2025/37

15.1.2025

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

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo ([1]),

previa consultazione del Comitato delle regioni,

deliberando secondo la procedura legislativa ordinaria ([2]),

considerando quanto segue:

(1) Il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio ([3]) istituisce un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti delle tecnologie dell'informazione e della comunicazione (TIC), dei servizi TIC e dei processi TIC nell'Unione, oltre che al fine di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cibersicurezza nell'Unione.

(2) Al fine di garantire la resilienza dell'Unione agli attacchi informatici e prevenire eventuali vulnerabilità nel mercato interno, il presente regolamento è inteso a integrare il quadro normativo orizzontale che stabilisce requisiti globali di cibersicurezza per i prodotti con elementi digitali a norma del regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio ([4]) prevedendo obiettivi di sicurezza per i servizi di sicurezza gestiti, nonché l'applicazione e l'affidabilità di tali servizi.

(3) I servizi di sicurezza gestiti sono forniti dai fornitori di servizi di sicurezza gestiti quali definiti all'articolo 6, punto 40), della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio ([5]). La definizione di servizi di sicurezza gestiti nel presente regolamento dovrebbe pertanto essere coerente con quella di fornitori di servizi di sicurezza gestiti della direttiva (UE) 2022/2555. Tali servizi consistono nello svolgimento di attività legate alla gestione dei rischi in materia di cibersicurezza dei loro clienti o nella fornitura di assistenza per tali attività e hanno acquisito un'importanza crescente nella prevenzione e attenuazione degli incidenti. Di conseguenza i fornitori di tali servizi sono considerati soggetti essenziali o importanti appartenenti a un settore ad alta criticità ai sensi della direttiva (UE) 2022/2555. Come affermato nel considerando 86 di tale direttiva, i fornitori di servizi di sicurezza gestiti in settori quali la risposta agli incidenti, i test di penetrazione, gli audit di sicurezza e la consulenza svolgono un ruolo particolarmente importante nell'assistere i soggetti nei loro sforzi per la prevenzione e il rilevamento degli incidenti, la risposta agli stessi o la ripresa da essi. Tuttavia, i fornitori di servizi di sicurezza gestiti sono stati essi stessi bersaglio di attacchi informatici e presentano un particolare rischio a causa della loro stretta integrazione nelle attività dei clienti. È quindi importante che i soggetti essenziali e importanti ai sensi della direttiva (UE) 2022/2555 esercitino una maggiore diligenza nella selezione dei fornitori di servizi di sicurezza gestiti.

([1]) GU C 349 del 29.9.2023, pag. 167.
([2]) Posizione del Parlamento europeo del 24 aprile 2024 (non ancora pubblicato nella Gazzetta Ufficiale) e decisione del Consiglio del 2 dicembre 2024.
([3]) 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») (GU L 151 del 7.6.2019, pag. 15).
([4]) Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva 2020/1828 (regolamento sulla ciberresilienza) (GU L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).
([5]) Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80).

(4) La definizione di servizi di sicurezza gestiti nell'ambito del presente regolamento comprende un elenco non esaustivo di servizi di sicurezza gestiti che potrebbero soddisfare le condizioni richieste dai sistemi europei di certificazione della cibersicurezza, quali servizi di gestione degli incidenti, i test di penetrazione, gli audit di sicurezza e la consulenza relativa all'assistenza tecnica. I servizi di sicurezza gestiti potrebbero comprendere servizi di cibersicurezza che sostengono la preparazione agli incidenti, la prevenzione, il rilevamento, l'analisi e l'attenuazione di tali incidenti, la risposta agli stessi e la ripresa da essi. Anche la fornitura di informazioni sulle minacce informatiche e la valutazione dei rischi relativi all'assistenza tecnica potrebbero essere considerate servizi di sicurezza gestiti. Vi potrebbero essere sistemi europei di certificazione della cibersicurezza distinti per diversi servizi di sicurezza gestiti. I certificati europei di cibersicurezza rilasciati conformemente a tali sistemi dovrebbero fare riferimento a specifici servizi di sicurezza gestiti di uno specifico fornitore di tali servizi.

(5) I fornitori di servizi di sicurezza gestiti possono, inoltre, svolgere un ruolo importante in relazione alle azioni dell'Unione a sostegno della risposta e della ripresa iniziale in caso di incidenti significativi e di incidenti di cibersicurezza su vasta scala, facendo affidamento sui servizi di fornitori privati di fiducia e sulla sperimentazione di soggetti critici per rilevare potenziali vulnerabilità sulla base di valutazioni coordinate a livello dell'Unione del rischio per la sicurezza. La certificazione dei servizi di sicurezza gestiti potrebbe svolgere un ruolo nella selezione dei fornitori di servizi di sicurezza gestiti di fiducia quali definiti nel regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio ([6]).

(6) Oltre a essere rilevante nell'ambito del processo di selezione riguardante la riserva dell'UE per la cibersicurezza istituita dal regolamento (UE) 2025/38, la certificazione dei servizi di sicurezza gestiti rappresenta anche un indicatore di qualità essenziale per i soggetti pubblici e privati che intendono acquistare tali servizi. Alla luce della criticità dei servizi di sicurezza gestiti e della sensibilità dei dati trattati, la certificazione potrebbe fornire ai potenziali clienti indicazioni e garanzie importanti sull'affidabilità di tali servizi. I sistemi europei di certificazione della cibersicurezza per i servizi di sicurezza gestiti sono intesi a contribuire a evitare la frammentazione del mercato interno. Il presente regolamento mira pertanto a migliorare il funzionamento del mercato interno.

(7) I sistemi europei di certificazione della cibersicurezza per i servizi di sicurezza gestiti dovrebbero portare alla diffusione di tali servizi e a una maggiore concorrenza tra i fornitori di servizi di sicurezza gestiti. Fatto salvo l'obiettivo di garantire livelli sufficienti e adeguati di conoscenze tecniche pertinenti e integrità professionale di tali fornitori, tali sistemi di certificazione dovrebbero pertanto agevolare l'ingresso nel mercato e l'offerta di servizi di sicurezza gestiti semplificando, per quanto possibile, i potenziali oneri normativi, amministrativi e finanziari che i fornitori, in particolare le piccole e medie imprese (PMI), incluse le microimprese, potrebbero incontrare quando offrono servizi di sicurezza gestiti. Inoltre, per incoraggiare la diffusione dei servizi di sicurezza gestiti e stimolarne la domanda, i sistemi europei di certificazione della cibersicurezza dovrebbero contribuire all'accessibilità di tali servizi, in particolare per gli attori di dimensioni più ridotte, come le PMI, incluse le microimprese, nonché per le autorità locali e regionali che dispongono di capacità e di risorse limitate, ma sono maggiormente esposte a violazioni della cibersicurezza con implicazioni finanziarie, giuridiche, reputazionali e operative.

(8) È importante aiutare le PMI, incluse le microimprese, ad attuare il presente regolamento e ad assumere personale con competenze e conoscenze specialistiche in materia di cibersicurezza necessarie per fornire servizi di sicurezza gestiti in conformità dei requisiti stabiliti nel presente regolamento. Il programma Europa digitale istituito dal regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio ([7]) e altri programmi pertinenti dell'Unione prevedono che la Commissione istituisca un sostegno finanziario e tecnico che consenta a tali imprese di contribuire alla crescita dell'economia dell'Unione e di rafforzare il livello comune di cibersicurezza nell'Unione, anche razionalizzando il sostegno finanziario del programma Europa digitale e di altri programmi pertinenti dell'Unione e sostenendo le PMI, incluse le microimprese.

(9) Il sistemi europei di certificazione della cibersicurezza per i servizi di sicurezza gestiti dovrebbe contribuire alla disponibilità di servizi sicuri e di elevata qualità che garantiscano una transizione digitale sicura e al conseguimento degli obiettivi stabiliti nel programma strategico per il decennio digitale 2030 istituito dalla decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio ([8]), in particolare per quanto riguarda l'obiettivo di far sì che il 75 % delle imprese dell'Unione inizi a fare uso di servizi di cloud computing, big data o intelligenza artificiale, che

([6]) Regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti informatici, e di preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694 (regolamento sulla cibersolidarietà) (GU L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

([7]) Regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio, del 29 aprile 2021, che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240 (GU L 166 dell'11.5.2021, pag. 1).

([8]) Decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che istituisce il programma strategico per il decennio digitale 2030 (GU L 323 del 19.12.2022, pag. 4).

oltre il 90 % delle PMI, incluse le microimprese, raggiunga almeno un livello minimo di intensità digitale e che i servizi pubblici principali siano accessibili online.

(10) Oltre a garantire l'avviamento dei prodotti TIC, dei servizi TIC o dei processi TIC, i servizi di sicurezza gestiti spesso forniscono funzionalità di servizio aggiuntive basate sulla competenza, sulla perizia e sull'esperienza del personale dei fornitori di tali servizi. Al fine di garantire una qualità molto elevata dei servizi di sicurezza gestiti forniti, occorre prevedere, tra gli obiettivi di sicurezza, competenze, perizia ed esperienza di altissimo livello, nonché procedure interne appropriate. Pertanto, al fine di garantire che tutti gli aspetti relativi ai servizi di sicurezza gestiti siano coperti da sistemi europei di certificazione della cibersicurezza dedicati, è necessario modificare il regolamento (UE) 2019/881. È opportuno tenere conto dei risultati e delle raccomandazioni della valutazione e del riesame di cui al regolamento (UE) 2019/881.

(11) Al fine di agevolare la crescita di un mercato interno affidabile, creando nel contempo partenariati con paesi terzi che condividono gli stessi principi, il processo di certificazione stabilito nel quadro europeo di certificazione della cibersicurezza previsto dal regolamento (UE) 2019/881 dovrebbe essere attuato in modo da facilitare il riconoscimento internazionale e l'allineamento alle norme internazionali.

(12) L'Unione si trova ad affrontare un divario di talenti caratterizzato da una carenza di professionisti qualificati, oltre a un panorama di minacce in rapida evoluzione, come riconosciuto nella comunicazione della Commissione del 18 aprile 2023 dal titolo «Colmare il divario di talenti nel settore della cibersicurezza per rafforzare la competitività, la crescita e la resilienza dell'UE ("Accademia per le competenze in materia di cibersicurezza")». Le risorse didattiche e le tipologie di formazione formale sono varie e le conoscenze possono essere acquisite in diversi modi: formalmente, ad esempio attraverso la frequenza di studi universitari o di corsi, o informalmente, ad esempio attraverso formazioni sul posto di lavoro o un'esperienza lavorativa nel settore pertinente. Pertanto, al fine di facilitare l'emergere di servizi di sicurezza gestiti e di elevata qualità e di disporre di un quadro più chiaro della composizione della forza lavoro dell'Unione nel settore della cibersicurezza, è importante rafforzare la cooperazione tra gli Stati membri, la Commissione, l'Agenzia dell'Unione europea per la cibersicurezza istituita dal regolamento (UE) 2019/881 (ENISA) e i portatori di interessi, compresi il settore privato e il mondo accademico, attraverso lo sviluppo di partenariati pubblico-privati, il sostegno a iniziative di ricerca e innovazione, lo sviluppo e il riconoscimento reciproco di norme comuni e la certificazione delle competenze in materia di cibersicurezza, anche attraverso il quadro europeo delle competenze in materia di cibersicurezza. Tale cooperazione agevolerebbe, inoltre, la mobilità dei professionisti della cibersicurezza all'interno dell'Unione come pure l'integrazione delle conoscenze e della formazione in materia di cibersicurezza nei programmi di istruzione, garantendo al contempo l'accesso agli apprendistati e ai tirocini per i giovani, tra cui le persone che vivono in regioni svantaggiate, come le isole e le regioni scarsamente popolate, rurali e periferiche. È importante che tale cooperazione miri ad attrarre un maggior numero di donne e ragazze nel settore e contribuisca ad affrontare il divario di genere in ambito scientifico, tecnologico, ingegneristico e matematico, e che il settore privato miri a fornire una formazione sul posto di lavoro che tenga conto delle competenze più richieste, coinvolgendo la pubblica amministrazione e le start-up, nonché le PMI, incluse le microimprese. È anche importante che i fornitori e gli Stati membri collaborino e contribuiscano alla raccolta di dati sulla situazione e sull'evoluzione del mercato del lavoro della cibersicurezza.

(13) L'ENISA svolge un ruolo importante nella preparazione delle proposte di sistemi europei di certificazione della cibersicurezza. In sede di preparazione del progetto di bilancio generale dell'Unione, la Commissione dovrebbe proporre le necessarie risorse di bilancio per la tabella dell'organico dell'ENISA, conformemente alla procedura di cui all'articolo 29 del regolamento (UE) 2019/881.

(14) Il presente regolamento prevede modifiche mirate del regolamento (UE) 2019/881 per permettere l'istituzione di sistemi europei di certificazione della cibersicurezza per i servizi di sicurezza gestiti. Nel fare ciò, specifica e chiarisce inoltre alcune disposizioni di tale regolamento relative alla preparazione e al funzionamento di tutti i sistemi europei di certificazione della cibersicurezza al fine di garantirne la trasparenza e l'apertura. Queste ultime modifiche, che si limitano a specificare o chiarire il regolamento (UE) 2019/881, in particolare le modifiche relative alle informazioni che l'ENISA deve fornire quando trasmette una proposta di sistema, quelle relative ai gruppi di lavoro ad hoc istituiti per ciascuna proposta di sistema e quelle relative all'informazione e alla consultazione in merito ai sistemi europei di certificazione della cibersicurezza, non dovrebbero in alcun modo pregiudicare la valutazione e il riesame più ampi di tale regolamento previsti a norma dell'articolo 67 dello stesso, in particolare la valutazione dell'impatto, dell'efficacia e dell'efficienza del titolo relativo al quadro di certificazione della cibersicurezza. La valutazione e il riesame di tale titolo dovrebbero basarsi su un'ampia consultazione dei portatori di interessi e su un'analisi completa e approfondita delle procedure interessate.

(15) Poiché l'obiettivo del presente regolamento, vale a dire quello di permettere l'istituzione di sistemi europei di certificazione della cibersicurezza per i servizi di sicurezza gestiti, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo della sua portata e dei suoi effetti, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(16) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([9]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 10 gennaio 2024,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

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.»;

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 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;

([9]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

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 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.»;

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.»;

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 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 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, 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 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 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 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 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 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 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 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.»;

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;»;

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;»;

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;»;

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;»;

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;»;

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 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 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.»;

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 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);»;

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.

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.

Articolo 2

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.

Fatto a Bruxelles, il 19 dicembre 2024

Per il Parlamento europeo	*Per il Consiglio*
La presidente	*Il presidente*
R. METSOLA	BÓKA J.

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 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.»;

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.».

In relazione al presente atto è stata formulata una dichiarazione, che figura nella GU C, C/2025/307, 15.1.2025, ELI: http://data.europa.eu/eli/C/2025/307/oj.