RELAZIONE ILLUSTRATIVA

Il presente schema di decreto legislativo si prefigge di dare attuazione alla delega di cui all'articolo 16 della legge 17 marzo 2026, n. 36, *"Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2025"* (nel seguito indicata anche con "legge delega"), il quale, recando la "*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*", dispone che il Governo sia chiamato ad adottare, entro tre mesi dalla data di entrata in vigore della suddetta legge, uno o più`decreti legislativi per adeguare la normativa nazionale alle disposizioni del regolamento (UE) 2025/37 e per coordinare le discipline di settore vigenti al quadro normativo europeo in materia.

In particolare, il citato regolamento (UE) 2025/37 introduce delle modifiche al regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio (cosiddetto *Cybersecurity Act* o regolamento CSA), al fine di estendere il sistema europeo di certificazione della cybersicurezza ai servizi di sicurezza gestiti.

A tal proposito, appare opportuno richiamare il contesto normativo europeo e, in particolare, il *Cybersecurity Act,* con il quale il legislatore europeo ha posto le basi per l'introduzione di sistemi europei di certificazione della cybersicurezza al fine di garantire un livello adeguato di cybersicurezza dei prodotti delle tecnologie dell'informazione e della comunicazione (TIC), dei servizi TIC e dei processi TIC all'interno dell'Unione europea, anche nell'ottica di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cybersicurezza.

In esecuzione del menzionato regolamento (UE) 2019/881, è stato adottato il regolamento di esecuzione (UE) 2024/482 della Commissione del 31 gennaio 2024, recante "*modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC)*", mediante il quale sono stati specificati i ruoli, le norme e gli obblighi, nonché la struttura del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC) in conformità con il quadro europeo di certificazione della cibersicurezza di cui al regolamento CSA. Il menzionato regolamento di esecuzione, infatti, costituisce il primo sistema di certificazione della cybersicurezza dei prodotti TIC, servizi TIC e processi TIC adottato a livello europeo.

A livello nazionale, al fine di assicurare l'adeguamento dell'ordinamento interno al regolamento (UE) 2019/881, è stato adottato il decreto legislativo 3

agosto 2022 n. 123[1], recante "*Norme di adeguamento della normativa nazionale alle disposizioni del Titolo III «Quadro di certificazione della cibersicurezza» 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 cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»)*".

In particolare, il menzionato decreto legislativo ha previsto, in coerenza con la designazione di cui all'articolo 7, comma 1, lettera e), del decreto-legge 14 giugno 2021, n. 82[2], convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, che l'autorità nazionale di certificazione della cybersicurezza sia l'Agenzia per la Cybersicurezza Nazionale (di seguito anche "ACN") e che la medesima Agenzia sia anche l'autorità di vigilanza del mercato. Tali attività – *i.e.* le attività dell'autorità nazionale di certificazione della cybersicurezza relative al rilascio di certificati europei di cybersicurezza e le attività di vigilanza - sono rigorosamente separate in quanto sono svolte, indipendentemente le une dalle altre, da due distinte articolazioni dell'Agenzia. Il decreto legislativo n. 123 del 2022, inoltre, ha definito il quadro sanzionatorio di riferimento, come previsto dall'articolo 65 del regolamento CSA.

In tale quadro normativo, il regolamento (UE) 2025/37, entrato in vigore il 4 febbraio 2025 e obbligatorio nonché direttamente applicabile in ciascuno Stato membro, apporta delle modifiche mirate al regolamento (UE) 2019/881, al fine di estendere il sistema europeo di certificazione della cybersicurezza ai servizi di sicurezza gestiti.

In particolare, i «servizi di sicurezza gestiti» sono definiti come "*un servizio prestato a un terzo consistente nello svolgimento di attività, o nella fornitura*

1 Il decreto legislativo n. 123 del 2022 è stato adottato in attuazione della delega contenuta nell'articolo 18 della legge 22 aprile 2021, n. 53, recante "*Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2019-2020*".

2 L'articolo 7, comma 1, lettera e), del decreto-legge n. 82 del 2021 prevede "*L'Agenzia: [...]*
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 Ministero 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:
1) *accredita, ai sensi dell'articolo 60, paragrafo 1, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza;*
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 di cui al numero 1) della presente lettera, al rilascio del certificato europeo di sicurezza cibernetica*".

di assistenza per tali attività, legate alla gestione dei rischi in materia di cibersicurezza, ad esempio servizi di gestione degli incidenti, test di penetrazione, audit di sicurezza e consulenza, tra cui consulenza specialistica, relativa all'assistenza tecnica" (*Cfr.* articolo 2, punto 14-*bis*), del regolamento (UE) 2019/881, introdotto dall'articolo 1, paragrafo 1), lettera d), del regolamento (UE) 2025/37).

I servizi di sicurezza gestiti svolgono, infatti, un ruolo sempre più importante nella prevenzione, nel rilevamento, nella risposta e nell'attenuazione degli incidenti di cybersicurezza, tanto da essere considerati soggetti "essenziali" o "importanti" ai sensi della direttiva (UE) 2022/2555 (c.d. direttiva NIS 2). Da qui l'esigenza di sottoporre anche tali servizi a sistemi europei di certificazione, in un'ottica di armonizzazione che si è resa necessaria a causa del rischio reale di una frammentazione del mercato interno dovuto alla scelta di alcuni Stati membri di avviare l'adozione di autonomi sistemi di certificazione dei servizi di sicurezza gestiti, ma anche a causa della questione, non irrilevante, dell'individuazione dell'autorità a cui siano riconosciuti i necessari poteri di certificazione e di vigilanza rispetto ai suindicati servizi.

Il regolamento (UE) 2025/37, dunque, persegue molteplici obiettivi di sicurezza:

- garantire che i servizi di sicurezza gestiti siano erogati con adeguati livelli di competenza, esperienza e qualità;
- garantire un elevato livello di protezione dei dati (in termini di riservatezza, integrità e disponibilità) trattati nel corso dell'esecuzione di detti servizi;
- garantire idonee politiche di accesso ai dati da parte di persone e sistemi;
- attuare politiche di monitoraggio dell'accesso ai suddetti dati;
- garantire che i prodotti, i servizi e i processi TIC, nonché *l'hardware*, impiegati nella fornitura dei servizi di sicurezza gestiti siano sicuri per impostazione predefinita (*security by default*) e per progettazione (*security by design*).

Il regolamento in esame, inoltre, è complementare al regolamento (UE) 2025/38 (c.d. regolamento sulla cyber solidarietà o CSoA), la cui delega per adeguare l'ordinamento interno è contenuta nell'articolo 17 della legge delega. Il CSoA, infatti, all'articolo 14, istituisce la "riserva dell'UE per la cybersicurezza", per la cui costituzione si prevede un processo di selezione dei fornitori valutati anche in base al possesso di una certificazione della cybersicurezza europea o nazionale.

Il regolamento (UE) 2025/37, in particolare, mira ad assicurare il pieno raggiungimento degli seguenti obiettivi specifici:

- estendere il sistema europeo di certificazione della cybersicurezza, istituito dal *Cybersecurity Act*, ai servizi di sicurezza gestiti;
- garantire una qualità molto elevata dei servizi di sicurezza gestiti, facendo sì che i relativi fornitori osservino degli standard di competenza, perizia ed esperienza di altissimo livello, prevedendo l'implementazione di procedure interne appropriate;
- promuovere una maggiore concorrenza tra i fornitori di servizi di sicurezza gestiti, semplificando, per quanto possibile, i potenziali oneri normativi, amministrativi e finanziari che tali fornitori, in particolare le piccole e medie imprese (PMI), incluse le microimprese, potrebbero incontrare quando offrono servizi di sicurezza gestiti;
- favorire il mercato transfrontaliero di servizi di sicurezza gestiti attraverso l'istituzione di un meccanismo unico di certificazione, contribuendo alla disponibilità di servizi sicuri e di elevata qualità che garantiscano una transizione digitale sicura, anche al fine di rispettare gli obiettivi stabiliti nel programma strategico per il decennio digitale 2030 istituito dalla decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio del 14 dicembre 2022;
- accrescere il livello complessivo della cybersicurezza, agevolando l'emergere di fornitori di servizi di cybersicurezza affidabili.

Pertanto, come anticipato, l'articolo 16 della legge delega prevede l'adozione da parte del Governo di uno o più`decreti legislativi per adeguare la normativa nazionale alle disposizioni del regolamento (UE) 2025/37 e per coordinare le discipline di settore vigenti al quadro normativo europeo in materia, osservando, oltre ai princìpi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, i seguenti princìpi 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 necessarie ad assicurare la corretta e integrale applicazione del regolamento (UE) 2019/881, 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), punti 1) e 2), del medesimo decreto-legge n. 82 del 2021, in conformità con le pertinenti disposizioni del regolamento (UE) 2019/881"

Ciò premesso, definiti gli obiettivi e gli spazi d'intervento per il Governo in base all'articolo 16 della legge delega, si è scelto di operare attraverso un singolo decreto legislativo recante tutte le riforme necessarie per assicurare la corretta e integrale applicazione del regolamento (UE) 2019/881, anche con riguardo alle modifiche apportate dal regolamento (UE) 2025/37, nell'ordinamento interno.

Appare opportuno evidenziare che gli interventi di seguito illustrati, anche alla luce della presentazione il 20 gennaio 2026 da parte della Commissione di un pacchetto di riforme destinato – tra l'altro – alla revisione integrale del *Cybersecurity Act*, sono stati elaborati con il fine principale di assicurare l'adeguamento dell'ordinamento interno al regolamento (UE) 2025/37 e di apportare minime modifiche alla normativa vigente volte a garantire la piena aderenza con l'intero sistema europeo di certificazione della cybersicurezza.

In particolare, il presente decreto legislativo intende apportare, da un lato, delle modifiche al decreto legislativo n. 123 del 2022 e al decreto legislativo 7 marzo 2005, n. 82 (in pieno esercizio del principio e criterio direttivo specifico di delega di cui alla lettera a), e, dall'altro, al decreto-legge n. 82 del 2021 (in attuazione del principio e criterio direttivo specifico di delega di cui alla lettera b).

Lo schema di decreto è inviato alle Camere ai sensi dell'articolo 31 della legge n. 234 del 2012, in forza del richiamo di cui all'articolo 1 della legge delega.

***

Il decreto legislativo si compone di **4 articoli**.

L'**articolo 1** reca le modifiche al decreto legislativo n. 123 del 2022 volte ad assicurare la corretta e integrale applicazione del regolamento (UE) 2019/881, anche con riguardo alle modifiche apportate dal regolamento (UE) 2025/37, in attuazione del principio e criterio direttivo specifico di cui alla lettera a) dell'articolo 16, comma 2, della legge delega.

In particolare, il **comma 1**, **lettera a)**, apporta modifiche all'articolo 3, comma 1, del decreto legislativo n. 123 del 2022, avente ad oggetto le definizioni, e nel dettaglio:

- al **numero 1)**, si introduce la lettera a-*bis*), che prevede la definizione di "servizio di sicurezza gestito", mutuandola da quanto previsto dal regolamento (UE) 37/2025;
- al **numero 2)**, si apporta una modifica alla definizione di "messa a disposizioni sul mercato", contenuta nella lettera d) del citato articolo 3 del decreto legislativo n. 123 del 2022, al fine di inserire il riferimento ai servizi di sicurezza gestiti;

- al **numero 3)**, si apporta una modifica alla definizione di “ritiro”, contenuta nella lettera f) del citato articolo 3 del decreto legislativo n. 123 del 2022, al fine di inserire il riferimento ai servizi di sicurezza gestiti;
- al **numero 4)**, si apporta una modifica alla definizione di “vigilanza del mercato”, contenuta nella lettera g) del citato articolo 3 del decreto legislativo n. 123 del 2022, al fine di specificare che l’attività di vigilanza è riferita anche ai servizi di sicurezza gestiti;
- al **numero 5)**, si apporta una modifica alla definizione di “dichiarazione UE di conformità”, contenuta nella lettera u) del citato articolo 3 del decreto legislativo n. 123 del 2022, al fine di inserire il riferimento ai servizi di sicurezza gestiti;
- al **numero 6)**, si apporta una modifica alla definizione di “certificato europeo di cybersicurezza”, contenuta nella lettera z) del citato articolo 3 del decreto legislativo n. 123 del 2022, al fine di inserire il riferimento ai servizi di sicurezza gestiti.

La **lettera b) del comma 1**, invece, reca modifiche all’articolo 5, del decreto legislativo n. 123 del 2022, relativo alla disciplina delle attività di vigilanza del mercato.

Nel dettaglio, la novella introdotta con il **numero 1)** della citata lettera b) incide sulla lettera b), del comma 4 del richiamato articolo 5, a mente del quale si prevede, tra i casi di revoca dei certificati non conformi alla normativa di riferimento, la revoca di un certificato con livello di affidabilità di base o sostanziale nel caso in cui il certificato non conforme sia relativo ad un prodotto TIC, servizio TIC o processo TIC che abbia comportato un concreto e dimostrato pregiudizio ad un servizio essenziale ai sensi dell’allegato II del decreto legislativo 18 maggio 2018, n. 65 e successive modificazioni o servizio di comunicazione elettronica ai sensi del decreto legislativo 1° agosto 2003, n. 259 e successive modificazioni o alla salute o all’incolumità personale.

La novella intende, da un lato, inserire tra i casi di revoca anche quelli dei certificati con livello di affidabilità di base o sostanziale relativi ai servizi di sicurezza gestiti (non contemplati dalla disciplina vigente) e, dall’altro, aggiornare i riferimenti normativi contenuti nella disposizione oggetto di modifica alla luce dell’evoluzione del quadro normativo di riferimento. A tale ultimo fine, viene inserito il riferimento ai soggetti essenziali di cui all’articolo 6, commi 1 e 2, del decreto legislativo 4 settembre 2024, n. 138 (di recepimento della direttiva NIS 2), nel novero dei quali sono ricondotti i prestatori di servizi essenziali indicati nell’allegato II dell’abrogato decreto legislativo n. 65 del 2018 (di recepimento della NIS 1) nonché i prestatori di servizi di comunicazione elettronica ai sensi del decreto legislativo 1° agosto 2003, n. 259 (cd. soggetti TELCO).

Al contempo, la modifica di cui al comma 1, lettera b), **numero 2)** del presente decreto legislativo interviene sul comma 5 del menzionato articolo 5 del decreto legislativo n. 123 del 2022, che disciplina le modalità di revoca per i casi stabiliti al citato comma 4 della medesima disposizione. Per quanto di interesse, la disposizione vigente prevede che nell'ipotesi di non conformità di un certificato di livello di base o sostanziale – relativo ora anche a un servizio di sicurezza gestito – l'organismo di valutazione della conformità che ha emesso il certificato non conforme debba revocarlo entro 5 giorni dalla richiesta in tal senso dell'Agenzia. In caso di inerzia dell'organismo di valutazione della conformità, spetta all'Agenzia, nell'esercizio di un potere sostitutivo, provvedere alla revoca del certificato non conforme nei successivi 5 giorni. La novella intende ottimizzare il procedimento appena descritto al fine di assicurare il rispetto dei termini richiamati, prevedendo, in caso di revoca del certificato da parte dell'organismo di valutazione della conformità, una contestuale comunicazione all'Agenzia.

Il comma 1, lettera b), **numero 3)**, dell'articolo in esame, invece, interviene sull'articolo 5, comma 6, del decreto legislativo n. 123 del 2022, il quale disciplina le modalità di gestione dei certificati non conformi che non sono direttamente revocati secondo le previsioni del comma 4. Invero, il citato comma 6 prevede che, in tali casi, l'Agenzia chiede all'organismo di valutazione della conformità di revocare il certificato o di ricondurlo a conformità entro 120 giorni, operando delle modifiche al certificato anche alla luce dell'eventuale integrazione dell'attività di valutazione. In caso di mancata revoca o riconduzione a conformità del certificato, il certificato stesso decade. Orbene, la modifica apportata prevede la possibilità per l'Agenzia di indicare un termine - anche inferiore a 120 giorni - per ricondurre a conformità il certificato. Tale novella, infatti, fonda la propria *ratio* sull'evidenza che non tutte le irregolarità necessitano di un termine così ampio (120 giorni) per essere sanate e, pertanto, si reputa necessario, al fine di ricondurre a conformità il certificato nel più breve termine possibile, prevedere anche la possibilità per l'autorità nazionale per la vigilanza del mercato (i.e. ACN) di indicare un termine proporzionato rispetto all'irregolarità riscontrata.

Infine, la modifica di cui al comma 1, lettera b), **numero 4)**, dell'articolo in esame è volto a correggere un mero errore materiale.

La **lettera c), del comma 1** dell'articolo in commento apporta delle modifiche all'articolo 6, comma 1, del decreto legislativo n. 123 del 2022, il quale definisce le modalità per l'emissione dei certificati di cybersicurezza a livello nazionale per i livelli di affidabilità elevato (art. 56, paragrafo 6, del regolamento (UE) 2019/881).

La modifica apportata mira, in primo luogo, a specificare che l'Agenzia, tramite l'Organismo di Certificazione della Sicurezza Informatica (OCSI), rilascia anche i certificati di cybersicurezza di livello di base o sostanziale,

assicurando la corretta e integrale applicazione del regolamento (UE) 2019/881.

In particolare, il regolamento CSA prevede, all'articolo 56, paragrafo 4), che gli organismi di valutazione della conformità rilasciano certificati europei della cybersicurezza con riferimento al livello di affidabilità di base o sostanziale. In deroga a tale previsione, il paragrafo 5) del medesimo articolo dispone che, in casi debitamente giustificati, un sistema europeo di certificazione della cybersicurezza può prevedere che i certificati emessi sulla base di tale sistema siano rilasciati solo da un ente pubblico.

Da tale deroga, si evince, a contrario, che il "regime ordinario" per il rilascio dei certificati europei della cybersicurezza con riferimento al livello di affidabilità di base o sostanziale non prevede alcuna restrizione, potendo rilasciare i menzionati certificati sia gli organismi di valutazione della conformità pubblici (come l'Agenzia) sia i privati. Tale interpretazione è stata, tra l'altro, confermata dai competenti uffici della Commissione europea nell'ambito di una interlocuzione informale a livello tecnico portata avanti dall'ACN.

In secondo luogo, la novella in esame corregge un mero errore materiale, prevedendo che gli esperti e i laboratori di prova abilitati di cui può avvalersi l'Agenzia per svolgere la propria attività di certificazione devono essere iscritti nell'elenco dei laboratori di prova e degli esperti per le attività di certificazione (e non nell'elenco dei laboratori di prova e degli esperti per le attività di vigilanza, come riportato nella formulazione attualmente vigente).

Il **comma 1, lettera d)**, dell'articolo in esame modifica l'articolo 7 del decreto legislativo n. 123 del 2022, il quale disciplina le modalità di rilascio e gestione delle dichiarazioni UE di conformità da parte dei fabbricanti o fornitori, in linea con l'articolo 55 del regolamento CSA.

In particolare, il comma 1 del menzionato articolo 7 stabilisce che i fabbricanti e fornitori di prodotti TIC, ai sensi dell'articolo 54, paragrafo 1, lettera e), del regolamento (UE) 2019/881, possono rilasciare dichiarazioni UE di conformità per dimostrare il rispetto dei requisiti tecnici previsti da un sistema di certificazione per il livello di affidabilità di base. Il comma 2, invece, prevede che i citati fabbricanti o fornitori deve rendere disponibile all'Agenzia la dichiarazione di conformità, la relativa documentazione e le altre informazioni pertinenti. La copia di una dichiarazione UE di conformità è trasmessa all'Agenzia e a ENISA.

Orbene, la novella in esame, ai **numeri 1) e 2)**, mira a estendere la disciplina appena richiamata ai servizi di sicurezza gestiti.

La **lettera e)**, del **comma 1**, dell'articolo in commento novella l'articolo 9, comma 3, del decreto legislativo n. 123 del 2022, il quale prevede la possibilità per l'Agenzia, in conformità all'articolo 57 del regolamento CSA e in assenza di un sistema europeo di certificazione, di introdurre dei sistemi di

certificazione nazionali della cybersicurezza per prodotti TIC, servizi TIC e processi TIC. La modifica in esame è volta a estendere la possibilità di adottare sistemi di certificazione nazionali della cybersicurezza anche per i servizi di sicurezza gestiti.

Al **comma 1, lettera f)**, dell'articolo in esame sono previste le modifiche all'articolo 10 del decreto legislativo n. 123 del 2022, il quale reca la disciplina del quadro sanzionatorio.

Nel dettaglio, per quanto concerne la modifica apportata al **numero 1)**, si intende effettuare un allineamento della disposizione concernente la disciplina del procedimento sanzionatorio con quella contenuta nel decreto-legge n. 82 del 2021.

Invero, l'articolo 17, comma 4-*quater*, del citato decreto-legge demanda a un regolamento – da adottare con decreto del Presidente del Consiglio dei ministri, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, sentito il Comitato interministeriale per la cybersicurezza e acquisito il parere delle competenti Commissioni parlamentari – la disciplina del procedimento sanzionatorio amministrativo dell'Agenzia e, in particolare, dei termini e delle modalità per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni di competenza dell'Agenzia ai sensi del presente decreto e delle altre disposizioni che assegnano poteri accertativi e sanzionatori all'Agenzia. La medesima disposizione prevede, inoltre, che nelle more dell'adozione di tale regolamento, ai procedimenti sanzionatori si applichino le disposizioni contenute nelle sezioni I e II del capo I della legge 24 novembre 1981, n. 689.

Tanto posto, stante la portata "orizzontale" della disposizione appena richiamata, la novella è volta a operare un coordinamento con la disciplina vigente, prevedendo che, anche con riferimento al procedimento sanzionatorio previsto dal decreto legislativo n. 123 del 2022, l'Agenzia operi sulla base del proprio regolamento e, nelle more della sua adozione, sulla base delle disposizioni contenute nelle sezioni I e II del capo I della legge n. 689 del 1981.

Le modifiche apportate dai numeri **2)**, **3)**, **4)** e **5)**, invece, mirano ad integrare le fattispecie sanzionabili previste, rispettivamente, dai commi 4, 5, 8 e 16 dell'articolo 10 del decreto legislativo n. 123 del 2022 con il riferimento ai servizi di sicurezza gestiti, in piena attuazione del principio e criterio specifico di delega di cui all'articolo 16, comma 2, lettera a), della legge delega.

Inoltre, il menzionato numero 5), prevede, in raccordo e in coerenza con la novella di cui alla lettera b), numero 1), del presente decreto legislativo, l'aggiornamento dei riferimenti normativi contenuti all'articolo 10, comma 16, del decreto legislativo n. 123 del 2022, sostituendo i rinvii all'abrogato decreto legislativo 18 maggio 2018, n. 65 (di recepimento della NIS 1) con

quelli al vigente decreto legislativo n. 138 del 2024 (di recepimento della NIS 2).

La **lettera g)**, del **comma 1**, dell'articolo in esame apporta una modifica all'articolo 13 del decreto legislativo n. 123 del 2022, che disciplina la destinazione dei proventi derivanti dalle attività dell'Agenzia. In particolare, il comma 1 del citato articolo 13 prevede che le attività di vigilanza, di certificazione, di autorizzazione, di abilitazione siano sottoposte a tariffa e che i relativi proventi siano 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, per incrementare la dotazione degli appositi capitoli dell'Agenzia. Il comma 3, del medesimo articolo, invece, prevede che gli introiti derivanti dalle sanzioni pecuniarie siano 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, per incrementare la dotazione degli appositi capitoli dell'Agenzia.

Al **numero 1)** la modifica interviene sul citato articolo 13, comma 1, del decreto legislativo n. 123 del 2022, al fine di individuare in modo più puntuale la posta contabile (ci si riferisce al capitolo di spesa di cui all'articolo 18, comma 1 del decreto-legge n. 82 del 2021) destinataria dei proventi derivanti dalle attività di vigilanza, di certificazione, di autorizzazione e di abilitazione svolte dall'Agenzia, a seguito dell'esperimento della prevista procedura di riassegnazione. Infatti, il decreto-legge istitutivo dell'Agenzia per la cybersicurezza nazionale prevede, all'articolo 18, l'istituzione, nello stato di previsione del Ministero dell'economia e delle finanze, di un apposito capitolo per la costituzione e l'espletamento dei compiti istituzionali conferiti alla citata Agenzia. Si evidenzia, al riguardo, che la modifica in parola uniforma la previsione alle disposizioni, che ugualmente autorizzano la riassegnazione di entrate al bilancio dell'Agenzia, quali l'articolo 18 del citato decreto-legge n. 82 del 2021 e l'articolo 38 del decreto legislativo n. 138 del 2024.

Al **numero 2)**, con le medesime finalità appena illustrate per la riformulazione di cui al numero 1), si interviene sul comma 3 del richiamato articolo 13 del decreto legislativo n. 123 del 2022. In questo caso, inoltre, si introduce, come ulteriore destinazione degli introiti derivanti dalle sanzioni pecuniarie, anche le attività di ricerca e formazione concernenti la certificazione della cybersicurezza dei già trattati servizi di sicurezza gestiti.

All'**articolo 2**, in attuazione del principio e criterio direttivo specifico di cui alla lettera a) dell'articolo 16, comma 2, della legge delega, apporta delle modifiche all'articolo 35, commi 4 e 5, del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale).

In particolare, il richiamato articolo 35 prevede:

- al comma 4, che i dispositivi sicuri di firma devono essere dotati di certificazione di sicurezza ai sensi dello schema nazionale di cui al comma 5;

- al comma 5, che la conformità ai requisiti di sicurezza dei dispositivi per la creazione di una firma elettronica qualificata o di un sigillo elettronico prescritti dall'Allegato II del regolamento (UE) n. 910/2014 (c.d. eIDAS) sia accertata, in Italia, dall'Organismo di certificazione della sicurezza informatica (OCSI) sulla base allo schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione, fissato con decreto del Presidente del Consiglio dei Ministri, o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con i Ministri delle comunicazioni, delle attività produttive e dell'economia e delle finanze. Tale schema nazionale può, inoltre, prevedere la valutazione e la certificazione relativamente ad ulteriori criteri europei ed internazionali, anche riguardanti altri sistemi e prodotti afferenti al settore suddetto.

Come noto, il decreto del Presidente del Consiglio dei ministri 30 ottobre 2003, recante "*Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art. 10, comma 1, del decreto legislativo 23 febbraio 2002, n. 10*", pubblicato sulla Gazzetta Ufficiale della Repubblica italiana n. 98 del 27 aprile 2004, ha previsto l'istituzione dell'Organismo di certificazione della sicurezza informatica (OCSI) nonché la definizione dello schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione (c.d. schema nazionale di certificazione).

L'articolo 57 del regolamento (UE) 2019/881 prevede che i sistemi nazionali di certificazione della cybersicurezza e le procedure correlate per i prodotti TIC, servizi TIC e processi TIC coperti da un sistema europeo di certificazione della cybersicurezza cessano di produrre effetti a decorrere dalla data stabilita nell'atto di esecuzione adottato a norma dell'articolo 49, paragrafo 7.

In attuazione del citato articolo 49, paragrafo 7, la Commissione ha adottato, come richiamato in premessa, il regolamento di esecuzione (UE) 2024/482, il quale, definendo il primo schema europeo di certificazione della cybersicurezza dei prodotti TIC, servizi TIC e processi TIC basato sui criteri comuni (EUCC), prevede, all'articolo 49, che tutti i sistemi nazionali di certificazione della cybersicurezza e le procedure correlate per i prodotti e i processi TIC contemplati dal predetto schema europeo di certificazione cessino di produrre effetti decorsi 12 mesi dall'entrata in vigore del regolamento di esecuzione (il regolamento, ai sensi dell'articolo 50, paragrafo 1), è entrato in vigore il 27 febbraio 2025).

Pertanto, a decorrere dal 27 febbraio 2026, lo schema nazionale di certificazione cesserà di produrre effetti.

Alla luce della ricostruzione fornita, la modifica contenuta all'**articolo 2, comma 1, numero 2),** del presente decreto legislativo risulta necessaria per garantire il coordinamento delle disposizioni settoriali vigenti con la normativa dettata dal *Cybersecurity Act* e dai relativi atti di esecuzione: in particolare, si prevede che 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 (UE) n. 910/2014 (c.d. eIDAS) sia accertata, a livello nazionale, dall'Organismo di certificazione della sicurezza informatica (OCSI), il quale opererà necessariamente sulla base dello schema europeo di certificazione della cybersicurezza. Si precisa che l'introduzione dell'acronimo "OCSI" costituisce una modifica di mero *drafting* volta a rendere inequivocabile la volontà di riferirsi all'Organismo istituito ai sensi del richiamato decreto del Presidente del Consiglio dei ministri 30 ottobre 2003.

Conseguentemente, l'**articolo 2, comma 1, numero 1)**, del presente decreto legislativo apporta una mera modifica di coordinamento, sostituendo il riferimento allo schema nazionale di per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione con quello all'articolo 30 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 (c.d. regolamento eIDAS), il quale reca la disciplina della certificazione dei dispositivi per la creazione di una firma elettronica qualificata. Appare opportuno evidenziare che, in attuazione del comma 4 del richiamato articolo 30 del regolamento eIDAS, la Commissione ha adottato la decisione di esecuzione n. 2016/650, del 25 aprile 2016, nel cui Allegato sono elencate le norme per valutare la sicurezza dei prodotti delle tecnologie dell'informazione applicabili alla certificazione dei dispositivi per la creazione di una firma elettronica qualificata o per la creazione di un sigillo elettronico qualificato: tali norme corrispondono ai criteri comuni (c.d. "*common criteria*") che sono alla base dell'EUCC (il sistema europeo di certificazione della cibersicurezza basato su criteri comuni, adottato con il richiamato regolamento di esecuzione (UE) 2024/482 della Commissione del 31 gennaio 2024.

L'**articolo 3** del decreto legislativo in esame reca le novelle al decreto-legge n. 82 del 2021, in applicazione del principio e criterio direttivo specifico di cui alla lettera b) dell'articolo 16 della legge delega, con il quale si conferisce una delega al Governo a modificare, in conformità agli articoli 56, comma 6, e 60 del *Cybersecurity Act*, l'articolo 7, comma 1, lettera e), numeri 1) e 2), del citato decreto-legge, con riferimento alle modalità di accreditamento, autorizzazione e delega degli organismi ivi previsti (Ministero della difesa e Ministero dell'interno).

Invero, l'attuale formulazione dell'articolo 7, comma 1, lettera e), del decreto-legge n. 82 del 2021, prevede che l'Agenzia (in qualità di NCCA - *National Cybersecurity Certification Authorities*):

"*1) accredita, ai sensi dell'articolo 60, paragrafo 1, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza;*

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 di cui al numero 1) della presente legge, al rilascio del certificato europeo di sicurezza cibernetica".

La modifica del menzionato articolo 7, comma 1, lettera e), è volta ad assicurare la piena conformità all'articolo 60 del regolamento CSA, il quale dispone:

- al paragrafo 1, che: "*Gli organismi di valutazione della conformità sono accreditati da organismi nazionali di accreditamento designati ai sensi del regolamento (CE) n. 765/2008 [*in Italia, Accredia[3]*]. Tale accreditamento è rilasciato solo se l'organismo di valutazione della conformità soddisfa i requisiti indicati nell'allegato del presente regolamento*";

- al paragrafo 3, che: "*Qualora i sistemi europei di certificazione della cibersicurezza stabiliscano requisiti specifici o supplementari a norma dell'articolo 54, paragrafo 1, lettera f), solo gli organismi di valutazione della conformità che soddisfano detti requisiti sono autorizzati dall'autorità nazionale di certificazione della cibersicurezza a svolgere i compiti previsti da tali sistemi*."

Pertanto, la novella, all'**articolo 3, comma 1,** del presente decreto legislativo chiarisce che le funzioni di accreditamento non sono espletate dall'ACN (in quanto ente non rientrante tra gli organismi nazionali di accreditamento designati ai sensi del regolamento (CE) n. 765/2008): la medesima Agenzia, invece, è deputata, in qualità di Autorità nazionale di certificazione della cybersicurezza, a rilasciare - ai sensi del richiamato articolo 60, paragrafo 3, del regolamento (UE) 2019/881 - l'autorizzazione agli organismi di valutazione della conformità che soddisfano i requisiti specifici o supplementari che un sistema europeo di certificazione della cybersicurezza stabilisce a norma dell'articolo 54, paragrafo 1, lettera f), del citato regolamento.

3 Accredia è l'ente designato dal Governo italiano, ai sensi del regolamento (CE) 765/2008, per valutare la competenza, l'imparzialità e la trasparenza degli Organismi di valutazione della conformità mediante il processo di accreditamento.

Posto che la citata autorizzazione permette di operare in specifici sistemi europei di certificazione della cybersicurezza (come, ad esempio, il sistema EUCC per prodotti TIC, servizi TIC e processi TIC, introdotto - come accennato - dal regolamento di esecuzione (UE) 2024/482 della Commissione), è stato eliminato il riferimento ai "*sistemi di rispettiva competenza*", al fine di coordinare la disposizione in esame con il dettato europeo.

Alla luce della ricostruzione fornita, il **numero 1)**, del **comma 1**, dell'articolo 3 del decreto legislativo in esame sostituisce l'articolo 7, comma 1, lettera e), numero 1) del decreto-legge n. 82 del 2021 al fine di prevedere che l'Agenzia autorizzi, ai sensi dell'articolo 60, paragrafo 3, del regolamento (UE) 2019/881, 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.

Il **comma 1, numero 2)**, invece, in stretta correlazione con la modifica appena illustrata e al fine di assicurare una piena portata applicativa all'articolo 7, comma 1, lettera e), numero 2) del decreto-legge n. 82 del 2021, precisa che le strutture dei richiamati Ministeri sono accreditate ai sensi dell'articolo 60, paragrafo 1, del regolamento (UE) 2019/881: in particolare, per poter esercitare la delega per l'emissione di certificati di cybersicurezza con livello di affidabilità elevato (di cui all'articolo 56, paragrafo 6, lettera b), del regolamento (UE) 2019/881) le strutture dei due Ministeri devono essere accreditate, posto che l'articolo 60, paragrafo 1, del citato regolamento prevede che "*Gli organismi di valutazione della conformità sono accreditati da organismi nazionali di accreditamento designati ai sensi del regolamento (CE) n. 765/2008*".

L'**articolo 4** del decreto legislativo in esame reca, infine, in stretta aderenza con quanto previsto dall'articolo 16, comma 3, della legge delega, la clausola di invarianza finanziaria.

TABELLA DI CONCORDANZA

(comma 2, art. 31 della L. 234/2012 e s.m.i.)

Attuazione nazionale del regolamento (UE) 2025/37

delega di cui all'articolo 16 della legge 17 marzo 2026, n. 36

"Schema di decreto legislativo 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"

Premessa

Di seguito si riporta la tabella di concordanza ai sensi dell'articolo 31, comma 2, della legge 24 dicembre 2012, n. 234.

Non trattandosi del recepimento di una direttiva europea, bensì dell'adeguamento della normativa nazionale ad un regolamento europeo, solo alcuni articoli regolamento (UE) 2025/37 richiedono adempimenti nazionali, essendo il richiamato regolamento già entrato in vigore in tutti gli Stati membri dal 4 febbraio 2025 ed operativo per le molte parti.

Posto che il regolamento (UE) 2025/37 apporta delle modifiche al regolamento (UE) 2019/881, lo schema di decreto legislativo in esame intende apportare delle modifiche al decreto legislativo 3 agosto 2022 n. 123, il quale reca le "*Norme di adeguamento della normativa nazionale alle disposizioni del Titolo III «Quadro di certificazione della cibersicurezza» 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 cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»)*".

Pertanto, nella successiva tabella di concordanza si presentano per ogni articolo del regolamento (UE) 2025/37 le corrispondenti modifiche necessarie alla normativa nazionale (*i.e.* al decreto legislativo n. 123 del 2022) per realizzare i necessari adempimenti nazionali.

Tali modifiche risultano essere attuativi del criterio e principio direttivo di cui alla all'articolo 16, comma 2, lettera a) della legge 17 marzo 2026, n. 36, a mente del quale: "*apportare alla normativa vigente e, in particolare, al decreto legislativo 3 agosto 2022, n. 123, tutte le modifiche e le integrazioni necessarie ad assicurare la corretta e integrale applicazione del regolamento (UE) 2019/881, 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* ".

Articoli e paragrafi del Regolamento (UE) 2025/37	**Adeguamento normativa interna – modifiche al D.Lgs. 123/2022**
Articolo 1 **Modifiche del regolamento (UE) 2019/881** Il regolamento (UE) 2019/881 è così modificato:	
1) all'articolo 1, paragrafo 1, primo comma, la lettera b) è sostituita dalla seguente: «b) un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza nell'Unione dei prodotti TIC, dei servizi TIC, dei processi TIC e dei servizi di sicurezza gestiti, oltre che al fine di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cibersicurezza nell'Unione.»;	**La disposizione ha una portata generale e permea tutte le modifiche di seguito riportate in quanto introduce i servizi di sicurezza gestiti nel quadro dei sistemi europei di certificazione della cibersicurezza**
2) l'articolo 2 è così modificato: a) i punti 9), 10) e 11) sono sostituiti dai seguenti: «9) "sistema europeo di certificazione della cibersicurezza": una serie completa di regole, requisiti tecnici, norme e procedure stabiliti a livello di Unione e che si applicano alla certificazione o alla valutazione della conformità di specifici prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti; 10) "sistema nazionale di certificazione della cibersicurezza": una serie completa di regole, requisiti	9) "sistema europeo di certificazione della cibersicurezza": non sono richiesti adempimenti normativi per gli Stati membri 10) "sistema nazionale di certificazione della cibersicurezza": non sono richiesti adempimenti

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
tecnici, norme e procedure elaborati e adottati da un'autorità pubblica nazionale e che si applicano alla certificazione o alla valutazione della conformità dei prodotti TIC, dei servizi TIC, dei processi TIC o dei servizi di sicurezza gestiti che rientrano nell'ambito di applicazione del sistema specifico; 11) "certificato europeo di cibersicurezza": un documento rilasciato dall'organismo pertinente 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 di sicurezza specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;»; b) è inserito il punto seguente: «14 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 cibersicurezza, ad esempio servizi di gestione degli incidenti, test di penetrazione, audit di sicurezza e consulenza, tra cui consulenza specialistica, relativa all'assistenza tecnica;»; c) i punti 20), 21) e 22) sono sostituiti dai seguenti: «20) "specifica tecnica": un documento che prescrive i requisiti tecnici che un prodotto TIC, un servizio TIC, un processo TIC o un servizio di sicurezza gestito deve soddisfare o le relative procedure di valutazione della conformità; 21) "livello di affidabilità": base per la fiducia nel fatto che un prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito soddisfa i requisiti di sicurezza di uno specifico sistema europeo di	normativi per gli Stati membri 11) "certificato europeo di cibersicurezza": **necessita di adeguamento l'articolo 3, comma 1, lett. z) del d.lgs. 123/2022** 14 bis) "servizio di sicurezza gestito": **necessita di adeguamento l'articolo 3, comma 1, del d.lgs. 123/2022** 20) "specifica tecnica": non sono richiesti adempimenti normativi per gli Stati membri 21) "livello di affidabilità": non sono richiesti adempimenti normativi per gli Stati membri 22) "autovalutazione di conformità": **necessita di**

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
certificazione della cibersicurezza e indica il livello al quale un prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito è stato valutato, ma di per sé non misura la sicurezza del prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito interessato; 22) “autovalutazione di conformità”: un'azione effettuata da un fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti che valuta se tali prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti soddisfino i requisiti di uno specifico sistema europeo di certificazione della cibersicurezza.»;	**adeguamento l’articolo 3, comma 1, lett. u), del d.lgs. 123/2022**
3) all'articolo 4, il paragrafo 6 è sostituito dal seguente: «6. L'ENISA promuove l'uso della certificazione europea della cibersicurezza, con l'obiettivo di evitare la frammentazione del mercato interno. L'ENISA contribuisce all'istituzione e al mantenimento di un apposito quadro europeo di certificazione della cibersicurezza, conformemente al titolo III del presente regolamento, al fine di aumentare la trasparenza dei prodotti TIC, dei servizi TIC, dei processi TIC e dei servizi di sicurezza gestiti in termini di cibersicurezza, rafforzando in tal modo la fiducia nel mercato unico digitale e la sua competitività.»;	Non sono richiesti adempimenti normativi per gli Stati membri
4) l'articolo 8 è così modificato: a) il paragrafo 1 è così modificato: i) la frase introduttiva è sostituita dalla seguente: «1. L'ENISA sostiene e promuove lo sviluppo e l'attuazione della politica dell'Unione in materia di certificazione della cibersicurezza dei prodotti TIC, dei servizi TIC, dei processi TIC e dei servizi di sicurezza	Non sono richiesti adempimenti normativi per gli Stati membri

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
gestiti, come stabilito al titolo III del presente regolamento: »; ii) la lettera b) è sostituita dalla seguente: «b) preparando proposte di sistemi europei di certificazione della cibersicurezza (proposte di sistemi) per prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti conformemente all'articolo 49;»; b) il paragrafo 3 è sostituito dal seguente: «3. L'ENISA elabora e pubblica orientamenti e sviluppa buone pratiche in merito ai requisiti di cibersicurezza per i prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti, in cooperazione con le autorità nazionali di certificazione della cibersicurezza e con il settore in modo formale, strutturato e trasparente.»; c) il paragrafo 5 è sostituito dal seguente: «5. L'ENISA facilita la definizione e l'adozione di norme europee e internazionali in materia di gestione dei rischi e di sicurezza dei prodotti TIC, dei servizi TIC, dei processi TIC e dei servizi di sicurezza gestiti.»;	
5) l'articolo 46 è sostituito dal seguente: «Articolo 46 Quadro europeo di certificazione della cibersicurezza 1. È istituito il quadro europeo di certificazione della cibersicurezza al fine di migliorare le condizioni di funzionamento del mercato interno aumentando il livello di cibersicurezza all'interno dell'Unione e rendendo possibile, a livello di Unione, un approccio armonizzato dei sistemi europei di certificazione della cibersicurezza allo scopo di creare un mercato unico digitale per i prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti. 2. Il quadro europeo di certificazione della	Non sono richiesti adempimenti normativi per gli Stati membri

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
cibersicurezza prevede un meccanismo volto a istituire sistemi europei di certificazione della cibersicurezza e ad attestare che i prodotti TIC, i servizi TIC e i processi TIC valutati nell'ambito di tali sistemi siano conformi a determinati requisiti di sicurezza al fine di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, servizi e processi o accessibili tramite essi per tutto il loro ciclo di vita. Esso attesta, inoltre, che i servizi di sicurezza gestiti valutati nell'ambito di tali sistemi sono conformi a determinati requisiti di sicurezza ai fini della protezione della disponibilità, dell'autenticità, dell'integrità e della riservatezza dei dati consultati, trattati, conservati o trasmessi in relazione alla prestazione di tali servizi, e che tali servizi sono forniti continuamente con la competenza, la perizia e l'esperienza richieste da personale avente un livello sufficiente e adeguato di conoscenze tecniche pertinenti e integrità professionale.»;	
6) l'articolo 47 è così modificato: a) il paragrafo 2 è sostituito dal seguente: «2. Il programma di lavoro progressivo dell'Unione include in particolare un elenco di prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti, o delle relative categorie, che possono beneficiare dell'inclusione nell'ambito di applicazione di un sistema europeo di certificazione della cibersicurezza.»; b) il paragrafo 3 è così modificato: i) la frase introduttiva è sostituita dalla seguente: «3. L'inclusione, nel programma di lavoro progressivo dell'Unione, di specifici prodotti TIC, servizi TIC,	Non sono richiesti adempimenti normativi per gli Stati membri

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
processi TIC o servizi di sicurezza gestiti, o delle relative categorie, è giustificata sulla base di una o più delle seguenti motivazioni: »; ii) la lettera a) è sostituita dalla seguente: «a) la disponibilità e lo sviluppo di sistemi nazionali di certificazione della cibersicurezza relativi a specifiche categorie di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti e in particolare in relazione al rischio di frammentazione;»; iii) è inserita la lettera seguente: «c bis) gli sviluppi tecnologici nonché la disponibilità e lo sviluppo di sistemi internazionali di certificazione della cibersicurezza e di norme internazionali e norme utilizzate dall'industria;»;	
7) l'articolo 49 è così modificato: a) i paragrafi da 1a 4 sono sostituiti dai seguenti: «1. A seguito di una richiesta della Commissione a norma dell'articolo 48, l'ENISA prepara una proposta di sistema che soddisfi i requisiti applicabili di cui agli articoli 51, 51 bis, 52 e 54. 2. A seguito di una richiesta dell'ECCG a norma dell'articolo 48, paragrafo 2, l'ENISA può preparare una proposta di sistema che soddisfi i requisiti applicabili di cui agli articoli 51, 51 bis, 52 e 54. Qualora respinga tale richiesta, l'ENISA motiva il proprio rifiuto. Ogni decisione di rifiuto della richiesta è presa dal consiglio di amministrazione. 3. In sede di preparazione di una proposta di sistema, l'ENISA consulta tempestivamente tutti i pertinenti portatori di interessi mediante un processo di consultazione formale, aperto, trasparente e inclusivo. Quando trasmette la proposta di sistema alla	Non sono richiesti adempimenti normativi per gli Stati membri

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
Commissione a norma del paragrafo 6, l'ENISA fornisce informazioni sulle modalità con cui ha si è conformata a tale paragrafo. 4. Per ciascuna proposta di sistema, l'ENISA istituisce un gruppo di lavoro ad hoc in conformità dell'articolo 20, paragrafo 4, con l'obiettivo di fornire all'ENISA consulenza e competenze specifiche. Tali gruppi di lavoro ad hoc comprendono, se del caso e fatte salve le procedure e la discrezionalità previste dall'articolo 20, paragrafo 4, esperti delle amministrazioni pubbliche degli Stati membri, delle istituzioni, degli organi e degli organismi dell'Unione, nonché del settore privato.»; b) il paragrafo 7 è sostituito dal seguente: «7. La Commissione, sulla base della proposta di sistema preparata dall'ENISA, può adottare atti di esecuzione, prevedendo un sistema europeo di certificazione della cibersicurezza per i prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti che soddisfa i requisiti pertinenti di cui agli articoli 51, 51 bis, 52 e 54. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 66, paragrafo 2.»;	
8) è inserito l'articolo seguente: «Articolo 49 bis Informazione e consultazione sui sistemi europei di certificazione della cibersicurezza 1. La Commissione rende pubbliche le informazioni concernenti la sua richiesta all'ENISA relativa alla preparazione di una proposta di sistema o alla revisione di un sistema europeo di certificazione della cibersicurezza esistente di cui all'articolo 48. 2. Nel corso della preparazione di una proposta di	Non sono richiesti adempimenti normativi per gli Stati membri

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
sistema da parte dell'ENISA a norma dell'articolo 49, il Parlamento europeo, il Consiglio o entrambi possono chiedere alla Commissione, in qualità di presidente dell'ECCG, e all'ENISA di presentare, su base trimestrale, le pertinenti informazioni relative a un progetto di proposta di sistema. Su richiesta del Parlamento europeo o del Consiglio, l'ENISA, d'intesa con la Commissione e fatto salvo l'articolo 27, può mettere a disposizione del Parlamento europeo e del Consiglio le parti pertinenti di un progetto di proposta di sistema con modalità adeguate al livello di riservatezza richiesto e, se del caso, limitate. 3. Al fine di rafforzare il dialogo tra le istituzioni dell'Unione e di contribuire a un processo di consultazione formale, aperto, trasparente e inclusivo, il Parlamento europeo, il Consiglio o entrambi possono invitare la Commissione e l'ENISA a discutere questioni relative al funzionamento dei sistemi europei di certificazione della cibersicurezza per prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti. 4. Nel valutare il presente regolamento a norma dell'articolo 67, la Commissione tiene conto, se del caso, degli elementi derivanti dai pareri espressi dal Parlamento europeo e dal Consiglio sulle questioni di cui al paragrafo 3 del presente articolo.»;	
9) l'articolo 51 è così modificato: a) il titolo è sostituito dal seguente: «Obiettivi di sicurezza dei sistemi europei di certificazione della cibersicurezza per i prodotti TIC, i servizi TIC e i processi TIC»; b) la frase introduttiva è sostituita dalla seguente: «I sistemi europei di certificazione della cibersicurezza	Non sono richiesti adempimenti normativi per gli Stati membri

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
per i prodotti TIC, i servizi TIC o i processi TIC sono progettati per conseguire, a seconda del caso, almeno gli obiettivi di sicurezza seguenti: »;	
10) è inserito l'articolo seguente: «Articolo 51 bis Obiettivi di sicurezza dei sistemi europei di certificazione della cibersicurezza per i servizi di sicurezza gestiti I sistemi europei di certificazione della cibersicurezza per i servizi di sicurezza gestiti sono progettati per conseguire, se del caso, almeno gli obiettivi di sicurezza seguenti: a) che i servizi di sicurezza gestiti siano forniti con la competenza, la perizia e l'esperienza richieste e il personale responsabile della prestazione di tali servizi possieda un livello sufficiente e adeguato di conoscenze e competenze tecniche nel settore specifico, un'esperienza sufficiente e appropriata e la massima integrità professionale; b) che il fornitore predisponga procedure interne appropriate affinché i servizi di sicurezza gestiti forniti abbiano sempre un livello di qualità sufficiente e adeguato; c) che i dati consultati, conservati, trasmessi o altrimenti trattati in relazione alla fornitura dei servizi di sicurezza gestiti siano protetti contro l'accesso, l'archiviazione, la divulgazione, la distruzione o altro tipo di trattamento, accidentali o non autorizzati, la perdita o l'alterazione o la mancanza di disponibilità; d) che la disponibilità dei dati, dei servizi e delle	Non sono richiesti adempimenti normativi per gli Stati membri

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
funzioni e l'accesso agli stessi siano ripristinati in modo tempestivo in caso di incidente fisico o tecnico; e) che le persone, i programmi o le macchine autorizzati possano accedere esclusivamente ai dati, ai servizi o alle funzioni per i quali dispongono dei diritti di accesso; f) che sia conservata una registrazione, disponibile per la valutazione, dei dati, dei servizi o delle funzioni per i quali è stato effettuato l'accesso, e che sono stati utilizzati o altrimenti trattati, in quale momento e da chi; g) che i prodotti TIC, i servizi TIC e i processi TIC avviati nella fornitura dei servizi di sicurezza gestiti siano sicuri fin dalla progettazione e per impostazione predefinita e, se del caso, includano gli ultimi aggiornamenti connessi alla sicurezza e non contengano vulnerabilità note.»;	
11) l'articolo 52 è così modificato: a) il paragrafo 1 è sostituito dal seguente: «1. I sistemi europei di certificazione della cibersicurezza possono specificare per i prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti uno o più dei livelli di affidabilità seguenti: “di base”, “sostanziale” o “elevato”. Il livello di affidabilità è commisurato al livello del rischio associato al previsto uso del prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito, in termini di probabilità e impatto di un incidente.»; b) il paragrafo 3 è sostituito dal seguente: «3. I requisiti di sicurezza corrispondenti a ogni livello di affidabilità sono indicati nel sistema europeo di certificazione della cibersicurezza pertinente, comprese le corrispondenti funzionalità di sicurezza e il rigore e la	Non sono richiesti adempimenti normativi per gli Stati membri

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
specificità corrispondenti della valutazione a cui deve essere sottoposto il prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito.»; c) i paragrafi 5, 6 e 7 sono sostituiti dai seguenti: «5. Un certificato europeo di cibersicurezza o una dichiarazione UE di conformità che si riferisca al livello di affidabilità "di base" assicura che i prodotti TIC, i servizi TIC, i processi TIC o i servizi di sicurezza gestiti per i quali sono rilasciati tale certificato o tale dichiarazione UE di conformità rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi di base noti di incidenti e attacchi informatici. Le attività di valutazione da intraprendere comprendono almeno un riesame della documentazione tecnica. Qualora tale riesame non sia appropriato, si ricorre ad attività di valutazione sostitutive di effetto equivalente. 6. Un certificato europeo di cibersicurezza che si riferisca al livello di affidabilità "sostanziale" assicura che i prodotti TIC, i servizi TIC, i processi TIC o i servizi di sicurezza gestiti per i quali è rilasciato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi noti connessi alla cibersicurezza e i rischi di incidenti e di attacchi informatici causati da soggetti dotati di abilità e risorse limitate. Le attività di valutazione da intraprendere comprendono almeno le seguenti: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note e un test per dimostrare che i prodotti TIC, i servizi TIC, i processi TIC o i servizi di sicurezza gestiti attuano	

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
correttamente le necessarie funzionalità di sicurezza. Qualora tali attività di valutazione non siano appropriate, si ricorre ad attività di valutazione sostitutive di effetto equivalente. 7. Un certificato europeo di cibersicurezza che si riferisca al livello di affidabilità "elevato" assicura che i prodotti TIC, i servizi TIC, i processi TIC o i servizi di sicurezza gestiti per i quali è rilasciato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo il rischio di attacchi informatici avanzati commessi da attori che dispongono di abilità e risorse significative. Le attività di valutazione da intraprendere comprendono almeno le seguenti: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note, un test per dimostrare che i prodotti TIC, i servizi TIC, i processi TIC o i servizi di sicurezza gestiti attuano correttamente le necessarie funzionalità di sicurezza, allo stato tecnologico più avanzato, e una valutazione della loro resistenza agli attacchi commessi da soggetti qualificati mediante test di penetrazione. Qualora tali attività di valutazione non siano appropriate, si ricorre ad attività sostitutive di effetto equivalente.»;	
12) all'articolo 53, i paragrafi 1, 2 e 3 sono sostituiti dai seguenti: «1. Un sistema europeo di certificazione della cibersicurezza può consentire un'autovalutazione della conformità sotto la sola responsabilità del fabbricante o del fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti. L'autovalutazione della conformità è consentita unicamente in relazione ai	par. 1 e 2: **necessita di adeguamento l'articolo 7, comma 1, del d.lgs. 123/2022**

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
prodotti TIC, ai servizi TIC, ai processi TIC o ai servizi di sicurezza gestiti che presentano un basso rischio corrispondente al livello di affidabilità “di base”. 2. Il fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti può rilasciare una dichiarazione UE di conformità in cui afferma che è stato dimostrato il rispetto dei requisiti previsti nel sistema. Rilasciando tale dichiarazione, il fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti si assume la responsabilità della conformità del prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito ai requisiti previsti in tale sistema. 3. Il fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti rende disponibile all'autorità nazionale di certificazione della cibersicurezza designata a norma dell'articolo 58, per il periodo stabilito nel corrispondente sistema europeo di certificazione della cibersicurezza, la dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti relative alla conformità al sistema dei prodotti TIC, dei servizi TIC, dei processi TIC o dei servizi di sicurezza gestiti. Una copia della dichiarazione UE di conformità è trasmessa all'autorità nazionale di certificazione della cibersicurezza e all'ENISA.»;	par. 3: **necessita di adeguamento l’articolo 7, comma 2, del d.lgs. 123/2022**

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
13) all'articolo 54, il paragrafo 1 è così modificato: a) la lettera a) è sostituita dalla seguente: «a) l'oggetto e l'ambito di applicazione del sistema di certificazione, compresi il tipo o le categorie di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti coperti;»;	a) la lettera a): non sono richiesti adempimenti normativi per gli Stati membri
b) la lettera g) è sostituita dalla seguente: «g) i criteri e i metodi di valutazione specifici da utilizzare, compresi i tipi di valutazione, al fine di dimostrare che gli obiettivi di sicurezza di cui agli articoli 51 e 51 bis sono stati conseguiti;»;	b) la lettera g): non sono richiesti adempimenti normativi per gli Stati membri
c) la lettera j) è sostituita dalla seguente: «j) le regole per il controllo della conformità dei prodotti TIC, dei servizi TIC, dei processi TIC o dei servizi di sicurezza gestiti ai requisiti dei certificati europei di cibersicurezza o delle dichiarazioni UE di conformità, compresi i meccanismi per dimostrare il mantenimento della conformità ai requisiti di cibersicurezza specificati;»;	c) la lettera j): non sono richiesti adempimenti normativi per gli Stati membri
d) la lettera l) è sostituita dalla seguente: «l) le regole riguardanti le conseguenze per i prodotti TIC, i servizi TIC, i processi TIC o i servizi di sicurezza gestiti che sono stati certificati o per i quali è stata rilasciata una dichiarazione UE di conformità ma che non sono conformi ai requisiti del sistema;»;	d) la lettera l): **necessita di adeguamento l'articolo 5, commi 4 e 5, del d.lgs. 123/2022**
e) la lettera o) è sostituita dalla seguente: «o) l'individuazione dei sistemi nazionali o internazionali di certificazione della cibersicurezza relativi allo stesso tipo o alle stesse categorie di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti, requisiti di sicurezza, criteri e metodi di valutazione nonché livelli di affidabilità;»;	e) la lettera o): non sono richiesti adempimenti normativi per gli Stati membri
	f) la lettera q): non sono richiesti adempimenti normativi per gli Stati membri

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
f) la lettera q) è sostituita dalla seguente: «q) il periodo di disponibilità della dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti che devono essere rese disponibili dal fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti;»;	
14) l'articolo 56 è così modificato: a) il paragrafo 1 è sostituito dal seguente: «1. I prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti certificati ricorrendo a un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 49 sono considerati conformi ai requisiti di tale sistema.»; b) il paragrafo 3 è così modificato: i) il primo comma è sostituito dal seguente: «La Commissione valuta periodicamente l'efficacia e l'utilizzo dei sistemi europei di certificazione della cibersicurezza adottati e l'eventuale necessità di rendere obbligatorio uno specifico sistema europeo di certificazione della cibersicurezza mediante pertinenti disposizioni di diritto dell'Unione al fine di garantire l'opportuno livello di cibersicurezza nell'Unione dei prodotti TIC, dei servizi TIC, dei processi TIC e, a decorrere dal 4 febbraio 2025, dei servizi di sicurezza gestiti e migliorare il funzionamento del mercato interno. La prima valutazione di questo genere è effettuata entro il 31 dicembre 2023 e le successive valutazioni sono effettuate almeno ogni due anni. Sulla base dei risultati di tali valutazioni, la Commissione individua i prodotti TIC, i servizi TIC, i processi TIC e i	a) il paragrafo 1: non sono richiesti adempimenti normativi per gli Stati membri b) il paragrafo 3: non sono richiesti adempimenti normativi per gli Stati membri

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
servizi di sicurezza gestiti coperti da un sistema di certificazione esistente che devono rientrare in un sistema obbligatorio di certificazione.»; ii) il terzo comma è così modificato: - la lettera a) è sostituita dalla seguente: «a) prende in considerazione l'impatto delle misure sui fabbricanti o fornitori di tali prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti e sugli utenti in termini di costi di tali misure nonché i benefici sociali o economici derivanti dal previsto aumento del livello di sicurezza per i prodotti TIC, i servizi TIC, i processi TIC o i servizi di sicurezza gestiti in questione;»; - la lettera d) è sostituita dalla seguente: «d) prende in considerazione le scadenze di attuazione e le misure transitorie e i periodi di transizione, in particolare con riferimento al possibile impatto delle misure sui fabbricanti o fornitori di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti, compresi gli interessi e i fabbisogni specifici delle PMI, incluse le microimprese;»; c) i paragrafi 7 e 8 sono sostituiti dai seguenti: «7. La persona fisica o giuridica che presenta i prodotti TIC, i servizi TIC, i processi TIC o i servizi di sicurezza gestiti per la certificazione mette a disposizione dell'autorità nazionale di certificazione della cibersicurezza designata a norma dell'articolo 58, qualora tale autorità sia l'organismo che rilascia il certificato europeo di cibersicurezza, o dell'organismo di valutazione della conformità di cui all'articolo 60 tutte le informazioni necessarie a espletare la certificazione. 8. Il titolare di un certificato europeo di cibersicurezza	c) i paragrafi 7 e 8: non sono richiesti adempimenti normativi per gli Stati membri

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
informa l'autorità o l'organismo di cui al paragrafo 7 delle eventuali vulnerabilità o irregolarità successivamente rilevate in relazione alla sicurezza dei prodotti TIC, dei servizi TIC, dei processi TIC o dei servizi di sicurezza gestiti certificati che possono incidere sulla conformità ai requisiti relativi alla certificazione. Tale autorità o organismo trasmette tali informazioni senza indebiti ritardi all'autorità nazionale di certificazione della cibersicurezza interessata.»;	
15) all'articolo 57, i paragrafi 1 e 2 sono sostituiti dai seguenti: «1. Fatto salvo il paragrafo 3 del presente articolo, i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti coperti da un sistema europeo di certificazione della cibersicurezza cessano di produrre effetti a decorrere dalla data stabilita nell'atto di esecuzione adottato a norma dell'articolo 49, paragrafo 7. I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti non coperti da un sistema europeo di certificazione della cibersicurezza restano in vigore. 2. Gli Stati membri non introducono nuovi sistemi nazionali di certificazione della cibersicurezza per prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti già coperti da un sistema europeo di certificazione della cibersicurezza in vigore.»;	**necessita di adeguamento l'articolo 9, comma 3, del d.lgs. 123/2022**

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
16) l'articolo 58 è così modificato: a) il paragrafo 7 è così modificato: i) le lettere a) e b) sono sostituite dalle seguenti: «a) supervisionano e fanno applicare le regole previste nei sistemi europei di certificazione della cibersicurezza a norma dell'articolo 54, paragrafo 1, lettera j), per il controllo della conformità dei prodotti TIC, dei servizi TIC, dei processi TIC e dei servizi di sicurezza gestiti ai requisiti dei certificati europei di cibersicurezza rilasciati nei rispettivi territori, in cooperazione con altre autorità di vigilanza del mercato competenti; b) controllano la conformità agli obblighi e fanno applicare gli obblighi che incombono ai fabbricanti o ai fornitori di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti che sono stabiliti nei rispettivi territori e che effettuano un'autovalutazione della conformità, e in particolare controllano la conformità agli obblighi e fanno applicare gli obblighi incombenti a tali fabbricanti o fornitori di cui all'articolo 53, paragrafi 2 e 3, e nel corrispondente sistema europeo di certificazione della cibersicurezza;»; ii) la lettera h) è sostituita dalla seguente: «h) cooperano con le altre autorità nazionali di certificazione della cibersicurezza o con altre autorità pubbliche, anche mediante lo scambio di informazioni sugli eventuali prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti non conformi ai requisiti del presente regolamento o ai requisiti di specifici sistemi europei di certificazione della cibersicurezza; e»; b) il paragrafo 9 è sostituito dal seguente: «9. Le autorità nazionali di certificazione della cibersicurezza cooperano tra di loro e con la	Non sono richiesti adempimenti normativi per gli Stati membri

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
Commissione, in particolare scambiandosi informazioni, esperienze e buone pratiche per quanto concerne la certificazione della cibersicurezza e le questioni tecniche riguardanti la cibersicurezza di prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti.»;	
17) all'articolo 59, paragrafo 3, le lettere b) e c) sono sostituite dalle seguenti: «b) le procedure di supervisione e applicazione delle regole per il controllo della conformità dei prodotti TIC, dei servizi TIC, dei processi TIC e dei servizi di sicurezza gestiti con i certificati europei di cibersicurezza a norma dell'articolo 58, paragrafo 7, lettera a); c) le procedure di monitoraggio e applicazione degli obblighi che incombono ai fabbricanti o ai fornitori di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti a norma dell'articolo 58, paragrafo 7, lettera b);»;	Non sono richiesti adempimenti normativi per gli Stati membri
18) all'articolo 67, i paragrafi 2 e 3 sono sostituiti dai seguenti: «2. La valutazione esamina inoltre l'impatto, l'efficacia e l'efficienza delle disposizioni del titolo III del presente regolamento, incluse le procedure che portano all'adozione dei sistemi europei di certificazione della cibersicurezza e le loro basi probatorie, per quanto riguarda gli obiettivi di garantire un livello adeguato di cibersicurezza nell'Unione dei prodotti TIC, dei servizi TIC, dei processi TIC e dei servizi di sicurezza gestiti e di migliorare il funzionamento del mercato interno.	Non sono richiesti adempimenti normativi per gli Stati membri

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
3. La valutazione esamina se siano necessari requisiti essenziali di cibersicurezza per l'accesso al mercato interno onde impedire l'ingresso nel mercato interno di prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti che non rispettano i requisiti di base in materia di cibersicurezza.».	
19) l'allegato è modificato conformemente all'allegato del presente regolamento.	Non sono richiesti adempimenti normativi per gli Stati membri
Articolo 2 **Entrata in vigore**	
Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea. Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.	Non sono richiesti adempimenti normativi per gli Stati membri
Allegato **L'allegato del regolamento (UE) 2019/881 è così modificato:**	
1) i punti da 2 a 5 sono sostituiti dai seguenti: «2. L'organismo di valutazione della conformità è un organismo terzo, indipendente dall'organizzazione o dai prodotti TIC, dai servizi TIC, dai processi TIC o dai servizi di sicurezza gestiti che valuta. 3. Un organismo appartenente a un'associazione d'imprese o a una federazione professionale che rappresenta imprese coinvolte nella progettazione, nella fabbricazione, nella fornitura, nell'assemblaggio, nell'utilizzo o nella manutenzione dei prodotti TIC, dei servizi TIC, dei processi TIC o dei servizi di sicurezza gestiti che valuta può essere ritenuto un organismo di	Non sono richiesti adempimenti normativi per gli Stati membri

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
valutazione della conformità, a condizione che siano dimostrate la sua indipendenza e l'assenza di qualsiasi conflitto di interesse. 4. Gli organismi di valutazione della conformità, i loro alti dirigenti e le persone addette alla valutazione della conformità non sono né il progettista, né il fabbricante, né il fornitore, né l'installatore, né l'acquirente, né il proprietario, né l'utilizzatore, né il responsabile della manutenzione del prodotto TIC, del servizio TIC, del processo TIC o del servizio di sicurezza gestito sottoposto a valutazione, né il rappresentante autorizzato di uno di questi soggetti. Tale divieto non preclude l'uso dei prodotti TIC valutati che sono necessari per il funzionamento dell'organismo di valutazione della conformità o il loro uso per scopi privati. 5. Gli organismi di valutazione della conformità, i loro alti dirigenti e le persone addette alla valutazione della conformità non intervengono direttamente nella progettazione, fabbricazione o costruzione, nella fornitura, nella commercializzazione, nell'installazione, nell'uso o nella manutenzione dei prodotti TIC, dei servizi TIC, dei processi TIC o dei servizi di sicurezza gestiti sottoposti a valutazione, né rappresentano i soggetti impegnati in tali attività. Gli organismi di valutazione della conformità, i loro alti dirigenti e le persone addette alla valutazione della conformità non intraprendono attività alcuna che possa essere in conflitto con la loro indipendenza di giudizio o integrità riguardo alle loro attività di valutazione della conformità. Tale divieto vale in particolare per i servizi di consulenza.»;	

Articoli e paragrafi del Regolamento (UE) 2025/37	Adeguamento normativa interna – modifiche al D.Lgs. 123/2022
2) il punto 10 è così modificato: a) la frase introduttiva è sostituita dalla seguente: «10. In ogni momento, per ogni procedura di valutazione della conformità e per ogni tipo, categoria o sottocategoria di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti, l'organismo di valutazione della conformità dispone: »; b) la lettera c) è sostituita dalla seguente: «c) di procedure per svolgere le attività che tengano debitamente conto delle dimensioni di un'impresa, del settore in cui opera, della sua struttura, del grado di complessità della tecnologia del prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito in questione e della natura di massa o seriale del processo produttivo.»; 3) i punti 19 e 20 sono sostituiti dai seguenti: «19. Gli organismi di valutazione della conformità sono conformi ai requisiti della pertinente norma armonizzata quale definita all'articolo 2, punto 9), del regolamento (CE) n. 765/2008 per quanto riguarda l'accreditamento degli organismi di valutazione della conformità che effettuano la certificazione dei prodotti TIC, dei servizi TIC, dei processi TIC o dei servizi di sicurezza gestiti. 20. Gli organismi di valutazione della conformità si assicurano che i laboratori di prova utilizzati ai fini della valutazione della conformità siano conformi ai requisiti della pertinente norma armonizzata quale definita all'articolo 2, punto 9), del regolamento (CE) n. 765/2008 per quanto riguarda l'accreditamento dei laboratori che effettuano prove.».	

RELAZIONE TECNICA

Il presente schema di decreto legislativo esercita la delega conferita al Governo dall'articolo 16 della legge 17 marzo 2026, n. 36 il quale, recando la "*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*", dispone l'adozione di uno o più decreti legislativi per adeguare la normativa nazionale alle disposizioni del regolamento (UE) 2025/37 e per coordinare le discipline di settore vigenti al quadro normativo europeo in materia.

Il regolamento (UE) 2025/37, in particolare, reca talune modifiche al regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019 (*Cybersecurity Act* o regolamento CSA), al fine di estendere il sistema europeo di certificazione della cybersicurezza anche nei confronti dei servizi di sicurezza gestiti.

Lo schema di decreto legislativo si compone di **4 articoli**.

L'**articolo 1** reca modifiche al decreto legislativo 3 agosto 2022, n. 123, volte ad assicurare la corretta e integrale applicazione del regolamento (UE) 2019/881, anche con riguardo alle modifiche apportate dal regolamento (UE) 2025/37, in attuazione del principio e criterio direttivo specifico di cui alla lettera *a*) dell'articolo 16, comma 2, della legge delega.

In particolare, il **comma 1**, **lettera *a*)**, modifica l'articolo 3, comma 1, del decreto legislativo 3 agosto 2022, n. 123, introducendo la definizione di "servizio di sicurezza gestito" e adegua le definizioni già presenti integrandole, laddove necessario, con il riferimento ai citati servizi di sicurezza gestiti.

La **lettera *b*) del comma 1**, invece, reca modifiche all'articolo 5, del decreto legislativo 3 agosto 2022, n. 123, che disciplina le attività di vigilanza del mercato.

In particolare, la disposizione di cui al **numero 1)** inserisce tra i casi di revoca dei certificati non conformi anche i certificati con livello di affidabilità di base o sostanziale relativi ai servizi di sicurezza gestiti e, al contempo, aggiorna i riferimenti ivi contenuti richiamando i soggetti essenziali di cui all'articolo 6, commi 1 e 2, del decreto legislativo 4 settembre 2024, n. 138 (con il quale è stata recepita all'interno dell'ordinamento nazionale la direttiva UE 2022/2555).

Il comma 1, lettera *b*), **numero 2)** modifica l'articolo 5 comma 5, del decreto legislativo 3 agosto 2022, n. 123. La disposizione intende ottimizzare il procedimento di revoca dei certificati di livello di affidabilità di base o sostanziale non conformi – relativi ora anche a un servizio di sicurezza gestito – al fine di assicurare il rispetto dei termini indicati nel richiamato articolo 5, comma 5, prevedendo, in caso di revoca del certificato da parte dell'organismo di valutazione della conformità, una contestuale comunicazione all'Agenzia dell'avvenuta revoca.

Il comma 1, lettera *b)*, **numero 3)**, dell'articolo in esame, interviene sull'articolo 5, comma 6, del decreto legislativo 3 agosto 2022, n. 123, che disciplina la modalità di gestione dei certificati non conformi che non sono direttamente revocati in base ai casi stabiliti dal menzionato comma 4 della medesima disposizione. La modifica apportata, in conformità al principio di proporzionalità, prevede la possibilità per l'Agenzia di indicare un termine - anche inferiore a 120 giorni - per ricondurre a conformità il certificato.

Infine, la modifica di cui al comma 1, lettera *b*), **numero 4)**, sana un mero errore materiale presente all'articolo 5, comma 9, del decreto legislativo 3 agosto 2022, n. 123.

Il comma 1 lettera *c*) dell'articolo in esame apporta modifiche all'articolo 6, del decreto legislativo 3 agosto 2022, n. 123, che disciplina il rilascio dei certificati di cybersicurezza. In particolare, interviene sul comma 1 del citato articolo 6, specificando che l'Agenzia, tramite l'Organismo di Certificazione della Sicurezza Informatica (di seguito OCSI), rilascia anche i certificati di cybersicurezza di livello di base o sostanziale e, in secondo luogo, corregge un mero errore materiale.

Il **comma 1, lettera *d*)**, dell'articolo in esame, **numeri 1) e 2)** modifica l'articolo 7 del decreto legislativo 3 agosto 2022, n. 123, il quale disciplina le modalità di rilascio e gestione delle dichiarazioni UE di conformità da parte dei fabbricanti o fornitori, in coerenza con l'articolo 55 del regolamento CSA.

In particolare, il comma 1 del menzionato articolo 7 stabilisce che i costruttori e fornitori, ai sensi dell'articolo 54, paragrafo 1, lettera *e*), del regolamento (UE) 2019/881, possono rilasciare dichiarazioni UE di conformità per dimostrare il rispetto di requisiti tecnici previsti da un sistema di certificazione per il livello di affidabilità di base. Il comma 2, invece, prevede che il fabbricante o fornitore di prodotti TIC deve rendere disponibile all'Agenzia la dichiarazione di conformità, la relativa documentazione e le altre informazioni pertinenti. La copia di una dichiarazione UE di conformità è trasmessa all'Agenzia e ad *European Network and Information Security Agency* (ENISA).

La disposizione in esame, quindi, estende la disciplina appena richiamata ai servizi di sicurezza gestiti.

Il **comma 1 lettera *e*)**, modifica l'articolo 9, comma 3, del decreto legislativo 3 agosto 2022, n. 123, prevedendo la possibilità per l'Agenzia di introdurre dei sistemi di certificazione nazionali della cybersicurezza non solo per i prodotti TIC, i servizi TIC e i processi TIC (come previsto attualmente dalla disposizione citata), ma anche per i sistemi di sicurezza gestiti, nell'ambito di progetti di ricerca e di formazione. La disposizione estende la facoltà dell'Agenzia di introdurre sistemi di certificazione nazionali anche per i servizi di sicurezza gestiti, già previsti dal decreto legislativo 3 agosto 2022, n. 123 per quanto concerne i prodotti TIC, i servizi TIC e i processi TIC.

Il **comma 1, lettera *f*)**, modifica l'articolo 10 del decreto legislativo 3 agosto 2022, n. 123, il quale reca la disciplina del quadro sanzionatorio per la violazione del regolamento europeo e dei sistemi europei di certificazione della cybersicurezza.

In particolare, la disposizione di cui al **numero 1)**, prevede che, relativamente al procedimento sanzionatorio amministrativo dell'Agenzia, si applichi la disciplina di cui all'articolo 17, comma 4*quater*, del decreto-legge n. 82 del 2021, che demanda ad un decreto del Presidente del Consiglio dei ministri la disciplina del procedimento sanzionatorio in capo all'Agenzia. In particolare, la disposizione in esame prevede che, anche con riferimento al procedimento sanzionatorio previsto dal decreto legislativo 3 agosto 2022, n. 123, l'Agenzia per la cybersicurezza nazionale operi sulla base del proprio regolamento e, nelle more della sua adozione, sulla base delle disposizioni contenute nelle sezioni I e II, del capo I, della legge n. 689 del 1981.

Le disposizioni di cui ai numeri **2)**, **3)**, **4)** e **5)**, integrano le fattispecie sanzionabili previste, rispettivamente, dai commi 4, 5, 8 e 16 dell'articolo 10 del decreto legislativo 3 agosto 2022, n. 123 con il riferimento ai servizi di sicurezza gestiti.

In particolare, la disposizione di cui al numero 5) aggiorna i riferimenti normativi contenuti nell'articolo 10, comma 16, del decreto legislativo 3 agosto 2022, n. 123, sostituendo i richiami all'abrogato decreto legislativo 18 maggio 2018, n. 65 (di recepimento della direttiva (UE) 2016/1148) con quelli al vigente decreto legislativo n. 138 del 2024 .

La **lettera *g*)**, del **comma 1**, dell'articolo in esame modifica l'articolo 13 del decreto legislativo 3 agosto 2022, n. 123, che disciplina la destinazione dei proventi derivanti dalle attività dell'Agenzia.

In particolare, la norma di cui al **numero 1)** modifica il citato articolo 13, comma 1, del decreto legislativo 3 agosto 2022, n. 123, al fine di individuare in modo più puntuale la posta contabile (ci si riferisce al capitolo di spesa di cui all'articolo 18, comma 1 del decreto-legge n. 82 del 2021) destinataria dei proventi derivanti dalle attività di vigilanza, di certificazione, di autorizzazione e di abilitazione svolte dall'Agenzia, a seguito dell'esperimento della prevista procedura di riassegnazione. Infatti, il decreto-legge istitutivo dell'Agenzia per la cybersicurezza nazionale prevede, all'articolo 18, l'istituzione, nello stato di previsione del Ministero dell'economia e delle finanze, di un apposito capitolo per la costituzione e l'espletamento dei compiti istituzionali conferiti alla citata Agenzia. Si evidenzia che la modifica in parola uniforma la previsione alle disposizioni, che ugualmente autorizzano la riassegnazione di entrate al bilancio dell'Agenzia, quali l'articolo 18 del citato decreto-legge n. 82 del 2021 e l'articolo 38 del decreto legislativo 4 settembre 2024, n. 138.

La disciplina di cui al **numero 2)**, con le medesime finalità appena illustrate per la riformulazione di cui al numero 1), modifica il comma 3 del richiamato articolo 13 del decreto legislativo 3 agosto 2022, n. 123 introducendo, come ulteriore destinazione degli introiti derivanti dalle sanzioni pecuniarie di cui all'articolo 10 del citato decreto legislativo, anche le attività di ricerca e formazione concernenti la certificazione della cybersicurezza dei già trattati servizi di sicurezza gestiti.

L'**articolo 2**, modifica l'articolo 35, commi 4 e 5, del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale).

In particolare, si prevede che 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 (UE) n. 910/2014 (c.d. eIDAS) sia accertata, a livello nazionale, dall'OCSI, il quale opererà necessariamente sulla base dello schema europeo di certificazione della cybersicurezza. La disposizione, in particolare, sopprime il riferimento allo schema nazionale di certificazione all'articolo 35, commi 4 e 5, del Codice dell'amministrazione digitale, posta la sua perdita di efficacia, a decorrere dal 27 febbraio 2026, dovuta all'adozione del regolamento di esecuzione (UE) 2024/482 della Commissione del 31 gennaio 2024. Il menzionato regolamento, definendo il primo schema europeo di certificazione della cybersicurezza dei prodotti TIC, servizi TIC e processi TIC basato sui criteri comuni, prevede, all'articolo 49, che tutti i sistemi nazionali di certificazione della cybersicurezza e le procedure correlate per i prodotti e i processi TIC contemplati predetto schema europeo di certificazione cessino di produrre effetti decorsi 12 mesi dall'entrata in vigore del regolamento di esecuzione (il regolamento di esecuzione (UE) 2024/482, ai sensi dell'articolo 50, è entrato in vigore il 27 febbraio 2025). Si precisa che l'introduzione dell'acronimo "OCSI" costituisce

una modifica di mero *drafting* volta a rendere inequivocabile la volontà di riferirsi all' "Organismo di certificazione della sicurezza informatica".

L'**articolo 3** modifica l'articolo 7 del decreto-legge n. 82 del 2021.

In particolare, il **comma 1, lettera *a*), numero 1)**, sostituisce l'articolo 7, comma 1, lettera *e*), numero 1) del decreto-legge n. 82 del 2021 prevedendo che l'Agenzia autorizzi, ai sensi dell'articolo 60, paragrafo 3, del regolamento (UE) 2019/881, 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.

Il **comma 1, numero 2)**, in stretta correlazione con la modifica appena illustrata e al fine di assicurare una piena portata applicativa all'articolo 7, comma 1, lettera *e*), numero 2) del decreto-legge n. 82 del 2021, precisa che le strutture dei richiamati Ministeri sono accreditate ai sensi dell'articolo 60, paragrafo 1, del regolamento (UE) 2019/881.

L'articolo 4 recala clausola di invarianza finanziaria, prevedendo che le amministrazioni interessate provvedono agli adempimenti previsti dal 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.

Ministero dell'Economia e delle Finanze

DIPARTIMENTO DELLA RAGIONERIA GENERALE DELLO STATO

VERIFICA DELLA RELAZIONE TECNICA

La verifica della presente relazione tecnica, effettuata ai sensi e per gli effetti dell'art. 17, comma 3, della legge 31 dicembre 2009, n. 196 ha avuto esito Positivo.

Il Ragioniere Generale dello Stato

Firmato digitalmente

ANALISI TECNICO-NORMATIVA

Amministrazione proponente: Presidenza del Consiglio dei Ministri

Titolo: Schema di decreto legislativo recante "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".

Referente: dott. Alessandro Travisani

******

PARTE I. ASPETTI TECNICO-NORMATIVI DI DIRITTO INTERNO

1) Obiettivi e necessità dell'intervento normativo. Coerenza con il programma di Governo.
Il presente schema di decreto legislativo, in coerenza con il programma di Governo, si prefigge di dare attuazione alla delega di cui all'articolo 16 della legge 17 marzo 2026, n. 36, "*Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2025*" (nel seguito indicata anche con "legge delega"), il quale, recando la "*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*", dispone che il Governo sia chiamato ad adottare, entro tre mesi dalla data di entrata in vigore della suddetta legge, uno o più decreti legislativi per adeguare la normativa nazionale alle disposizioni del regolamento (UE) 2025/37 e per coordinare le discipline di settore vigenti al quadro normativo europeo in materia.
Oltre ai princìpi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, lo schema di decreto legislativo in esame è stato predisposto sulla base dei seguenti princìpi 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 necessarie ad assicurare la corretta e integrale applicazione del regolamento (UE) 2019/881, 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), punti 1) e 2), del medesimo decreto-legge n. 82 del 2021, in conformità con le pertinenti disposizioni del regolamento (UE) 2019/881".

Pertanto, l'obiettivo della proposta normativa può essere riassunto nella previsione contenuta nel richiamato articolo 16 della legge n. 36 del 2026, ossia adeguare la normativa nazionale alle disposizioni di cui al regolamento (UE) 2025/37 e coordinare le discipline di settore vigenti con il quadro normativo europeo in materia.
Lo schema provvedimentale in esame, dunque, si prefigge di esercitare la delega conferita dall'articolo 16 della richiamata legge di delegazione europea 2025, sulla base dei citati princìpi e criteri direttivi specifici ivi indicati, rendendo, in particolare, il quadro nazionale di certificazione della cybersicurezza coerente con quello previsto dal regolamento (UE) 2019/881 (c.d. *Cybersecurity Act* o regolamento CSA), così come modificato dal citato regolamento (UE) 2025/37.

2) Analisi del quadro normativo nazionale.

Il quadro normativo nazionale è costituito dalle seguenti disposizioni:

- il decreto legislativo 3 agosto 2022, n. 123, recante "*Norme di adeguamento della normativa nazionale alle disposizioni del Titolo III «Quadro di certificazione della cibersicurezza» 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 cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»)*";
- 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*" e, in particolare, l'articolo 7, comma 1, lettera e);
- all'articolo 35, commi 4 e 5, il decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale", e, in particolare, l'articolo 35, commi 4 e 5;
- il decreto del Presidente del Consiglio dei ministri 30 ottobre 2003, recante "*Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art. 10, comma 1, del decreto legislativo 23 febbraio 2002, n. 10*", pubblicato sulla Gazzetta Ufficiale della Repubblica italiana n. 98 del 27 aprile 2004.

Nel dettaglio, al fine di assicurare l'adeguamento dell'ordinamento interno al regolamento (UE) 2019/881, è stato adottato il decreto legislativo n. 123 del 2022[1], recante "*Norme di adeguamento della normativa nazionale alle disposizioni del Titolo III «Quadro di certificazione della cibersicurezza» 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 cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»)*".

[1] Il decreto legislativo n. 123 del 2022 è stato adottato in attuazione della delega contenuta nell'articolo 18 della legge 22 aprile 2021, n. 53, recante "*Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2019-2020*".

Il menzionato decreto legislativo ha previsto, in coerenza con la designazione di cui all'articolo 7, comma 1, lettera e), del decreto-legge n. 82 del 2021[2], che l'autorità nazionale di certificazione della cybersicurezza sia l'Agenzia per la cybersicurezza nazionale (di seguito anche "ACN") e che la medesima Agenzia sia anche l'autorità di vigilanza del mercato. Tali attività – *i.e.* le attività dell'autorità nazionale di certificazione della cybersicurezza relative al rilascio di certificati europei di cybersicurezza e le connesse attività di vigilanza – sono rigorosamente separate in quanto sono svolte, indipendentemente le une dalle altre, da due distinte articolazioni dell'Agenzia. Il decreto legislativo n. 123 del 2022, inoltre, ha definito il quadro sanzionatorio di riferimento, come previsto dall'articolo 65 del regolamento CSA.
L'ACN, quale l'autorità nazionale di certificazione della cybersicurezza, rilascia i certificati di cybersicurezza tramite l'Organismo di Certificazione della Sicurezza Informatica (OCSI).
L'OCSI è stato istituito con il decreto del Presidente del Consiglio dei ministri 30 ottobre 2003 e, il medesimo decreto ha anche definito lo schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione (c.d. schema nazionale di certificazione). Dal primo luglio 2022, l'OCSI è incardinato in ACN, in seguito al trasferimento di competenze in materia di certificazione della cybersicurezza dal Ministero dello sviluppo economico all'Agenzia, previsto dall'articolo 7, lettera e) del decreto-legge n. 82 del 2021, attuato con il decreto del Presidente del Consiglio dei Ministri 15 giugno 2022.
Infine, l'OCSI svolge un ruolo di accertamento di conformità requisiti di sicurezza dei dispositivi per la creazione di una firma elettronica qualificata o di un sigillo elettronico ai sensi del decreto legislativo n. 82 del 2005. Nel dettaglio, l'articolo 35 del Codice dell'amministrazione digitale prevede:
- al comma 4, che i dispositivi sicuri di firma devono essere dotati di certificazione di sicurezza ai sensi dello schema nazionale di cui al comma 5;
- al comma 5, che la conformità ai requisiti di sicurezza dei dispositivi per la creazione di una firma elettronica qualificata o di un sigillo elettronico prescritti dall'Allegato II del regolamento (UE) n. 910/2014 (c.d. eIDAS) sia accertata, in Italia, dall'OCSI sulla base allo schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione, fissato con decreto del Presidente del Consiglio dei Ministri, o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con i Ministri delle comunicazioni, delle attività produttive e dell'economia e delle finanze. Tale schema

---

[2] L'articolo 7, comma 1, lettera e), del decreto-legge n. 82 del 2021 prevede "*L'Agenzia: [...]*
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 Ministero 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:
1) accredita, ai sensi dell'articolo 60, paragrafo 1, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza;
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 di cui al numero 1) della presente lettera, al rilascio del certificato europeo di sicurezza cibernetica".

nazionale può, inoltre, prevedere la valutazione e la certificazione relativamente ad ulteriori criteri europei ed internazionali, anche riguardanti altri sistemi e prodotti afferenti al settore suddetto.

3) Incidenza delle norme proposte sulle leggi e sui regolamenti vigenti.

Il presente schema di decreto intende introdurre tutte le riforme necessarie per assicurare la corretta e integrale applicazione del regolamento (UE) 2019/881, anche con riguardo alle modifiche apportate dal regolamento (UE) 2025/37, nell'ordinamento interno, adeguando il sistema nazionale di certificazione della cybersicurezza con riferimento ai servizi di sicurezza gestiti.

In particolare, il presente decreto legislativo intende apportare, da un lato, delle modifiche al decreto legislativo n. 123 del 2022 e al decreto legislativo 7 marzo 2005, n. 82 (in pieno esercizio del principio e criterio direttivo specifico di delega di cui alla lettera a)), e, dall'altro, al decreto-legge n. 82 del 2021 (in attuazione del principio e criterio direttivo specifico di delega di cui alla lettera b)).

Nel dettaglio, le modifiche apportate al decreto legislativo n. 123 del 2022 sono volte ad adeguare l'ordinamento interno alle disposizioni del regolamento (UE) 2025/37, estendendo il quadro nazionale di certificazione della cybersicurezza ai servizi di sicurezza gestiti. Tale intervento è stato condotto apportando delle modifiche alle definizioni, alle attività di vigilanza del mercato e di emissione dei certificati di cybersicurezza nonché di gestione delle dichiarazioni UE di conformità da parte dei fabbricanti o fornitori, alla possibilità di introdurre dei sistemi di certificazione nazionali della cybersicurezza in assenza di un sistema europeo di certificazione, alla disciplina del quadro sanzionatorio e della destinazione dei proventi.

Gli interventi sul decreto legislativo n. 82 del 2005 risultano necessari per garantire il coordinamento delle disposizioni settoriali vigenti con la normativa dettata dal *Cybersecurity Act* e dai relativi atti di esecuzione: in particolare, la novella sopprime il riferimento allo schema nazionale di certificazione contenuto nel citato articolo 35, commi 4 e 5, del Codice dell'amministrazione digitale, posta la perdita di efficacia, a decorrere dal 27 febbraio 2026, del menzionato schema nazionale di certificazione dovuta all'adozione del regolamento di esecuzione (UE) 2024/482 della Commissione del 31 gennaio 2024. Il citato regolamento di esecuzione, definendo il primo schema europeo di certificazione della cybersicurezza dei prodotti TIC, servizi TIC e processi TIC basato sui criteri comuni (EUCC), prevede, all'articolo 49, che tutti i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti e i processi TIC contemplati predetto schema europeo di certificazione cessino di produrre effetti decorsi 12 mesi dall'entrata in vigore del regolamento di esecuzione (il regolamento di esecuzione (UE) 2024/482, ai sensi dell'articolo 50, è entrato in vigore il 27 febbraio 2025).

Infine, la modifica dell'articolo 7, comma 1, lettera e), del decreto-legge n. 82 del 2021 si rende necessaria in quanto la citata disposizione, prevedendo che il compito di accreditamento delle strutture del Ministero dell'interno e della difesa avvenga ad opera dell'ACN, risulta non allineata con quanto previsto dall'articolo 60 del regolamento (UE) 2019/881. Invero, al fine di dare attuazione del principio e criterio direttivo specifico di delega di cui all'articolo

16, comma 2, lettera b), della legge di delegazione europea 2025, le modifiche introdotte sono volte a chiarire che le funzioni di accreditamento non sono espletate dall'ACN (in quanto ente non rientrante tra gli organismi nazionali di accreditamento designati ai sensi del regolamento (CE) n. 765/2008): la medesima Agenzia, invece, è deputata, in qualità di Autorità nazionale di certificazione della cybersicurezza, a rilasciare - ai sensi del richiamato articolo 60, paragrafo 3, del regolamento (UE) 2019/881 - l'autorizzazione agli organismi di valutazione della conformità che soddisfano i requisiti specifici o supplementari che un sistema europeo di certificazione della cybersicurezza stabilisce a norma dell'articolo 54, paragrafo 1, lettera f), del citato regolamento

4) Analisi della compatibilità dell'intervento con i principi costituzionali.

Il provvedimento è stato predisposto nel rispetto delle norme costituzionali, sia in relazione all'adempimento degli obblighi derivanti dall'ordinamento europeo, sia in relazione al riparto di competenze legislative tra Stato e regioni.

Non si rilevano profili di incompatibilità tra le misure contenute nel decreto legislativo con i principi costituzionali, con la giurisprudenza della Corte costituzionale, né con altre disposizioni vigenti.

5) Analisi della compatibilità dell'intervento con le competenze e le funzioni delle regioni ordinarie e a statuto speciale nonché degli enti locali.

Non si rilevano problemi di compatibilità dell'intervento con le competenze e le funzioni delle regioni, sia ordinarie sia a statuto speciale, nonché degli enti locali, in armonia con quanto previsto dall'articolo 117 della Costituzione.

6) Verifica della compatibilità con i principi di sussidiarietà, differenziazione e adeguatezza sanciti dall'articolo 118, primo comma, della Costituzione.

Non si rilevano problemi di compatibilità dell'intervento con i principi di sussidiarietà, differenziazione e adeguatezza sanciti dall'articolo 118, primo comma, della Costituzione.

7) Verifica dell'assenza di rilegificazioni e della piena utilizzazione delle possibilità di delegificazione e degli strumenti di semplificazione normativa.

Il provvedimento non comporta effetti di rilegificazione e non prevede l'utilizzo di strumenti di delegificazione e semplificazione normativa.

8) Verifica dell'esistenza di progetti di legge vertenti su materia analoga all'esame del Parlamento e relativo stato dell'iter.

Non risultano iniziative concernenti analoga materia all'esame del Parlamento.

9) Indicazione delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi di costituzionalità sul medesimo o analogo oggetto.

Non vi sono da segnalare indicazioni della giurisprudenza e non risultano pendenti giudizi di costituzionalità sull'oggetto del presente decreto.

PARTE II. CONTESTO NORMATIVO DELL'UNIONE EUROPEA E INTERNAZIONALE

10) Analisi della compatibilità dell'intervento con l'ordinamento dell'Unione europea.

Il provvedimento in esame non presenta profili di incompatibilità con il diritto dell'Unione europea. Si tratta, invero, di un decreto legislativo recante norme di adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2025/37 del Parlamento europeo e del Consiglio del 19 dicembre 2024.

11) Verifica dell'esistenza di procedure di infrazione da parte della Commissione europea sul medesimo o analogo oggetto.

Attualmente non risultano procedure di infrazioni aperte sulla materia oggetto del decreto.

12) Analisi della compatibilità dell'intervento con gli obblighi internazionali.

Il decreto in esame non presenta profili di incompatibilità con obblighi internazionali.

13) Indicazione delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte di giustizia dell'Unione europea sul medesimo o analogo oggetto.

Non vi sono da segnalare indicazioni della giurisprudenza e non risultano giudizi pendenti innanzi alla Corte di Giustizia vertenti sul medesimo o analogo oggetto.

14) Indicazione delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte europea dei diritti dell'uomo sul medesimo o analogo oggetto.

Non si è a conoscenza di linee prevalenti della giurisprudenza e non risultano giudizi pendenti innanzi alla Corte Europea dei Diritti dell'Uomo.

15) Eventuali indicazioni sulle linee prevalenti della regolamentazione sul medesimo oggetto da parte di altri Stati membri dell'Unione europea.

Non vi sono indicazioni da segnalare in ordine alle linee prevalenti adottate sul medesimo oggetto da parte di altri Stati membri dell'Unione europea.

PARTE III. ELEMENTI DI QUALITÀ SISTEMATICA E REDAZIONALE DEL TESTO

1) Individuazione delle nuove definizioni normative introdotte dal testo, della loro necessità, della coerenza con quelle già in uso.

In armonia con quanto previsto dal regolamento (UE) 2025/37, è stata introdotta la definizione di "servizi di sicurezza gestiti" (articolo 1, comma 1, lettera a) dello schema di decreto legislativo). L'esigenza dell'inserimento di tale definizione, in conformità con la tecnica

legislativa utilizzata anche a livello europeo, scaturisce dalla necessità di adeguare l'ordinamento interno alle disposizioni del richiamato regolamento europeo, il quale ha esteso il sistema di certificazione per la cybersicurezza ai citati servizi di sicurezza gestiti.
Inoltre, sono state adeguate le definizioni già presenti nel decreto legislativo n. 123 del 2022 inserendovi, laddove necessario, il riferimento ai citati servizi di sicurezza gestiti (ci si riferisce alle definizioni di "messa a disposizione sul mercato"; "ritiro"; "vigilanza del mercato"; "dichiarazione UE di conformità"; "certificato di cybersicurezza").
Tali interventi non si sovrappongono o si pongono in conflitto con le definizioni già consolidate nella legislazione di settore.
Tanto premesso, non vengono utilizzate definizioni normative che non appartengano già al linguaggio tecnico giuridico della materia regolata con le disposizioni contenute nel decreto legislativo in esame.

2) ***Verifica della correttezza dei riferimenti normativi contenuti nel progetto, con particolare riguardo alle successive modificazioni e integrazioni subite dai medesimi.***

È stata verificata positivamente la correttezza dei riferimenti normativi contenuti negli articoli del provvedimento.

3) ***Ricorso alla tecnica della novella legislativa per introdurre modificazioni e integrazioni a disposizioni vigenti.***

Nella predisposizione del provvedimento in esame si è ritenuto opportuno perseguire l'opzione della novella legislativa (apportando delle modifiche ai testi normativi vigenti mediante l'adozione di un decreto legislativo), anziché adottare un nuovo testo normativo sostitutivo dei precedenti, al fine di assicurare una piena aderenza ai criteri e principi direttivi specifici individuati dal menzionato articolo 16 della legge delega, che prevedono di apportare le modifiche e integrazioni necessarie sia alla normativa vigente e, in particolare, al decreto legislativo n. 123 del 2022 (principio e criterio direttivo specifico di delega di cui alla lettera a)) che al decreto-legge n. 82 del 2021 (principio e criterio direttivo specifico di delega di cui alla lettera b)). In particolare, tale scelta è coerente con la tecnica legislativa utilizzata a livello unionale: infatti, il regolamento (UE) 2025/37 apporta delle modifiche al regolamento (UE) 2019/881.
Le disposizioni contenute nel decreto legislativo prevedono la modifica delle seguenti disposizioni vigenti.
Le modifiche apportate al decreto legislativo 3 agosto 2022, n. 123 (articolo 1) sono:

- all'articolo 3, comma 1;
- all'articolo 5, commi 4, 5, 6 e 9;
- all'articolo 6, comma 1;
- all'articolo 7, commi 1 e 2;
- all'articolo 9, comma 3;
- all'articolo 10, commi 1, 4, 5, 8 e 16;
- all'articolo 13, commi 1 e 3.

La modifica apportata al decreto legislativo 7 marzo 2005, n. 82, interviene sull'articolo 35, commi 4 e 5 (articolo 2).
La modifica apportata al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, interviene sull'articolo 7, comma 1, lettera e), numeri 1) e 2) (articolo 3).
Le modifiche sopra riportate assicurano l'omogeneità della disciplina rispetto al quadro normativo di riferimento europeo e nazionale.

4) ***Individuazione di effetti abrogativi impliciti di disposizioni dell'atto normativo e loro traduzione in norme abrogative espresse nel testo normativo.***

Non si ravvisano effetti abrogativi impliciti nelle disposizioni contenute nel presente decreto legislativo.

5) ***Individuazione di disposizioni dell'atto normativo aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica o derogatorie rispetto alla normativa vigente.***

Non sussistono disposizioni dell'atto normativo aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica.

6) ***Verifica della presenza di deleghe aperte sul medesimo oggetto, anche a carattere integrativo o correttivo.***

L'articolo 16 della legge di delegazione europea 2025 ha conferito apposita delega legislativa 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, oltreché dei principi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, anche dei principi e criteri direttivi specifici ivi indicati.

7) ***Indicazione degli eventuali atti successivi attuativi e dei motivi per i quali non è possibile esaurire la disciplina con la normativa proposta e si rende necessario il rinvio a successivi provvedimenti attuativi; verifica della congruità dei termini previsti per la loro adozione.***

Lo schema di decreto legislativo non prevede l'adozione di atti attuativi.

8) ***Verifica della piena utilizzazione e dell'aggiornamento di dati e di riferimenti statistici attinenti alla materia oggetto del provvedimento, ovvero indicazione della necessità di commissionare all'Istituto nazionale di statistica apposite elaborazioni statistiche con correlata indicazione nella relazione tecnica della sostenibilità dei relativi costi.***

Per la predisposizione del provvedimento in esame sono stati utilizzati i dati informativi già in possesso dell'Amministrazione proponente e non è stato necessario commissionare l'acquisizione di ulteriori dati statistici o informativi.