soppressi.

Art. 3.

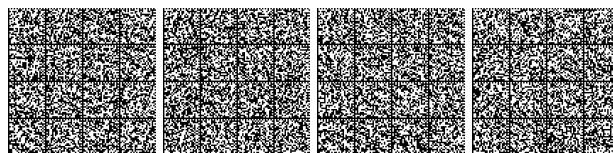
Modifiche all'articolo 7 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109

1. All'articolo 7, comma 1, lettera e), del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, sono apportate le seguenti modificazioni:

a) il numero 1) è sostituito dal seguente:

«1) autorizza, ai sensi dell'articolo 60, paragrafo 3, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi europei di certificazione della cybersicurezza che stabiliscono requisiti specifici o supplementari a norma dell'articolo 54, paragrafo 1, lettera f), del citato regolamento (UE) 2019/881»;

b) al numero 2), le parole: «di cui al numero 1) della presente lettera» sono sostituite dalle seguenti: «ai sensi dell'articolo 60, paragrafo 1, del citato regolamento (UE) 2019/881».



Art. 4.

Clausola di invarianza finanziaria

1. Le amministrazioni interessate provvedono all'attuazione del presente decreto con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.

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 1° ottobre 2026

MATTARELLA

MELONI, *Presidente del Consiglio dei ministri*

FOTI, *Ministro per gli affari europei, il PNRR e le politiche di coesione*

TAJANI, *Ministro degli affari esteri e della cooperazione internazionale*

NORDIO, *Ministro della giustizia*

GIORGETTI, *Ministro dell'economia e delle finanze*

URSO, *Ministro delle imprese e del made in Italy*

PIANTEDOSI, *Ministro dell'interno*

CROSETTO, *Ministro della difesa*

Visto, il Guardasigilli: NORDIO

N O T E

AVVERTENZA:

— Il testo delle note qui pubblicato è stato redatto dall'amministrazione competente per materia, ai sensi dell'art. 10, commi 2 e 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 D.P.R. 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 (GUUE).

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, quinto comma, della Costituzione conferisce al Presidente della Repubblica il potere di promulgare le leggi ed emanare i decreti aventi valore di legge e i regolamenti.

— Si riporta il testo dell'articolo 14 della legge 23 agosto 1988, n. 400, recante: «Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei ministri», pubblicata nella *Gazzetta Ufficiale* n. 214 del 12 settembre 1988:

«Art. 14 (*Decreti legislativi*). — 1. I decreti legislativi adottati dal Governo ai sensi dell'articolo 76 della Costituzione sono emanati dal Presidente della Repubblica con la denominazione di "decreto legislativo" e con l'indicazione, nel preambolo, della legge di delegazione, della deliberazione del Consiglio dei ministri e degli altri adempimenti del procedimento prescritti dalla legge di delegazione.

2. L'emanazione del decreto legislativo deve avvenire entro il termine fissato dalla legge di delegazione; il testo del decreto legislativo adottato dal Governo è trasmesso al Presidente della Repubblica, per la emanazione, almeno venti giorni prima della scadenza.

3. Se la delega legislativa si riferisce ad una pluralità di oggetti distinti suscettibili di separata disciplina, il Governo può esercitarla mediante più atti successivi per uno o più degli oggetti predetti. In relazione al termine finale stabilito dalla legge di delegazione, il Governo informa periodicamente le Camere sui criteri che segue nell'organizzazione dell'esercizio della delega.

4. In ogni caso, qualora il termine previsto per l'esercizio della delega ecceda in due anni, il Governo è tenuto a richiedere il parere delle Camere sugli schemi dei decreti delegati. Il parere è espresso dalle Commissioni permanenti delle due Camere competenti per materia entro sessanta giorni, indicando specificamente le eventuali disposizioni non ritenute corrispondenti alle direttive della legge di delegazione. Il Governo, nei trenta giorni successivi, esaminato il parere, ritrasmette, con le sue osservazioni e con eventuali modificazioni, i testi alle Commissioni per il parere definitivo che deve essere espresso entro trenta giorni.»

— Si riporta il testo degli articoli 31 e 32 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», pubblicata nella *Gazzetta Ufficiale* n. 3 del 4 gennaio 2013:

«Art. 31 (*Procedure per l'esercizio delle deleghe legislative conferite al Governo con la legge di delegazione europea*). — 1. In relazione alle deleghe legislative conferite con la legge di delegazione europea per il recepimento delle direttive, il Governo adotta i decreti legislativi entro il termine di quattro mesi antecedenti a quello di recepimento indicato in ciascuna delle direttive; per le direttive il cui termine così determinato sia già scaduto alla data di entrata in vigore della legge di delegazione europea, ovvero scada nei tre mesi successivi, il Governo adotta i decreti legislativi di recepimento entro tre mesi dalla data di entrata in vigore della medesima legge; per le direttive che non prevedono un termine di recepimento, il Governo adotta i relativi decreti legislativi entro dodici mesi dalla data di entrata in vigore della legge di delegazione europea.

2. I decreti legislativi sono adottati, nel rispetto dell'articolo 14 della legge 23 agosto 1988, n. 400, su proposta del Presidente del Consiglio dei ministri o del Ministro per gli affari europei e del Ministro con competenza prevalente nella materia, di concerto con i Ministri degli affari esteri, della giustizia, dell'economia e delle finanze e con gli altri Ministri interessati in relazione all'oggetto della direttiva. I decreti legislativi sono accompagnati da una tabella di concordanza tra le disposizioni in essi previste e quelle della direttiva da recepire, predisposta dall'amministrazione con competenza istituzionale prevalente nella materia.

3. La legge di delegazione europea indica le direttive in relazione alle quali sugli schemi dei decreti legislativi di recepimento è acquisito il parere delle competenti Commissioni parlamentari della Camera dei deputati e del Senato della Repubblica. In tal caso gli schemi dei decreti legislativi sono trasmessi, dopo l'acquisizione degli altri pareri previsti dalla legge, alla Camera dei deputati e al Senato della Repubblica affinché su di essi sia espresso il parere delle competenti Commissioni parlamentari. Decorsi quaranta giorni dalla data di trasmissione, i decreti sono emanati anche in mancanza del parere. Qualora il termine per l'espressione del parere parlamentare di cui al presente comma ovvero i diversi termini previsti dai commi 4 e 9 scadano nei trenta giorni che precedono la scadenza dei termini di delega previsti ai commi 1 o 5 o successivamente, questi ultimi sono prorogati di tre mesi.

4. Gli schemi dei decreti legislativi recanti recepimento delle direttive che comportino conseguenze finanziarie sono corredati della relazione tecnica di cui all'articolo 17, comma 3, della legge 31 dicembre 2009, n. 196. Su di essi è richiesto anche il parere delle Com-



missioni parlamentari competenti per i profili finanziari. Il Governo, ove non intenda conformarsi alle condizioni formulate con riferimento all'esigenza di garantire il rispetto dell'articolo 81, quarto comma, della Costituzione, ritrasmette alle Camere i testi, corredati dei necessari elementi integrativi d'informazione, per i pareri definitivi delle Commissioni parlamentari competenti per i profili finanziari, che devono essere espressi entro venti giorni.

5. Entro ventiquattro mesi dalla data di entrata in vigore di ciascuno dei decreti legislativi di cui al comma 1, nel rispetto dei principi e criteri direttivi fissati dalla legge di delegazione europea, il Governo può adottare, con la procedura indicata nei commi 2, 3 e 4, disposizioni integrative e correttive dei decreti legislativi emanati ai sensi del citato comma 1, fatto salvo il diverso termine previsto dal comma 6.

6. Con la procedura di cui ai commi 2, 3 e 4 il Governo può adottare disposizioni integrative e correttive di decreti legislativi emanati ai sensi del comma 1, al fine di recepire atti delegati dell'Unione europea di cui all'articolo 290 del Trattato sul funzionamento dell'Unione europea, che modificano o integrano direttive recepite con tali decreti legislativi. Le disposizioni integrative e correttive di cui al primo periodo sono adottate nel termine di cui al comma 5 o nel diverso termine fissato dalla legge di delegazione europea. Resta ferma la disciplina di cui all'articolo 36 per il recepimento degli atti delegati dell'Unione europea che recano meri adeguamenti tecnici.

7. I decreti legislativi di recepimento delle direttive previste dalla legge di delegazione europea, adottati, ai sensi dell'articolo 117, quinto comma, della Costituzione, nelle materie di competenza legislativa delle regioni e delle province autonome, si applicano alle condizioni e secondo le procedure di cui all'articolo 41, comma 1.

8. I decreti legislativi adottati ai sensi dell'articolo 33 e attinenti a materie di competenza legislativa delle regioni e delle province autonome sono emanati alle condizioni e secondo le procedure di cui all'articolo 41, comma 1.

9. Il Governo, quando non intende conformarsi ai pareri parlamentari di cui al comma 3, relativi a sanzioni penali contenute negli schemi di decreti legislativi recanti attuazione delle direttive, ritrasmette i testi, con le sue osservazioni e con eventuali modificazioni, alla Camera dei deputati e al Senato della Repubblica. Decorso venti giorni dalla data di ritrasmissione, i decreti sono emanati anche in mancanza di nuovo parere».

«Art. 32 (*Principi e criteri direttivi generali di delega per l'attuazione del diritto dell'Unione europea*). — 1. Salvi gli specifici principi e criteri direttivi stabiliti dalla legge di delegazione europea e in aggiunta a quelli contenuti nelle direttive da attuare, i decreti legislativi di cui all'articolo 31 sono informati ai seguenti principi e criteri direttivi generali:

a) le amministrazioni direttamente interessate provvedono all'attuazione dei decreti legislativi con le ordinarie strutture amministrative, secondo il principio della massima semplificazione dei procedimenti e delle modalità di organizzazione e di esercizio delle funzioni e dei servizi;

b) ai fini di un migliore coordinamento con le discipline vigenti per i singoli settori interessati dalla normativa da attuare, sono introdotte le occorrenti modificazioni alle discipline stesse, anche attraverso il riassetto e la semplificazione normativa con l'indicazione esplicita delle norme abrogate, fatti salvi i procedimenti oggetto di semplificazione amministrativa ovvero le materie oggetto di delegificazione;

c) gli atti di recepimento di direttive dell'Unione europea non possono prevedere l'introduzione o il mantenimento di livelli di regolazione superiori a quelli minimi richiesti dalle direttive stesse, ai sensi dell'articolo 14, commi 24-bis, 24-ter e 24-quater, della legge 28 novembre 2005, n. 246;

d) al di fuori dei casi previsti dalle norme penali vigenti, ove necessario per assicurare l'osservanza delle disposizioni contenute nei decreti legislativi, sono previste sanzioni amministrative e penali per le infrazioni alle disposizioni dei decreti stessi. Le sanzioni penali, nei limiti, rispettivamente, dell'ammenda fino a 150.000 euro e dell'arresto fino a tre anni, sono previste, in via alternativa o congiunta, solo nei casi in cui le infrazioni ledano o esponano a pericolo interessi costituzionalmente protetti. In tali casi sono previste: la pena dell'ammenda alternativa all'arresto per le infrazioni che esponano a pericolo o danneggino l'interesse protetto; la pena dell'arresto congiunta a quella dell'ammenda per le infrazioni che rechino un danno di particolare gravità. Nelle predette ipotesi, in luogo dell'arresto e dell'ammenda, possono essere previste anche le sanzioni alternative di cui agli articoli 53 e seguenti del decreto legislativo 28 agosto 2000, n. 274, e la relativa competenza

del giudice di pace. La sanzione amministrativa del pagamento di una somma non inferiore a 150 euro e non superiore a 150.000 euro è prevista per le infrazioni che ledono o esponano a pericolo interessi diversi da quelli indicati dalla presente lettera. Nell'ambito dei limiti minimi e massimi previsti, le sanzioni indicate dalla presente lettera sono determinate nella loro entità, tenendo conto della diversa potenzialità lesiva dell'interesse protetto che ciascuna infrazione presenta in astratto, di specifiche qualità personali del colpevole, comprese quelle che impongono particolari doveri di prevenzione, controllo o vigilanza, nonché del vantaggio patrimoniale che l'infrazione può recare al colpevole ovvero alla persona o all'ente nel cui interesse egli agisce. Ove necessario per assicurare l'osservanza delle disposizioni contenute nei decreti legislativi, sono previste inoltre le sanzioni amministrative accessorie della sospensione fino a sei mesi e, nei casi più gravi, della privazione definitiva di facoltà e diritti derivanti da provvedimenti dell'amministrazione, nonché sanzioni penali accessorie nei limiti stabiliti dal codice penale. Al medesimo fine è prevista la confisca obbligatoria delle cose che servirono o furono destinate a commettere l'illecito amministrativo o il reato previsti dai medesimi decreti legislativi, nel rispetto dei limiti stabiliti dall'articolo 240, terzo e quarto comma, del codice penale e dall'articolo 20 della legge 24 novembre 1981, n. 689, e successive modificazioni. Entro i limiti di pena indicati nella presente lettera sono previste sanzioni anche accessorie identiche a quelle eventualmente già comminate dalle leggi vigenti per violazioni omogenee e di pari offensività rispetto alle infrazioni alle disposizioni dei decreti legislativi. Nelle materie di cui all'articolo 117, quarto comma, della Costituzione, le sanzioni amministrative sono determinate dalle regioni;

e) al recepimento di direttive o all'attuazione di altri atti dell'Unione europea che modificano precedenti direttive o atti già attuati con legge o con decreto legislativo si procede, se la modificazione non comporta ampliamento della materia regolata, apportando le corrispondenti modificazioni alla legge o al decreto legislativo di attuazione della direttiva o di altro atto modificato;

f) nella redazione dei decreti legislativi di cui all'articolo 31 si tiene conto delle eventuali modificazioni delle direttive dell'Unione europea comunque intervenute fino al momento dell'esercizio della delega;

g) quando si verificano sovrapposizioni di competenze tra amministrazioni diverse o comunque siano coinvolte le competenze di più amministrazioni statali, i decreti legislativi individuano, attraverso le più opportune forme di coordinamento, rispettando i principi di sussidiarietà, differenziazione, adeguatezza e leale collaborazione e le competenze delle regioni e degli altri enti territoriali, le procedure per salvaguardare l'unitarietà dei processi decisionali, la trasparenza, la celerità, l'efficacia e l'economicità nell'azione amministrativa e la chiara individuazione dei soggetti responsabili;

h) qualora non siano di ostacolo i diversi termini di recepimento, vengono attuate con un unico decreto legislativo le direttive che riguardano le stesse materie o che comunque comportano modifiche degli stessi atti normativi;

i) è assicurata la parità di trattamento dei cittadini italiani rispetto ai cittadini degli altri Stati membri dell'Unione europea e non può essere previsto in ogni caso un trattamento sfavorevole dei cittadini italiani.»

— Si riporta il testo dell'articolo 16 della legge 17 marzo 2026, n. 36, recante «Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2025», pubblicata nella *Gazzetta Ufficiale* n. 70 del 25 marzo 2026:

«Art. 16 (*Delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2025/37 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti*). — 1. Il Governo è delegato ad adottare, entro tre mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi per adeguare la normativa nazionale alle disposizioni del regolamento (UE) 2025/37 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, e per coordinare le discipline di settore vigenti con il quadro normativo europeo in materia.

2. Nell'esercizio della delega di cui al comma 1, il Governo osserva, oltre ai principi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, i seguenti principi e criteri direttivi specifici:

a) apportare alla normativa vigente e, in particolare, al decreto legislativo 3 agosto 2022, n. 123, tutte le modifiche e le integrazioni ne-



cessarie ad assicurare la corretta e integrale applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, anche con riguardo alle modifiche apportate dal regolamento (UE) 2025/37, e delle pertinenti norme tecniche di regolamentazione e di attuazione, nonché a garantire il coordinamento con le disposizioni settoriali vigenti;

b) apportare al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, le modifiche e le integrazioni necessarie a specificare le modalità di esercizio delle funzioni attribuite all'Agenzia per la cybersicurezza nazionale in materia di accreditamento, autorizzazione e delega degli organismi di cui all'articolo 7, comma 1, lettera e), numeri 1) e 2), del medesimo decreto-legge n. 82 del 2021, in conformità alle pertinenti disposizioni del regolamento (UE) 2019/881.

3. Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni interessate provvedono all'adempimento dei compiti derivanti dall'esercizio della delega di cui al presente articolo con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.»

— Il regolamento (UE) 2025/37 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti è pubblicato nella GUUE 15 gennaio 2025, Serie L.

— Il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 è pubblicato nella GUUE 7 giugno 2019, n. L 151.

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

— Il decreto-legge 14 giugno 2021, n. 82, recante «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale» è pubblicato nella *Gazzetta Ufficiale* n. 140 del 14 giugno 2021 e convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, pubblicata nella *Gazzetta Ufficiale* n. 185 del 4 agosto 2021.

— Il decreto legislativo 3 agosto 2022, n. 123, recante «Norme di adeguamento della normativa nazionale alle disposizioni del Titolo III «Quadro di certificazione della cybersicurezza» del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»)» è pubblicato nella *Gazzetta Ufficiale* n. 194 del 20 agosto 2022.

— La legge 28 giugno 2024, n. 90, recante «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» è pubblicata nella *Gazzetta Ufficiale* n. 153 del 2 luglio 2024.

— Il decreto legislativo 4 settembre 2024, n. 138, recante «Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148» è pubblicato nella *Gazzetta Ufficiale* n. 230 del 1° ottobre 2024.

Note all'art. 1:

— Si riporta il testo degli articoli 3, 5, 6, 7, 9, 10 e 13 del citato decreto legislativo 3 agosto 2022, n. 123, come modificato dal presente decreto:

«Art. 3 (Definizioni). — 1. Ai fini del presente decreto, oltre alle definizioni contenute nel regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, si applicano le seguenti:

a) «TIC»: Tecnologia dell'Informazione e della Comunicazione;

a-bis) «servizio di sicurezza gestito»: un servizio prestato a un terzo consistente nello svolgimento di attività o nella fornitura di assistenza per tali attività, legate alla gestione dei rischi in materia di cybersicurezza, ad esempio servizi di gestione degli incidenti, test di penetrazione, audit di sicurezza e consulenza, tra cui consulenza specialistica, relativa all'assistenza tecnica;

b) «Regolamento»: Titolo III del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo

all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013;

c) «quadro europeo di certificazione»: il Regolamento ed i successivi sistemi europei di certificazione adottati a norma dell'articolo 49 del Regolamento;

d) «messa a disposizione sul mercato»: la fornitura di un prodotto TIC, di un servizio TIC o di un servizio di sicurezza gestito per la distribuzione, il consumo o l'uso sul mercato dell'Unione Europea nel corso di un'attività commerciale, a titolo oneroso o gratuito;

e) «richiamo»: qualsiasi provvedimento volto ad ottenere la restituzione di un prodotto TIC che è già stato reso disponibile all'utilizzatore finale;

f) «ritiro»: qualsiasi provvedimento volto ad impedire la messa a disposizione sul mercato di un prodotto TIC, di un servizio TIC o di un servizio di sicurezza gestito nella catena della fornitura;

g) «vigilanza del mercato»: le attività svolte ed i provvedimenti adottati dall'Agenzia e dalle altre autorità pubbliche competenti per garantire che i prodotti TIC, i servizi TIC ed i processi TIC ad essi collegati nonché i servizi di sicurezza gestiti siano conformi ai requisiti stabiliti dal quadro europeo di certificazione e non pregiudichino la salute, la sicurezza o qualsiasi altro aspetto della protezione del pubblico interesse;

h) «Agenzia»: l'Agenzia per la cybersicurezza nazionale di cui all'articolo 5 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, designata dall'articolo 7, comma 1, lettera e), del medesimo decreto-legge, per l'Italia, quale autorità nazionale di certificazione della cybersicurezza, di cui all'articolo 58, paragrafo 1, del Regolamento;

i) «standard» o «norma»: una specifica tecnica, adottata da un organismo di normazione riconosciuto ai sensi dell'articolo 2, paragrafo 1, numero 1), del regolamento (UE) n. 1025/2012;

l) «norma armonizzata»: una norma europea adottata sulla base di una richiesta della Commissione Europea ai fini dell'applicazione della legislazione dell'Unione sull'armonizzazione ai sensi dell'articolo 2, paragrafo 1, numero 1, lettera c), del regolamento (UE) n. 1025/2012;

m) «Organismo di accreditamento»: l'organismo autorizzato a svolgere l'attività di accreditamento nel territorio dello Stato, ai sensi dell'articolo 2, paragrafo 1, numero 11, del regolamento (CE) 765/2008, designato con decreto del Ministro dello sviluppo economico del 22 dicembre 2009 in attuazione dell'articolo 4, comma 2, della legge 23 luglio 2009, n. 99;

n) «autorizzazione»: provvedimento con il quale l'Agenzia accerta il possesso, a norma dell'articolo 54, paragrafo 1, lettera f), del Regolamento, di requisiti specifici o supplementari a cui sono soggetti gli organismi di valutazione della conformità per poter operare nell'ambito di uno specifico sistema europeo di certificazione, in aggiunta a quanto già previsto nell'allegato del Regolamento;

o) «abilitazione»: provvedimento con il quale l'Agenzia accerta i requisiti necessari affinché un esperto o un laboratorio di prova possa coadiuvare l'Agenzia nelle attività di vigilanza nazionale o di rilascio dei certificati di cybersicurezza;

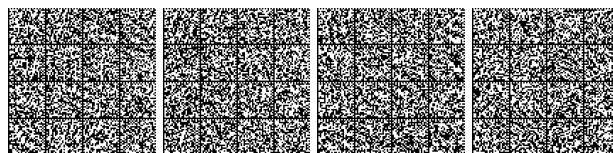
p) «laboratorio di prova»: organismo di valutazione della conformità che svolge verifiche documentali e/o prove in base alle norme armonizzate europee ed agli standard di riferimento ai sensi del sistema europeo di certificazione in cui è accreditato;

q) «organismo di certificazione»: organismo di valutazione della conformità che emette certificati europei di cybersicurezza in base alle norme armonizzate europee ed agli standard di riferimento ai sensi dell'articolo 54, paragrafo 1, lettera c), del Regolamento per il sistema di certificazione in cui è accreditato;

r) «elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale»: registro aggiornato dei laboratori di prova e degli esperti abilitati dall'Agenzia ad effettuare attività di valutazione di sicurezza informatica nell'ambito dei compiti di vigilanza nazionale dell'Agenzia;

s) «elenco dei laboratori di prova e degli esperti per le attività di certificazione»: registro aggiornato dei laboratori di prova e degli esperti abilitati dall'Agenzia ad effettuare attività di valutazione di sicurezza informatica nell'ambito dei compiti di rilascio dei certificati di cybersicurezza dell'Agenzia;

t) «Organismo di Certificazione della Sicurezza Informatica» o «OCST»: organismo di certificazione dell'Agenzia, accreditato ai sensi



dell'articolo 60, paragrafo 2, del Regolamento, istituito ai sensi dell'articolo 4 del decreto del Presidente del Consiglio dei ministri del 30 ottobre 2003, pubblicato nella *Gazzetta Ufficiale* n. 98 del 27 aprile 2004;

u) "dichiarazione UE di conformità": attestazione di conformità rilasciata da un fabbricante di *prodotti TIC*, un *fornitore di servizi TIC* o un *fornitore di servizi di sicurezza gestiti* ai sensi dell'articolo 53, paragrafo 1, del regolamento UE 2019/881, a seguito del processo di autovalutazione di conformità previsto dallo stesso articolo;

v) "emittenti delle dichiarazioni di conformità UE": i soggetti di cui all'articolo 53, paragrafo 1, del regolamento UE 2019/881;

z) "certificato europeo di cybersicurezza": un documento rilasciato da un organismo di certificazione che attesta che un determinato prodotto *TIC*, *servizio TIC*, *processo TIC* o *servizio di sicurezza gestito* è stato oggetto di una valutazione di conformità ai requisiti stabiliti da un sistema europeo di certificazione;

aa) "certificato europeo di cybersicurezza (o dichiarazione UE di conformità) non conforme": certificato europeo di cybersicurezza (o dichiarazione UE di conformità) che non soddisfa uno o più requisiti di un sistema europeo di certificazione ai sensi dell'articolo 54, paragrafo 1, del Regolamento;

bb) "revoca di un certificato europeo di cybersicurezza": annullamento di un certificato europeo di cybersicurezza prima della sua scadenza da parte dell'organismo di valutazione della conformità emittente o da parte dell'Agenzia;

cc) "revoca di una dichiarazione UE di conformità": annullamento di una dichiarazione UE di conformità prima della sua scadenza da parte del fabbricante o fornitore emittente;

dd) "livello di affidabilità di base": livello di affidabilità che soddisfa i requisiti ed è valutato con i criteri specificati al paragrafo 5 dell'articolo 52 del Regolamento;

ee) "livello di affidabilità sostanziale": livello di affidabilità che soddisfa i requisiti ed è valutato con i criteri specificati al paragrafo 6 dell'articolo 52 del Regolamento;

ff) "livello di affidabilità elevato": livello di affidabilità che soddisfa i requisiti ed è valutato con i criteri specificati al paragrafo 7 dell'articolo 52 del Regolamento;

gg) "ECCG": Gruppo europeo di certificazione della cybersicurezza, ai sensi dell'articolo 62 del Regolamento;

hh) "ENISA": l'Agenzia dell'Unione europea per la cybersicurezza di cui al Titolo II del regolamento (UE) 2019/881.

«Art. 5 (*Vigilanza nazionale*). — 1. L'Agenzia realizza l'attività di vigilanza del mercato in ambito nazionale ai fini della corretta applicazione delle regole previste dai sistemi europei di certificazione della cybersicurezza, con riferimento ai certificati di cybersicurezza ed alle dichiarazioni UE di conformità emessi nel territorio dello Stato, ai sensi dell'articolo 58, paragrafo 7, lettere a) e b), del Regolamento, vigilando sui fornitori e fabbricanti emittenti le dichiarazioni UE di conformità, sui titolari di certificati europei di cybersicurezza e sugli organismi di valutazione della conformità, ai sensi dell'articolo 58, paragrafo 8, del Regolamento. L'Agenzia, inoltre, ai sensi dell'articolo 58, paragrafo 7, lettere c), d) ed e), del Regolamento:

a) fatto salvo l'articolo 60, paragrafo 3, del Regolamento nonché quanto stabilito alla lettera b) del presente comma, assiste e sostiene attivamente l'Organismo di accreditamento nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità ai fini del Regolamento. Le modalità di sostegno ed assistenza dell'Agenzia all'Organismo di accreditamento per l'attività di vigilanza sono disciplinate da apposita convenzione o protocollo di intesa fra i medesimi soggetti;

b) monitora e vigila sulle attività degli organismi di valutazione della conformità pubblici di cui all'articolo 56, paragrafo 5, lettera b), del Regolamento;

c) ove previsto dal sistema di certificazione ai sensi dell'articolo 54, paragrafo 1, lettera f), del Regolamento, autorizza gli organismi di valutazione della conformità a norma dell'articolo 60, paragrafo 3, del Regolamento, e limita, sospende o revoca l'autorizzazione esistente qualora violino le prescrizioni del Regolamento medesimo, dandone notizia all'Organismo di accreditamento.

2. L'Agenzia, nello svolgimento dell'attività di vigilanza di cui al comma 1, opera anche in collaborazione con altre autorità di vigilanza del mercato competenti in Italia e con le autorità di vigilanza degli altri Stati membri ai sensi dell'articolo 58, paragrafo 7, lettere a) ed h), del Regolamento. L'Agenzia esegue l'attività di vigilanza di cui al comma 1 anche in collaborazione con le Forze dell'ordine.

3. L'Agenzia, nell'attività di vigilanza di cui al comma 1, può effettuare, nei confronti degli organismi di valutazione della conformità, dei titolari dei certificati europei di cybersicurezza e degli emittenti le dichiarazioni di conformità UE, indagini ed audit, ottenendo informazioni anche tramite l'accesso ai locali degli organismi di valutazione della conformità o dei titolari dei certificati europei di cybersicurezza, revocare certificati ai sensi del comma 4, irrogare sanzioni pecuniarie ed accessorie ai sensi dell'articolo 10. L'attività di vigilanza dell'Agenzia può prevedere prelievi di prodotti.

4. Nel caso in cui l'Agenzia, in esito alle attività di vigilanza di cui al comma 1, accerti l'emissione di un certificato non conforme, rilasciato ai sensi dell'articolo 56, paragrafi 4, 5, lettera b), o 6, lettere a) e b), del Regolamento, il certificato è sottoposto a revoca:

a) per il livello di affidabilità elevato;

b) per il livello di affidabilità di base o sostanziale nel caso in cui il certificato non conforme sia relativo ad un prodotto *TIC*, *servizio TIC*, *processo TIC* o *servizio di sicurezza gestito* che ha comportato un concreto e dimostrato pregiudizio a un soggetto essenziale di cui all'articolo 6, commi 1 e 2, del decreto legislativo 4 settembre 2024, n. 138, o alla salute o all'incolumità personale;

c) se previsto espressamente dallo specifico sistema europeo di certificazione.

5. Nella fattispecie di cui alla lettera a) del comma 4 l'Agenzia provvede direttamente alla revoca del certificato. Nella fattispecie di cui alla lettera b) del comma 4 l'Agenzia chiede all'organismo emittente il certificato di provvedere alla revoca del certificato, *dandone contestuale notifica all'Agenzia*, entro e non oltre cinque giorni e, in caso di inottemperanza, provvede direttamente entro i successivi cinque giorni. Nella fattispecie di cui alla lettera c) del comma 4 si provvede in base alle regole stabilite dal sistema specifico di certificazione.

6. Accertata l'emissione di un certificato non conforme rilasciato ai sensi dell'articolo 56, paragrafi 4, 5, lettera b), o 6, lettere a) e b), del Regolamento, in esito alle attività di vigilanza di cui al comma 1, fatti salvi i casi di revoca di cui alle lettere a), b) o c) del comma 4, l'Agenzia chiede all'organismo che ha emesso il certificato di ripetere in tutto o in parte l'attività di valutazione o integrare l'attività di valutazione con ulteriori verifiche e ricondurre il certificato a conformità entro i termini stabiliti dall'Agenzia e comunque non oltre centoventi giorni o revocare il certificato. In caso di mancata riconduzione a conformità o mancata revoca del certificato non conforme da parte dell'organismo, il certificato decade. La riconduzione a conformità o la revoca del certificato sono divulgate ai sensi dell'articolo 54, paragrafo 1, lettera s), del Regolamento.

7. L'Agenzia, per le prove tecniche nell'ambito delle attività di cui al comma 1, può effettuare valutazioni di sicurezza informatica anche attraverso esperti esterni o laboratori di prova abilitati dall'Agenzia, ai sensi dell'articolo 8, comma 4, e iscritti nell'elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale.

8. È fatto obbligo agli organismi di valutazione della conformità, ai titolari dei certificati europei di cybersicurezza ed agli emittenti delle dichiarazioni di conformità durante l'attività di vigilanza a cui sono sottoposti di cooperare con l'Agenzia nell'attività di verifica sui certificati e sulle dichiarazioni UE da essi emessi. Gli stessi mettono a disposizione, su richiesta dell'Agenzia, tutti i documenti di valutazione necessari per dimostrare la conformità dei certificati e le dichiarazioni oggetto di verifica da parte dell'Agenzia assieme agli strumenti di valutazione eventualmente forniti dal fabbricante o dal fornitore nell'attività di valutazione come indicato nei rapporti di valutazione. L'onere della prova della conformità di certificati e dichiarazioni è in capo agli organismi di valutazione della conformità, ai titolari dei certificati o agli emittenti delle dichiarazioni di conformità.

9. Ai sensi dell'articolo 30, commi 4 e 5, della legge 24 dicembre 2012, n. 234, gli oneri derivanti dall'applicazione dei commi 3 e 8 per i controlli effettuati dall'Agenzia e relativi in particolare all'impiego del personale in forza all'Agenzia, della strumentazione utilizzata nelle prove e dei materiali di consumo e per le missioni e spese generali, sono a carico dell'organismo di valutazione della conformità, del titolare del certificato o dell'emittente della dichiarazione UE di conformità sottoposto all'attività di vigilanza. Nel caso in cui l'attività di vigilanza includa ulteriori spese, tra cui l'utilizzo di laboratori di prova esterni ed eventuali spese di trasporto per prodotti prelevati o sequestrati da sottoporre a verifica, le ulteriori spese sono ugualmente a carico del soggetto sottoposto all'attività di vigilanza. Le somme di cui al presente comma sono determinate e sono da corrispondere ai sensi dell'articolo 13.»



«Art. 6 (*Rilascio dei certificati di cybersicurezza*). — 1. L'Agenzia rilascia i certificati di cybersicurezza con livello di affidabilità elevato, *sostanziale e di base* tramite l'Organismo di Certificazione della Sicurezza Informatica (OCSI), di cui all'articolo 60, paragrafo 2, del Regolamento, che si può avvalere di esperti o di laboratori di prova, ai sensi dell'articolo 8, comma 4, abilitati dall'Agenzia ad operare per proprio conto e iscritti nell'elenco dei laboratori di prova e degli esperti per le attività di *certificazione*, ferme restando, per specifici sistemi di certificazione, le possibili modalità di emissione dei certificati alternative ai sensi degli articoli 56, paragrafo 6, lettere a) e b), del Regolamento.

2. Ove uno specifico sistema di certificazione preveda il rilascio dei certificati con livello di affidabilità sostanziale o di base unicamente da parte di un organismo pubblico, ai sensi dell'articolo 56, paragrafo 5, del Regolamento, l'Agenzia rilascia tali certificati attraverso l'organismo di cui al comma 1. Il rilascio può avvenire ad opera di altro organismo di valutazione della conformità pubblico, accreditato dall'Organismo di Accreditamento, monitorato e vigilato dall'Agenzia, ai sensi dell'articolo 58, paragrafo 7, lettera d), del Regolamento, e designato dall'Agenzia ai sensi del provvedimento di cui all'articolo 4, comma 2, salvo diverse disposizioni dello specifico sistema europeo di certificazione.

3. La certificazione della cybersicurezza è volontaria, salvo diversamente specificato dal diritto dell'Unione o dal diritto nazionale, ai sensi dell'articolo 56, paragrafo 2, del Regolamento. In mancanza di un diritto dell'Unione armonizzato, l'Agenzia può adottare, previa consultazione con i portatori di interesse, regolamentazioni tecniche nazionali in cui sia prevista una certificazione obbligatoria nel quadro di un sistema europeo di certificazione della cybersicurezza ai sensi del decreto legislativo del 15 dicembre 2017, n. 223.

4. Ai sensi dell'articolo 30, commi 4 e 5, della legge 24 dicembre 2012, n. 234, gli oneri derivanti dall'applicazione dei commi 1 e 2 del presente articolo per il rilascio dei certificati da parte dell'Agenzia sono a carico del soggetto richiedente la certificazione. Le somme di cui al presente comma sono determinate e sono da corrispondere ai sensi dell'articolo 13.»

«Art. 7 (*Dichiarazioni UE di conformità*). — 1. In un sistema di certificazione in cui è autorizzata l'autovalutazione di conformità ai sensi dell'articolo 54, paragrafo 1, lettera e), del Regolamento, i fornitori o fabbricanti di prodotti TIC, *servizi TIC, processi TIC o servizi di sicurezza gestiti* possono rilasciare sotto la propria responsabilità dichiarazioni UE di conformità di livello di base per dimostrare il rispetto di requisiti tecnici previsti nel sistema.

2. Il fabbricante o fornitore di prodotti TIC, *servizi TIC, processi TIC o servizi di sicurezza gestiti* rende disponibile all'Agenzia, per il periodo stabilito nel corrispondente sistema europeo di certificazione della cybersicurezza ai sensi dell'articolo 54, paragrafo 1, lettera q), del Regolamento, la dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti relative alla conformità dei prodotti TIC, *servizi TIC o servizi di sicurezza gestiti* al sistema. Una copia della dichiarazione UE di conformità è trasmessa all'Agenzia e all'ENISA.

3. Ove l'Agenzia accerti la non conformità di una dichiarazione UE di conformità in esito alle attività di vigilanza di cui all'articolo 5, comma 1, è fatto obbligo al fabbricante o fornitore emittente di revisionare o revocare la dichiarazione UE di conformità entro trenta giorni dandone comunicazione all'Agenzia e all'ENISA, salvo diversa disposizione dello specifico sistema di certificazione.

4. Il rilascio di una dichiarazione UE di conformità è volontario, salvo diversamente specificato nel diritto dell'Unione o dal diritto nazionale, ai sensi dell'articolo 53, paragrafo 4 del Regolamento. In mancanza di un diritto dell'Unione armonizzato, l'Agenzia può stabilire l'obbligatorietà della dichiarazione UE di conformità nelle fattispecie di cui all'articolo 6, comma 3.»

«Art. 9 (*Attività di ricerca, formazione e sperimentazione nazionale nell'ambito della certificazione della cybersicurezza*). — 1. Allo scopo di elevare il livello nazionale di cybersicurezza, l'Agenzia può realizzare progetti di ricerca, ivi inclusi quelli per lo sviluppo di software, e di formazione, anche in collaborazione con università, centri di ricerca o laboratori specializzati nel campo della valutazione della sicurezza informatica, anche nel contesto di attività di supporto alla standardizzazione a livello nazionale, europeo ed internazionale.

2. L'Agenzia monitora gli sviluppi nel campo della certificazione della cybersicurezza, anche consultando i portatori di interesse

nazionale del settore e scambiando informazioni, esperienze e buone pratiche con la Commissione europea e le altre autorità nazionali della cybersicurezza.

3. Conformemente all'articolo 57 del Regolamento ed in assenza di un sistema europeo di certificazione, l'Agenzia può introdurre sistemi di certificazione nazionali della cybersicurezza, per prodotti TIC, *servizi TIC, processi TIC o servizi di sicurezza gestiti*».

«Art. 10 (*Quadro sanzionatorio*). — 1. L'Agenzia, anche ai sensi dell'articolo 7, comma 1, lettera e), del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, in caso di violazione degli obblighi del quadro europeo di certificazione della cybersicurezza, ai sensi degli articoli 58, paragrafo 8, lettera f), e 65 del Regolamento irroga sanzioni pecuniarie ed accessorie, chiedendo la cessazione immediata della violazione. Si applica l'articolo 17, comma 4-quater, del decreto-legge n. 82 del 2021.

2. Salvo che il fatto costituisca reato, l'organismo di valutazione della conformità che emette un certificato di cybersicurezza non conforme è punito con la sanzione del pagamento di una somma da 15.000 euro a 75.000 euro. In caso di omessa revoca di un certificato da parte dell'organismo su richiesta dell'Agenzia ai sensi dell'articolo 5, comma 5, si applica la sanzione del pagamento di una somma da 30.000 euro a 150.000 euro.

3. Salvo che il fatto costituisca reato, il fabbricante o fornitore che emette una dichiarazione UE di conformità volontaria non conforme è punito con la sanzione del pagamento di una somma da 15.000 euro a 75.000 euro. In caso di omessa revisione o revoca di dichiarazione UE di conformità volontaria o obbligatoria ai sensi dell'articolo 7, comma 3, si applica la sanzione del pagamento di una somma da 30.000 euro a 150.000 euro.

4. Salvo che il fatto costituisca reato, in caso di obbligatorietà di una dichiarazione UE di conformità, ai sensi dell'articolo 7, comma 4, o di un certificato di cybersicurezza, ai sensi dell'articolo 6, comma 3, il fabbricante o fornitore che mette a disposizione sul mercato un prodotto TIC, *un servizio TIC o un servizio di sicurezza gestito* privo di dichiarazione UE di conformità obbligatoria o con dichiarazione UE di conformità obbligatoria non conforme o in assenza del certificato di cybersicurezza obbligatorio, è punito con la sanzione del pagamento di una somma da 30.000 euro a 150.000 euro. Alla medesima sanzione è assoggettato il fabbricante o fornitore che per la messa a disposizione sul mercato di un prodotto TIC o di un servizio TIC si avvale di un processo TIC privo di dichiarazione UE di conformità obbligatoria o con dichiarazione UE di conformità obbligatoria non conforme o in assenza di certificato di cybersicurezza obbligatorio.

5. Nei casi di cui al comma 4 oppure ove, in esito ad un accertamento di non conformità ai sensi dei commi 4, 5 o 6 dell'articolo 5, sia revocato o decada un certificato obbligatorio per la messa a disposizione sul mercato di un prodotto TIC, *di un servizio TIC o di un servizio di sicurezza gestito*, l'Agenzia dispone il ritiro del prodotto o l'inibizione del servizio dal mercato a carico esclusivo del fabbricante o del fornitore indicando i tempi ed eventuali modalità per il richiamo dei prodotti già immessi sul mercato o per l'inibizione del servizio;

6. Salvo che il fatto costituisca reato, il fabbricante che non ottempera a quanto prescritto al comma 5 per il richiamo di prodotti già immessi sul mercato è assoggettato alla sanzione del pagamento di una somma da 60.000 euro a 300.000 euro. Nel caso in cui il fabbricante non ottemperi al richiamo di prodotti dal mercato, l'Agenzia, trascorsi sei mesi dalla scadenza fissata, può provvedere, al sequestro dei prodotti in questione dal mercato, a spese del fabbricante.

7. Salvo che il fatto costituisca reato, il fornitore che non ottempera a quanto prescritto al comma 5 per l'inibizione del servizio dal mercato è assoggettato alla sanzione amministrativa da 60.000 euro a 300.000 euro.

8. Salvo che il fatto costituisca reato, il titolare di un certificato europeo di cybersicurezza che non notifichi, ai sensi dell'articolo 56, paragrafo 8, del Regolamento, eventuali vulnerabilità o irregolarità rilevate in relazione alla sicurezza dei prodotti TIC, *servizi TIC, processi TIC o servizi di sicurezza gestiti* certificati è punito con la sanzione del pagamento di una somma da 60.000 euro a 300.000 euro. Alla medesima sanzione è assoggettato l'organismo di valutazione della conformità emittente un certificato di cybersicurezza o il suo titolare ovvero il fornitore o fabbricante emittente una dichiarazione UE di conformità, che dovesse rilevare o venire a conoscenza della presenza di vulnerabilità nel prodotto TIC, *servizio TIC, processo TIC o servizio di sicurezza gestito* certificato o dichiarato conforme, che non siano state riscontrate durante il processo di valutazione, e non ottemperi agli obblighi riguar-



danti il modo in cui segnalare e trattare le vulnerabilità previste per lo specifico sistema di certificazione ai sensi dell'articolo 54, paragrafo 1, lettera m), del Regolamento.

9. Salvo che il fatto costituisca reato, il fabbricante o fornitore che non renda disponibile, per il periodo stabilito ai sensi dell'articolo 54, paragrafo 1, lettera q), del Regolamento, la dichiarazione UE di conformità o la documentazione tecnica o tutte le altre informazioni pertinenti o non trasmetta una copia della dichiarazione UE di conformità all'Agenzia o ad ENISA ai sensi dell'articolo 53, paragrafo 3, del Regolamento ovvero non renda disponibili pubblicamente una o più delle informazioni previste ai sensi dell'articolo 55 del Regolamento o non rispetti il formato o le procedure di aggiornamento delle stesse informazioni ai sensi dell'articolo 54, paragrafo 1, lettera v), del Regolamento o pubblici informazioni non corrette sui certificati detenuti o sulle dichiarazioni UE di conformità emesse, è assoggettato alla sanzione del pagamento di una somma da 30.000 euro a 150.000 euro. Alla medesima sanzione è assoggettato il fornitore o fabbricante che non comunichi la revisione o la revoca di una dichiarazione UE di conformità ai sensi dell'articolo 7, comma 3, del presente decreto.

10. Salvo che il fatto costituisca reato, l'organismo di valutazione della conformità che non ottempera agli obblighi di divulgazione dei certificati europei di cybersicurezza rilasciati, modificati o revocati come previsto nell'ambito dello specifico sistema di certificazione, ai sensi dell'articolo 54, paragrafo 1, lettera s), del Regolamento, nonché secondo le modalità di cui all'articolo 5, comma 6, è assoggettato alla sanzione del pagamento di una somma da 30.000 euro a 150.000 euro. Alla medesima sanzione è assoggettato l'organismo di valutazione della conformità autorizzato dall'Agenzia ai sensi dell'articolo 60, paragrafo 3, del Regolamento, che non specifichi nella procedura per i reclami definita ai sensi dell'articolo 11, comma 2, l'inoltro degli stessi per conoscenza anche all'Agenzia.

11. Salvo che il fatto costituisca reato, nel caso di accertamento di esercizio di organismo di valutazione della conformità senza autorizzazione di cui all'articolo 60, paragrafo 3, del Regolamento si applica la sanzione del pagamento di una somma da 120.000 euro a 600.000 euro e al soggetto non possono essere rilasciate ulteriori autorizzazioni nei successivi tre anni dall'accertamento della violazione. Se l'autorizzazione è scaduta da meno di un anno la sanzione è compresa tra 30.000 euro e 150.000 euro ed il soggetto può richiedere il rilascio di nuova autorizzazione.

12. Salvo che i fatti costituiscano reato, il richiedente di una certificazione che nell'ambito dello svolgimento dell'attività di valutazione e di rilascio dei certificati, scientemente, fornisce dati, informazioni o documentazione falsi o ometta informazioni necessarie per espletare la certificazione, in violazione dell'articolo 54, paragrafo 1, lettera h), e dell'articolo 56, paragrafo 7, del Regolamento, è assoggettato alla sanzione del pagamento di una somma da 90.000 euro a 450.000 euro. Alla medesima sanzione è assoggettato il soggetto che, scientemente, durante le verifiche di vigilanza, a cui è sottoposto, ai sensi dell'articolo 5, comma 8, fornisce dati, informazioni o documentazione falsi.

13. Salvo che il fatto costituisca reato, il fabbricante che viola le condizioni di utilizzo degli eventuali marchi o etichette previste da un sistema europeo di certificazione, ai sensi dell'articolo 54, paragrafo 1, lettera i), del Regolamento, è assoggettato alla sanzione del pagamento di una somma da 30.000 euro a 150.000 euro.

14. Salvo che il fatto costituisca reato, l'organismo di valutazione della conformità che non ottempera agli eventuali obblighi riguardanti la conservazione dei registri di cui all'articolo 54, paragrafo 1, lettera n), del Regolamento, è assoggettato alla sanzione del pagamento di una somma da 45.000 euro a 225.000 euro.

15. L'Agenzia può impartire ordini o intimare diffide ai soggetti che operano in contrasto con quanto previsto dal quadro europeo di certificazione. Ai soggetti che non ottemperano nel termine indicato nell'ordine o nella diffida l'Agenzia commina la sanzione del pagamento di una somma da 200.000 euro ad 1.000.000 di euro. Se le violazioni riguardano provvedimenti adottati dall'Agenzia nei confronti di soggetti con fatturato pari almeno a 200.000.000 euro, si applica a ciascun soggetto interessato una sanzione amministrativa pecuniaria non inferiore allo 0,3 per cento e non superiore all'1,5 per cento del fatturato, restando comunque fermo il limite massimo di 5.000.000 di euro. Come riferimento per il fatturato si assume il valore realizzato dallo stesso soggetto nell'esercizio precedente a quello in cui sia stato impartito l'ordine o sia stata intimata la diffida.

16. Fermo restando il limite massimo di 5.000.000 di euro per la sanzione, i valori minimi e massimi delle sanzioni pecuniarie dal comma 2 al comma 15, sono triplicati, se la violazione ha riguardato un

certificato relativo ad un prodotto TIC, ad un servizio TIC, ad un processo TIC o a un servizio di sicurezza gestito rilasciato nell'ambito di un sistema di certificazione destinato, ai sensi dell'articolo 54, paragrafo 1, lettere a) o b), del Regolamento, all'utilizzo con le finalità o nell'ambito di un servizio erogato da un soggetto essenziale di cui all'articolo 6, commi 1 e 2, del decreto legislativo 4 settembre 2024, n. 138.

17. I criteri di graduazione nell'irrogazione delle sanzioni pecuniarie sono definiti con successivo provvedimento dell'Agenzia, adottato secondo la procedura di cui all'articolo 5, comma 3, alinea, del decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223. Nelle more dell'adozione del provvedimento di definizione dei criteri di graduazione si applicano i criteri di cui all'articolo 11 della legge 24 novembre 1981, n. 689.

18. Fermo restando il limite massimo di 5.000.000 di euro per la sanzione, le sanzioni amministrative pecuniarie previste ai commi dal 2 al 14 sono rivalutate ogni cinque anni con provvedimento dell'Agenzia, adottato secondo la procedura di cui all'articolo 5, comma 3, alinea, del regolamento adottato con decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223, in misura pari all'indice ISTAT dei prezzi al consumo previo arrotondamento all'unità di euro secondo il seguente criterio: se la parte decimale è inferiore a 50 centesimi l'arrotondamento va effettuato per difetto, se è uguale o superiore a 50 centesimi l'arrotondamento va effettuato per eccesso. L'importo della sanzione pecuniaria rivalutata secondo i predetti criteri si applica esclusivamente per le violazioni commesse successivamente alla data di entrata in vigore del provvedimento che lo prevede.

19. L'autorizzazione di un organismo di valutazione della conformità ad operare nel sistema europeo di certificazione ai sensi dell'articolo 60, paragrafo 3, del Regolamento, ove prevista, è sospesa per 6 mesi o revocata nel caso di più di due violazioni del quadro europeo di certificazione rispettivamente in un quinquennio o in un biennio. In caso di revoca dell'autorizzazione, il trasgressore non può ottenere nuova autorizzazione nei successivi cinque anni dal provvedimento di revoca.

20. L'Agenzia notifica alla Commissione europea il quadro sanzionatorio di cui al presente articolo entro sessanta giorni dalla data di entrata in vigore del presente decreto e provvede poi a dare notifica delle eventuali modifiche entro sessanta giorni successivi alle stesse.»

«Art. 13 (Destinazione dei proventi derivanti dalle attività dell'Agenzia). — 1. Le attività di vigilanza di cui all'articolo 5, comma 1, di certificazione di cui all'articolo 6, comma 1, di autorizzazione di cui all'articolo 8, comma 3, di abilitazione di cui all'articolo 8, comma 4, sono sottoposte a tariffa, da calcolarsi sulla base dei costi effettivi dei servizi resi. I relativi proventi sono versati ad apposito capitolo dell'entrata del bilancio dello Stato per essere successivamente riassegnati, con decreto del Ministro dell'economia e delle finanze sul pertinente capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, di cui all'articolo 18 del decreto-legge n. 82 del 2021. Con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, su proposta del Direttore generale dell'Agenzia, sono determinate le tariffe e modalità di riscossione.

2. Le spese per l'impiego di esperti o laboratori abilitati dall'Agenzia per le attività di vigilanza di cui all'articolo 5, comma 1, sono calcolate ai sensi del decreto di cui al comma 1.

3. Gli introiti derivanti dalle sanzioni pecuniarie di cui all'articolo 10 sono versati ad apposito capitolo dell'entrata del bilancio dello Stato per essere successivamente riassegnati con decreto del Ministro dell'economia e delle finanze sul pertinente capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, di cui all'articolo 18 del decreto-legge n. 82 del 2021, e destinati alle attività di ricerca e formazione concernenti la certificazione della cybersicurezza di prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti di cui all'articolo 9, comma 1.»

Note all'art. 2:

— Si riporta il testo dell'articolo 35 del citato decreto legislativo 7 marzo 2005, n. 82, come modificato dal presente decreto:

«Art. 35 (Dispositivi sicuri e procedure per la generazione della firma qualificata). — 1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:

a) sia riservata;

b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni;



c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.

1-bis. Fermo restando quanto previsto dal comma 1, i dispositivi per la creazione di una firma elettronica qualificata o di un sigillo elettronico soddisfano i requisiti di cui all'Allegato II del Regolamento eIDAS.

2. I dispositivi sicuri e le procedure di cui al comma 1 devono garantire l'integrità dei documenti informatici a cui la firma si riferisce. I documenti informatici devono essere presentati al titolare di firma elettronica, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma secondo quanto previsto dalle Linee guida.

3. Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica. La firma con procedura automatica è valida se apposta previo consenso del titolare all'adozione della procedura medesima.

4. I dispositivi sicuri di firma devono essere dotati di certificazione di sicurezza ai sensi dell'articolo 30 del regolamento eIDAS.

5. La conformità dei requisiti di sicurezza dei dispositivi per la creazione di una firma elettronica qualificata o di un sigillo elettronico prescritti dall'Allegato II del regolamento eIDAS è accertata, in Italia, dall'Organismo di certificazione della sicurezza informatica (OCSI). La valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati dal titolare delle chiavi di firma è effettuata dall'Agenzia per l'Italia digitale in conformità ad apposite linee guida da questa emanate, acquisito il parere obbligatorio dell'Organismo di certificazione della sicurezza informatica.

6. La conformità di cui al comma 5 è inoltre riconosciuta se accertata da un organismo all'uopo designato da un altro Stato membro e notificato ai sensi dell'articolo 30, comma 2, del Regolamento eIDAS. Ove previsto dall'organismo di cui al periodo precedente, la valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati dal titolare delle chiavi di firma è effettuata dall'AgID in conformità alle linee guida di cui al comma 5.».

Nota all'art. 3:

— Si riporta il testo dell'articolo 7 del citato decreto-legge 14 giugno 2021, n. 82, come modificato dal presente decreto:

«Art. 7 (Funzioni dell'Agenzia per la cybersicurezza nazionale).

— 1. L'Agenzia:

a) è Autorità nazionale per la cybersicurezza e, in relazione a tale ruolo, assicura, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni, ferme restando le attribuzioni del Ministro dell'interno in qualità di autorità nazionale di pubblica sicurezza, ai sensi della legge 1° aprile 1981, n. 121, il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore. Per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate restano fermi sia quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera l), della legge n. 124 del 2007, sia le competenze dell'Ufficio centrale per la segretezza di cui all'articolo 9 della medesima legge n. 124 del 2007;

b) predispone la strategia nazionale di cybersicurezza;

c) svolge ogni necessaria attività di supporto al funzionamento del Nucleo per la cybersicurezza, di cui all'articolo 8;

d) è Autorità nazionale competente NIS e Punto di contatto unico NIS di cui all'articolo 2, comma 1, lettere d) ed e), del decreto legislativo NIS, a tutela dell'unità giuridica dell'ordinamento;

d-bis) è Autorità nazionale di gestione delle crisi informatiche di cui all'articolo 2, comma 1, lettera g), del decreto legislativo NIS;

d-ter) è CSIRT nazionale, denominato CSIRT Italia, di cui all'articolo 2, comma 1, lettera i), del decreto legislativo NIS;

e) è Autorità nazionale di certificazione della cybersicurezza ai sensi dell'articolo 58 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Mi-

nistero dello sviluppo economico dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni; nello svolgimento dei compiti di cui alla presente lettera:

l) autorizza, ai sensi dell'articolo 60, paragrafo 3, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi europei di certificazione della cybersicurezza che stabiliscono requisiti specifici o supplementari a norma dell'articolo 54, paragrafo 1, lettera f), del citato regolamento (UE) 2019/881;

2) delega, ai sensi dell'articolo 56, paragrafo 6, lettera b), del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, il Ministero della difesa e il Ministero dell'interno, attraverso le rispettive strutture accreditate ai sensi dell'articolo 60, paragrafo 1, del citato regolamento (UE) 2019/881, al rilascio del certificato europeo di sicurezza cibernetica;

e-bis) è Autorità competente per l'esecuzione dei compiti previsti dal regolamento delegato (UE) 2024/1366 della Commissione, dell'11 marzo 2024, che integra il regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio;

f) assume tutte le funzioni in materia di cybersicurezza già attribuite dalle disposizioni vigenti al Ministero dello sviluppo economico, ivi comprese quelle relative:

l) al perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le funzioni attribuite al Centro di valutazione e certificazione nazionale ai sensi del decreto-legge perimetro, le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera c), del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131;

2) alla sicurezza e all'integrità delle comunicazioni elettroniche, di cui agli articoli 16-bis e 16-ter del decreto legislativo 1° agosto 2003, n. 259, e relative disposizioni attuative;

3) alla sicurezza delle reti e dei sistemi informativi, di cui al decreto legislativo NIS;

g) partecipa, per gli ambiti di competenza, al gruppo di coordinamento istituito ai sensi dei regolamenti di cui all'articolo 1, comma 8, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56;

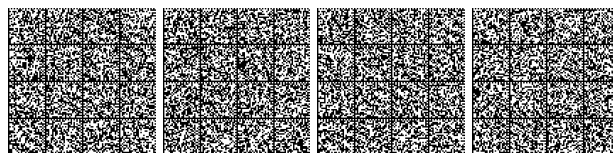
h) assume tutte le funzioni attribuite alla Presidenza del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera c), del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri n. 131 del 2020;

i) assume tutte le funzioni già attribuite al Dipartimento delle informazioni per la sicurezza (DIS), di cui all'articolo 4 della legge 3 agosto 2007, n. 124, dal decreto-legge perimetro e dai relativi provvedimenti attuativi e supporta il Presidente del Consiglio dei ministri ai fini dell'articolo 1, comma 19-bis, del decreto-legge perimetro;

l) provvede, sulla base delle attività di competenza del Nucleo per la cybersicurezza di cui all'articolo 8, alle attività necessarie per l'attuazione e il controllo dell'esecuzione dei provvedimenti assunti dal Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro;

m) assume tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti e, in particolare, quelle di cui all'articolo 51 del decreto legislativo 7 marzo 2005, n. 82, nonché quelle in materia di adozione di linee guida contenenti regole tecniche di cybersicurezza ai sensi dell'articolo 71 del medesimo decreto legislativo. L'Agenzia assume, altresì, i compiti di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, già attribuiti all'Agenzia per l'Italia digitale;

m-bis) provvede, anche attraverso un'apposita sezione nell'ambito della strategia di cui alla lettera b), allo sviluppo e alla diffusione di standard, linee guida e raccomandazioni al fine di rafforzare la cybersicurezza dei sistemi informatici, alla valutazione della sicurezza dei sistemi crittografici nonché all'organizzazione e alla gestione di at-



tività di divulgazione finalizzate a promuovere l'utilizzo della crittografia, anche a vantaggio della tecnologia blockchain, come strumento di cybersicurezza. L'Agenzia, anche per il rafforzamento dell'autonomia industriale e tecnologica dell'Italia, promuove altresì la collaborazione con centri universitari e di ricerca per la valorizzazione dello sviluppo di nuovi algoritmi proprietari, la ricerca e il conseguimento di nuove capacità crittografiche nazionali nonché la collaborazione internazionale con gli organismi esteri che svolgono analoghe funzioni. A tale fine, è istituito presso l'Agenzia, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, il Centro nazionale di crittografia, il cui funzionamento è disciplinato con provvedimento del direttore generale dell'Agenzia stessa. Il Centro nazionale di crittografia svolge le funzioni di centro di competenza nazionale per tutti gli aspetti della crittografia in ambito non classificato, ferme restando le competenze dell'Ufficio centrale per la segretezza, di cui all'articolo 9 della legge 3 agosto 2007, n. 124, con riferimento alle informazioni e alle attività previste dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera l), della citata legge n. 124 del 2007, nonché le competenze degli organismi di cui agli articoli 4, 6 e 7 della medesima legge;

m-ter) provvede alla qualificazione dei servizi cloud per la pubblica amministrazione nel rispetto della disciplina dell'Unione europea e del regolamento di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221;

m-quater) promuove e sviluppa ogni iniziativa, anche attraverso la conclusione di accordi di collaborazione con i privati, comunque denominati, nonché di partenariato pubblico-privato, volta a valorizzare l'intelligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale;

n) sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il CSIRT Italia di cui all'articolo 2, comma 1, lettera i) del decreto legislativo NIS. A tale fine, promuove iniziative di partenariato pubblico-privato per rendere effettive tali capacità;

n-bis) nell'ambito delle funzioni di cui al primo periodo della lettera n), svolge ogni attività diretta all'analisi e al supporto per il contenimento e il ripristino dell'operatività dei sistemi compromessi, con la collaborazione dei soggetti pubblici o privati che hanno subito incidenti di sicurezza informatica o attacchi informatici. La mancata collaborazione di cui al primo periodo è valutata ai fini dell'applicazione delle sanzioni previste dall'articolo 1, commi 10 e 14, del decreto-legge perimetro, per i soggetti di cui all'articolo 1, comma 2-bis, del medesimo decreto-legge perimetro, i soggetti essenziali e i soggetti importanti di cui all'articolo 6 del decreto legislativo NIS, del decreto legislativo NIS e di cui all'articolo 40, comma 3, alinea, del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259; restano esclusi gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, nonché gli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124;

n-ter) provvede alla raccolta, all'elaborazione e alla classificazione dei dati relativi alle notifiche di incidenti ricevute dai soggetti che a ciò siano tenuti in osservanza delle disposizioni vigenti. Tali dati sono resi pubblici nell'ambito della relazione prevista dall'articolo 14, comma 1, quali dati ufficiali di riferimento degli attacchi informatici portati ai soggetti che operano nei settori rilevanti per gli interessi nazionali nel campo della cybersicurezza. Agli adempimenti previsti dalla presente lettera si provvede con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente;

o) partecipa alle esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;

p) cura e promuove la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale. A tal fine, l'Agenzia esprime pareri non vincolanti sulle iniziative legislative o regolamentari concernenti la cybersicurezza;

q) coordina, in raccordo con il Ministero degli affari esteri e della cooperazione internazionale, la cooperazione internazionale nella materia della cybersicurezza. Nell'ambito dell'Unione europea e a livello internazionale, l'Agenzia cura i rapporti con i competenti organismi, istituzioni ed enti, nonché segue nelle competenti sedi istituzionali le

tematiche di cybersicurezza, fatta eccezione per gli ambiti in cui la legge attribuisce specifiche competenze ad altre amministrazioni. In tali casi, è comunque assicurato il raccordo con l'Agenzia al fine di garantire posizioni nazionali unitarie e coerenti con le politiche di cybersicurezza definite dal Presidente del Consiglio dei ministri;

r) perseguendo obiettivi di eccellenza, supporta negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionali, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche. A tali fini, l'Agenzia può promuovere, sviluppare e finanziare specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore. L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza e, in particolare, con il Ministero della difesa per gli aspetti inerenti alla ricerca militare. L'Agenzia può altresì promuovere la costituzione di aree dedicate allo sviluppo dell'innovazione finalizzate a favorire la formazione e il reclutamento di personale nei settori avanzati dello sviluppo della cybersicurezza, nonché promuovere la realizzazione di studi di fattibilità e di analisi valutative finalizzati a tale scopo;

s) stipula accordi bilaterali e multilaterali, anche mediante il coinvolgimento del settore privato e industriale, con istituzioni, enti e organismi di altri Paesi per la partecipazione dell'Italia a programmi di cybersicurezza, assicurando il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale;

t) promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della cybersicurezza e dei correlati servizi applicativi, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale. L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza e, in particolare, con il Ministero della difesa per gli aspetti inerenti a progetti e iniziative in collaborazione con la NATO e con l'Agenzia europea per la difesa;

u) svolge attività di comunicazione e promozione della consapevolezza in materia di cybersicurezza, al fine di contribuire allo sviluppo di una cultura nazionale in materia;

v) promuove la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza, in particolare favorendo l'attivazione di percorsi formativi universitari in materia, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati; nello svolgimento di tali compiti, l'Agenzia può avvalersi anche delle strutture formative e delle capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri interessati;

v-bis) può predisporre attività di formazione specifica riservate ai giovani che aderiscono al servizio civile regolato sulla base di apposite convenzioni. In ogni caso, il servizio prestato è, a tutti gli effetti, riconosciuto come servizio civile;

z) per le finalità di cui al presente articolo, può concludere accordi di collaborazione, comunque denominati, con soggetti privati, costituire e partecipare a partenariati pubblico-privato nel territorio nazionale, nonché, previa autorizzazione del Presidente del Consiglio dei ministri, a consorzi, fondazioni o società con soggetti pubblici e privati, italiani o di Paesi appartenenti all'Unione europea. Sulla base dell'interesse nazionale e previa autorizzazione del Presidente del Consiglio dei ministri, può altresì partecipare a consorzi, fondazioni o società con soggetti pubblici e privati di Paesi della NATO ovvero di Paesi extra-europei con i quali siano stati sottoscritti accordi di cooperazione o di partenariato per lo sviluppo di sistemi di intelligenza artificiale;

aa) è designata quale Centro nazionale di coordinamento ai sensi dell'articolo 6 del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

1-bis. Anche ai fini dell'esercizio delle funzioni di cui al comma 1, lettere r), s), t), u), v), z) e aa), presso l'Agenzia è istituito, con funzioni di consulenza e di proposta, un Comitato tecnico-scientifico, presieduto dal direttore generale della medesima Agenzia, o da un di-



rigente da lui delegato, e composto da personale della stessa Agenzia e da qualificati rappresentanti dell'industria, degli enti di ricerca, dell'accademia e delle associazioni del settore della sicurezza, designati con decreto del Presidente del Consiglio dei ministri. La composizione e l'organizzazione del Comitato tecnico-scientifico sono disciplinate secondo le modalità e i criteri definiti dal regolamento di cui all'articolo 6, comma 1. Per la partecipazione al Comitato tecnico-scientifico non sono previsti gettoni di presenza, compensi o rimborsi di spese.

2. Nell'ambito dell'Agenzia sono nominati, con decreto del Presidente del Consiglio dei ministri, il rappresentante nazionale, e il suo sostituto, nel Consiglio di direzione del Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca, ai sensi dell'articolo 12 del regolamento (UE) 2021/887.

4. Il Centro di valutazione e certificazione nazionale, istituito presso il Ministero dello sviluppo economico, è trasferito presso l'Agenzia.

5. Nel rispetto delle competenze del Garante per la protezione dei dati personali, l'Agenzia, per le finalità di cui al presente decreto, consulta il Garante e collabora con esso, anche in relazione agli incidenti che comportano violazioni di dati personali. L'Agenzia e il Garante possono stipulare appositi protocolli d'intenti che definiscono altresì le modalità della loro collaborazione nell'ambito delle risorse disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica.».

26G00207

DECRETI, DELIBERE E ORDINANZE MINISTERIALI

MINISTERO DELL'AGRICOLTURA, DELLA SOVRANITÀ ALIMENTARE E DELLE FORESTE

DECRETO 13 ottobre 2026.

Conferma dell'incarico al Consorzio di tutela del Peperone di Senise IGP a svolgere le funzioni di cui all'articolo 53 della legge 24 aprile 1998, n. 128, come modificato dall'articolo 14, comma 15, della legge 21 dicembre 1999, n. 526, per la IGP «Peperone di Senise».

IL DIRIGENTE DELLA PQA I
DELLA DIREZIONE GENERALE PER LA PROMOZIONE
DELLA QUALITÀ AGROALIMENTARE

Visto il regolamento (UE) 2024/1143 del Parlamento europeo e del Consiglio dell'11 aprile 2024 relativo alle indicazioni geografiche dei vini, delle bevande spiritose e dei prodotti agricoli, nonché alle specialità tradizionali garantite e alle indicazioni facoltative di qualità per i prodotti agricoli, che modifica i regolamenti (UE) n. 1308/2013, (UE) 2019/787 e (UE) 2019/1753 e che abroga il regolamento (UE) n. 1151/2012;

Visto in particolare l'art. 22 del regolamento (UE) 2024/1143 del Parlamento europeo e del Consiglio dell'11 aprile 2024 che istituisce il registro delle indicazioni geografiche protette di vini, delle bevande spiritose e dei prodotti agricoli dell'Unione;

Viste, inoltre, le premesse sulle quali è fondato il predetto regolamento e, in particolare, quelle relative alle esigenze dei consumatori che, chiedendo qualità e prodotti tradizionali, determinano una domanda di prodotti agricoli o alimentari con caratteristiche specifiche riconoscibili, in particolare modo quelle connesse all'origine geografica;

Considerato che tali esigenze possono essere soddisfatte dai consorzi di tutela che, in quanto costituiti dai soggetti direttamente coinvolti nella filiera produttiva, hanno un'esperienza specifica ed una conoscenza approfondita delle caratteristiche del prodotto;

Visto il regolamento di esecuzione (UE) 2025/26 della Commissione, del 30 ottobre 2024, che reca modalità di applicazione del regolamento (UE) 2024/1143 del Parla-

mento europeo e del Consiglio per quanto riguarda le registrazioni, le modifiche, le cancellazioni, l'applicazione della protezione, l'etichettatura e la comunicazione delle indicazioni geografiche e delle caratteristiche tradizionali garantite, che modifica il regolamento di esecuzione (UE) 2019/34 per quanto riguarda le indicazioni geografiche nel settore vitivinicolo e che abroga i regolamenti di esecuzione (UE) n. 668/2014 e (UE) 2021/1236;

Vista la legge 24 aprile 1998, n. 128, recante disposizioni per l'adempimento di obblighi derivanti dalla appartenenza dell'Italia alle Comunità europee - legge comunitaria 1995 - 1997;

Visto in particolare l'art. 53 della citata legge n. 128 del 1998, come modificato dall'art. 14, comma 15, della legge 21 dicembre 1999, n. 526 che individua le funzioni per l'esercizio delle quali i Consorzi di tutela delle DOP, delle IGP e delle STG possono ricevere, mediante provvedimento di riconoscimento, l'incarico corrispondente dal Ministero dell'agricoltura, della sovranità alimentare e delle foreste;

Visto il decreto 12 settembre 2000, n. 410 pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana - Serie generale - n. 9 del 12 gennaio 2001 - con il quale, in attuazione dell'art. 14, comma 16, della legge n. 526/1999, è stato adottato il regolamento concernente la ripartizione dei costi derivanti dalle attività dei consorzi di tutela delle DOP e delle IGP incaricati dal Ministero;

Visto il decreto legislativo 30 marzo 2001, n. 165, recante norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, ed in particolare l'art. 16, comma 1, lettera d);

Visto il decreto legislativo 19 novembre 2004, n. 297, pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana - Serie generale - n. 293 del 15 dicembre 2004 - recante «Disposizioni sanzionatorie in applicazione del regolamento (CEE) n. 2081/92, relativo alla protezione delle indicazioni geografiche e delle denominazioni di origine dei prodotti agricoli e alimentari»;

Visto il decreto dipartimentale 12 maggio 2010, n. 7422 recante disposizioni generali in materia di verifica delle attività istituzionali attribuite ai consorzi di tutela;

Visto il decreto-legge 11 novembre 2022, n. 173, coordinato con la legge 16 dicembre 2022, n. 204, recante «Disposizioni urgenti in materia di riordino delle attribui-

