Consiglio dell'Unione europea

Bruxelles, 29 maggio 2018
(OR. en)

9350/18

Fascicolo interistituzionale: 2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

NOTA

Origine:	presidenza
Destinatario:	Consiglio
n. doc. prec.:	8834/18
n. doc. Comm.:	12183/17
Oggetto:	Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione ("regolamento sulla cibersicurezza") - Orientamento generale

I. INTRODUZIONE

1. Il 13 settembre 2017, nel quadro della sua strategia per il mercato unico digitale, la Commissione ha adottato e trasmesso al Consiglio e al Parlamento europeo la proposta in oggetto[1], la cui base giuridica è l'articolo 114 del TFUE. Nell'ambito del cosiddetto "pacchetto sulla cibersicurezza", questa proposta si prefigge di conseguire un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione, allo scopo di garantire il buon funzionamento del mercato interno.

2. Il regolamento proposto stabilisce gli obiettivi, i compiti e gli aspetti organizzativi dell'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e crea un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti e dei servizi TIC nell'Unione. La proposta della Commissione è corredata di una valutazione d'impatto che esamina una serie specifica di otto opzioni strategiche, che includono il riesame dell'ENISA e la certificazione della cibersicurezza nel settore delle TIC.

3. Il regolamento proposto comprende due filoni principali:

   - un mandato permanente per l'Agenzia, con un campo di applicazione ben delineato alla luce delle esigenze nel quadro delle nuove priorità politiche e dei nuovi strumenti, e una serie rinnovata di compiti e funzioni per l'Agenzia, per permettere di sostenere in modo efficace ed efficiente gli sforzi degli Stati membri, delle istituzioni dell'UE e degli altri portatori d'interessi al fine di garantire un ciberspazio sicuro;

   - un quadro europeo di certificazione della cibersicurezza per i prodotti e servizi TIC e regole che disciplinano i sistemi europei di certificazione della cibersicurezza, per far sì che i certificati rilasciati nell'ambito di tali sistemi siano validi e riconosciuti in tutti gli Stati membri e per rispondere all'attuale frammentazione del mercato.

[1] Docc. 12183/17, 12183/1/17 REV 1, 12183/2/17 REV 2.

4. Nell'ottobre 2017 il Consiglio europeo[2] ha chiesto che le proposte della Commissione in materia di cibersicurezza siano elaborate in modo olistico, presentate tempestivamente ed esaminate senza indugio, sulla base di un piano d'azione che deve essere definito dal Consiglio.

5. Il 12 dicembre 2017 il Consiglio "Affari generali" ha adottato il piano d'azione[3] per l'attuazione delle conclusioni del Consiglio[4] sulla comunicazione congiunta[5] al Parlamento europeo e al Consiglio: "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE". Il piano d'azione rispecchia l'ambizione del Consiglio di raggiungere un orientamento generale sulla proposta entro luglio 2018.

6. Al Parlamento europeo Angelika NIEBLER (ITRE, PPE) è stata nominata relatrice. La votazione in commissione ITRE sulla relazione è prevista il 19 giugno 2018.

7. Il Comitato economico e sociale europeo ha adottato il suo parere il 14 febbraio 2018.

II. LAVORI NELL'AMBITO DEL CONSIGLIO

8. Il 26 settembre 2017 la Commissione ha presentato al Gruppo orizzontale "Questioni riguardanti il ciberspazio" (di seguito "il Gruppo") la proposta e la relativa valutazione d'impatto, cui ha fatto seguito, il 20 ottobre 2017, un esame della valutazione d'impatto in sede di Gruppo. Le successive discussioni si sono concentrate sulla capacità operativa dell'Agenzia, sulla possibilità di interazione con le autorità nazionali competenti e sull'impatto del quadro di certificazione per quanto riguarda mercato e competitività delle imprese. In generale, sia la valutazione che la proposta sono state accolte favorevolmente dalle delegazioni.

---

2 Doc. EUCO 14/17, punto 11.
3 Doc. 15748/17.
4 Doc. 14435/17.
5 Doc. 12211/17.

9. La discussione sulla proposta stessa in sede di Gruppo è iniziata nel novembre 2017 durante la presidenza estone ed è proseguita sotto la presidenza bulgara. Alla proposta sono state dedicate dodici riunioni, che hanno dato luogo a otto versioni rivedute consecutive del testo, al fine di pervenire ad un accordo su un orientamento generale nella prossima sessione del Consiglio TTE (Telecomunicazioni) che si terrà l'8 giugno 2018.

10. I risultati delle discussioni tenutesi in sede di Gruppo il 14 e 15 maggio 2018 e il testo di compromesso riveduto della presidenza figurano nell'allegato della presente nota. I considerando sono stati adattati per riflettere le modifiche apportate alle disposizioni sostanziali. Tutte le modifiche rispetto alla proposta della Commissione sono indicate in **grassetto** o con [...]. Le modifiche rispetto all'ultimo documento del Gruppo (8834/18) figurano in **grassetto sottolineato** e tutte le soppressioni sono indicate con **[...]**.

III. CONCLUSIONE

11. Il testo di compromesso della presidenza, riportato in allegato, rispecchia gli sforzi della presidenza e degli Stati membri per trovare un giusto equilibrio nel testo.

12. Il 25 maggio 2018 il Comitato dei rappresentanti permanenti ha raggiunto un accordo sul testo di compromesso della presidenza, fatte salve le modifiche apportate all'articolo 19, paragrafo 5, e all'articolo 48, paragrafo 5, riprese nell'allegato.

13. Si invita il Consiglio ad adottare un orientamento generale nella sessione dell'8 giugno 2018 e a incaricare la presidenza di avviare negoziati su questo fascicolo con i rappresentanti del Parlamento europeo e della Commissione europea.

ALLEGATO

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

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

(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[6],

visto il parere del Comitato delle regioni[7],

deliberando secondo la procedura legislativa ordinaria,

---

[6] GU C , , pag. .

[7] GU C , , pag. .

considerando quanto segue:

(1) Le reti e i sistemi informativi e le reti e i servizi di telecomunicazione svolgono un ruolo essenziale per la società e sono diventati i pilastri della crescita economica. Le tecnologie dell'informazione e della comunicazione sono alla base dei sistemi complessi su cui poggiano le attività della società, che fanno funzionare le nostre economie in settori essenziali quali la sanità, l'energia, la finanza e i trasporti e che, in particolare, contribuiscono al funzionamento del mercato interno.

(2) L'uso delle reti e dei sistemi informativi da parte di cittadini, imprese e amministrazioni pubbliche di tutta l'Unione è attualmente molto diffuso. La digitalizzazione e la connettività stanno diventando caratteristiche fondamentali di un numero di prodotti e servizi in costante aumento, e con l'avvento dell'internet degli oggetti (IoT) nel prossimo decennio dovrebbero essere disponibili in tutta l'UE milioni, se non miliardi, di dispositivi digitali connessi. Sebbene un numero crescente di dispositivi siano connessi a internet, la sicurezza e la resilienza non sono sufficientemente integrate nella progettazione, il che rende inadeguata la cibersicurezza. In tale contesto, l'uso limitato della certificazione fa sì che gli utenti aziendali e individuali dispongano di informazioni insufficienti sulle caratteristiche dei prodotti e dei servizi TIC in termini di cibersicurezza, il che mina la fiducia nelle soluzioni digitali.

(3) L'incremento della digitalizzazione e della connettività comporta maggiori rischi in termini di cibersicurezza, il che rende la società in generale più vulnerabile alle minacce informatiche e aggrava i pericoli cui sono esposte le persone, comprese quelle vulnerabili come i minori. Al fine di attenuare tale rischio per la società, occorre prendere tutti i provvedimenti necessari per migliorare la cibersicurezza nell'UE allo scopo di proteggere meglio dalle minacce informatiche le reti e i sistemi informativi, le reti di telecomunicazione, i prodotti digitali, i servizi e i dispositivi utilizzati da cittadini, amministrazioni pubbliche e imprese (dalle PMI ai gestori delle infrastrutture critiche).

(4) Gli attacchi informatici sono in aumento e la maggiore vulnerabilità dell'economia e della società connesse alle minacce e agli attacchi informatici impone un rafforzamento delle difese. Tuttavia, mentre gli attacchi informatici hanno spesso una dimensione transfrontaliera, le risposte politiche delle autorità incaricate della cibersicurezza e le competenze in materia di applicazione della legge sono prevalentemente nazionali. Gli incidenti informatici su vasta scala possono ostacolare la prestazione di servizi essenziali su tutto il territorio dell'UE. Ciò richiede capacità effettive di risposta e di gestione delle crisi a livello di UE, sulla base di apposite politiche e strumenti di più ampia portata per la solidarietà europea e l'assistenza reciproca. Inoltre, una valutazione periodica dello stato della cibersicurezza e della resilienza nell'Unione, che sia basata su dati affidabili a livello di Unione e su previsioni sistematiche degli sviluppi, delle sfide e delle minacce futuri, sia a livello di Unione sia a livello mondiale, è quindi importante per i responsabili delle politiche, il settore e gli utenti.

(5) Tenuto conto delle maggiori sfide che l'Unione si trova ad affrontare in materia di cibersicurezza, è necessario disporre di una serie completa di misure che si basino su precedenti azioni dell'Unione e promuovano obiettivi sinergici. Tra questi obiettivi figura la necessità di rafforzare ulteriormente le capacità e la preparazione degli Stati membri e delle imprese e di migliorare la cooperazione e il coordinamento tra gli Stati membri e le istituzioni, le agenzie e gli organismi dell'UE. Inoltre, data la natura transfrontaliera delle minacce informatiche, è necessario aumentare le capacità a livello di Unione che potrebbero integrare l'azione degli Stati membri, in particolare in caso di crisi e incidenti informatici transfrontalieri su vasta scala. Sono inoltre necessari ulteriori sforzi per accrescere la consapevolezza di cittadini e imprese circa le questioni riguardanti la cibersicurezza. Inoltre, la fiducia nel mercato unico digitale dovrebbe essere ulteriormente rafforzata fornendo informazioni trasparenti in merito al livello di sicurezza dei prodotti e dei servizi TIC. Il conseguimento di questo obiettivo può essere agevolato mediante una certificazione a livello di UE che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali.

(6) Nel 2004 il Parlamento europeo e il Consiglio hanno adottato il regolamento (CE) n. 460/2004[8] che istituisce l'ENISA al fine di contribuire ad assicurare un elevato ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito dell'Unione e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione a vantaggio dei cittadini, dei consumatori, delle imprese e delle amministrazioni pubbliche. Nel 2008 il Parlamento europeo e il Consiglio hanno adottato il regolamento (CE) n. 1007/2008[9] che ha prorogato il mandato dell'Agenzia fino a marzo 2012. Il regolamento (CE) n. 580/2011[10] ha prorogato ulteriormente il mandato dell'Agenzia fino al 13 settembre 2013. Nel 2013 il Parlamento europeo e il Consiglio hanno adottato il regolamento (CE) n. 526/2013[11] relativo all'ENISA e che abroga il regolamento (CE) n. 460/2004, che ha prorogato il mandato dell'Agenzia fino a giugno 2020.

---

8 Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione (GU L 77 del 13.3.2004, pag. 1).

9 Regolamento (CE) n. 1007/2008 del Parlamento europeo e del Consiglio, del 24 settembre 2008, che modifica il regolamento (CE) n. 460/2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione per quanto riguarda la durata dell'Agenzia (GU L 293 del 31.10.2008, pag. 1).

10 Regolamento (UE) n. 580/2011 del Parlamento europeo e del Consiglio, dell'8 giugno 2011, che modifica il regolamento (CE) n. 460/2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione per quanto riguarda la durata dell'Agenzia (GU L 165 del 24.6.2011, pag. 3).

11 Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004 (GU L 165 del 18.6.2013, pag. 41).

(7) L'Unione ha già adottato importanti provvedimenti per garantire la cibersicurezza e accrescere la fiducia nelle tecnologie digitali. Nel 2013 è stata adottata la strategia dell'UE per la cibersicurezza per orientare la risposta politica dell'Unione alle minacce e ai rischi per la cibersicurezza. Nell'ambito dei suoi sforzi volti a proteggere maggiormente gli europei durante la navigazione online, nel 2016 l'Unione ha adottato il primo atto legislativo nel settore della cibersicurezza, la direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione ("direttiva NIS"). La direttiva NIS ha stabilito obblighi concernenti le capacità nazionali nel campo della cibersicurezza, ha istituito i primi meccanismi volti a rafforzare la cooperazione strategica e operativa tra gli Stati membri e ha introdotto obblighi riguardanti le misure di sicurezza e le notifiche degli incidenti in tutti i settori che sono di vitale importanza per l'economia e la società, quali l'energia, i trasporti, l'acqua, i servizi bancari, le infrastrutture dei mercati finanziari, la sanità, le infrastrutture digitali e i fornitori di servizi digitali essenziali (motori di ricerca, servizi di cloud computing e mercati online). All'ENISA è stato attribuito un ruolo fondamentale nel sostegno all'attuazione di tale direttiva. Inoltre, la lotta efficace contro la cibercriminalità è una priorità importante dell'agenda europea sulla sicurezza e contribuisce al conseguimento dell'obiettivo generale di raggiungere un elevato livello di cibersicurezza.

(8) È noto che, dall'adozione della strategia dell'UE per la cibersicurezza del 2013 e dall'ultima revisione del mandato dell'Agenzia, il contesto politico generale è cambiato in modo significativo, anche in relazione a un contesto globale più incerto e meno sicuro. In tale contesto e nel quadro della nuova politica dell'Unione in materia di cibersicurezza, è necessario rivedere il mandato dell'ENISA per definirne il ruolo nel mutato ecosistema della cibersicurezza e garantire che contribuisca efficacemente alla risposta dell'Unione alle sfide poste in questo ambito dalla radicale trasformazione del panorama delle minacce, per far fronte al quale l'attuale mandato non è sufficiente, come riconosciuto dalla valutazione dell'Agenzia.

(9) L'Agenzia istituita dal presente regolamento dovrebbe succedere all'ENISA, istituita con il regolamento (UE) n. 526/2013. L'Agenzia dovrebbe svolgere i compiti che le sono conferiti dal presente regolamento e dagli atti legislativi dell'UE nel settore della cibersicurezza, anche fornendo consulenze e pareri e fungendo da centro di informazioni e conoscenze dell'Unione. Dovrebbe promuovere lo scambio di buone pratiche tra gli Stati membri e i portatori di interessi del settore privato, fornendo suggerimenti strategici alla Commissione europea e agli Stati membri, fungendo da punto di riferimento per iniziative politiche settoriali dell'Unione sulle questioni di cibersicurezza, promuovendo la cooperazione operativa tra gli Stati membri e tra questi ultimi e le istituzioni, le agenzie e gli organismi dell'UE.

(10) Nel quadro della decisione 2004/97/CE, Euratom, adottata nella riunione del Consiglio europeo del 13 dicembre 2003, i rappresentanti degli Stati membri hanno deciso che la sede dell'ENISA sarebbe stata in Grecia, in una città designata dal governo greco. Lo Stato membro ospitante dovrebbe garantire le migliori condizioni possibili per il corretto ed efficace funzionamento dell'Agenzia. Per uno svolgimento adeguato ed efficiente dei suoi compiti, per l'assunzione e il mantenimento del personale e per una maggiore efficacia delle attività relative alla creazione di una rete di contatti, è imprescindibile che l'Agenzia sia ubicata in una sede adeguata che garantisca, tra l'altro, collegamenti e infrastrutture di trasporto appropriati per i coniugi e i figli del personale. Le disposizioni necessarie dovrebbero essere fissate in un accordo concluso tra l'Agenzia e lo Stato membro ospitante previa approvazione del consiglio di amministrazione dell'Agenzia.

(11) Tenuto conto delle crescenti sfide in materia di cibersicurezza che l'Unione si trova ad affrontare, le risorse finanziarie e umane destinate all'Agenzia dovrebbero essere aumentate per riflettere il potenziamento del suo ruolo e dei suoi compiti, come pure la sua posizione cruciale nell'ecosistema delle organizzazioni che difendono l'ecosistema digitale europeo.

(12) È opportuno che l'Agenzia sviluppi e mantenga un elevato livello di competenza e che operi come punto di riferimento generando fiducia nel mercato interno grazie alla propria indipendenza, alla qualità delle consulenze e delle informazioni fornite, alla trasparenza delle procedure e dei metodi operativi come pure alla diligenza nell'esecuzione dei suoi compiti. Nello svolgimento dei suoi compiti l'Agenzia dovrebbe **sostenere** [...]gli sforzi nazionali e **contribuire in modo proattivo** agli sforzi dell'Unione, collaborando pienamente con istituzioni, agenzie [...]**e organismi** dell'Unione e con gli Stati membri. Inoltre, dovrebbe avvalersi dei contributi e della collaborazione del settore privato e di altri portatori d'interessi. È opportuno stabilire una serie di compiti che definiscano in che modo l'Agenzia deve raggiungere i propri obiettivi, lasciandole nel contempo una certa flessibilità di azione.

(13) L'Agenzia dovrebbe assistere la Commissione tramite consulenze, pareri e analisi su tutte le questioni inerenti all'Unione e riguardanti l'elaborazione di politiche e normative e l'aggiornamento e la revisione nel settore della cibersicurezza **e i relativi aspetti settoriali specifici al fine di rafforzare la pertinenza delle politiche e normative dell'UE aventi una dimensione legata alla cibersicurezza e assicurare la coerenza della loro attuazione a livello nazionale**[...]. L'Agenzia dovrebbe fungere da punto di riferimento per pareri e competenze sulle iniziative politiche e legislative dell'Unione in settori specifici che presentano aspetti correlati alla cibersicurezza.

(14) Il compito di base dell'Agenzia è promuovere l'attuazione coerente del pertinente quadro normativo, in particolare l'effettiva attuazione della direttiva NIS, che è essenziale ai fini del rafforzamento della ciberresilienza. In considerazione del panorama delle minacce informatiche in rapida evoluzione, è chiaro che gli Stati membri devono essere sostenuti da un approccio trasversale più ampio allo sviluppo della ciberresilienza.

(15) L'Agenzia dovrebbe assistere gli Stati membri e le istituzioni, le agenzie [...]**e gli organismi** dell'Unione nei loro sforzi volti a sviluppare e consolidare le capacità e la preparazione per prevenire e individuare [...]**le minacce** e gli incidenti [...]**informatici** e relativi alla sicurezza delle reti e dei sistemi informativi e per reagirvi. In particolare, dovrebbe sostenere lo sviluppo e il potenziamento dei CSIRT nazionali perché raggiungano un livello comune elevato di maturità nell'Unione. **Le attività svolte dall'ENISA in relazione alle capacità operative degli Stati membri dovrebbero essere esclusivamente complementari alle azioni intraprese dagli Stati membri per adempiere agli obblighi loro derivanti dalla direttiva NIS e non dovrebbero pertanto sostituirsi ad esse**[...].

(15 bis) L'Agenzia dovrebbe inoltre fornire assistenza nello sviluppo e nell'aggiornamento delle strategie dell'Unione e, su richiesta, degli Stati membri in materia di sicurezza delle reti e dei sistemi informativi, in particolare per quanto riguarda la cibersicurezza, promuovere la loro diffusione e seguire la loro attuazione. Dovrebbe inoltre offrire formazione e materiale formativo agli enti pubblici e, se del caso, "formare i formatori" al fine di assistere gli Stati membri nello sviluppo di capacità di formazione autonome.

(16) L'Agenzia dovrebbe assistere il gruppo di cooperazione istituito dalla direttiva NIS nell'esecuzione dei suoi compiti, in particolare mettendo a disposizione competenze, fornendo consulenze e agevolando lo scambio di migliori pratiche, specialmente per quanto riguarda l'individuazione degli operatori di servizi essenziali da parte degli Stati membri, anche in relazione alle dipendenze transfrontaliere, riguardo a rischi e incidenti.

(17) Al fine di promuovere la cooperazione tra il settore pubblico e il settore privato e all'interno di quest'ultimo, [...]**l'Agenzia dovrebbe** sostenere **la condivisione delle informazioni intra e intersettoriale, in particolare nei settori che figurano nell'allegato II della direttiva (UE) 2016/1148, fornendo migliori pratiche e orientamenti sugli strumenti disponibili, procedure e orientamenti su come affrontare le questioni normative relative alla condivisione delle informazioni, ad esempio agevolando** [...]la creazione di centri settoriali di condivisione e di analisi delle informazioni (ISAC)[...].

(18) L'Agenzia dovrebbe aggregare e analizzare le relazioni nazionali **volontariamente condivise** dei CSIRT e della CERT-UE, **allo scopo di assistere gli Stati membri nella** definizione di [...]**procedure**, lingua e terminologia comuni per lo scambio delle informazioni. Dovrebbe inoltre coinvolgere il settore privato, nel quadro della direttiva NIS che ha gettato le basi per lo scambio volontario di informazioni tecniche a livello operativo [...]**nell'ambito** della rete di CSIRT.

(19) L'Agenzia dovrebbe contribuire a una risposta a livello di UE in caso di crisi e incidenti di cibersicurezza transfrontalieri su vasta scala. Dovrebbe espletare questa funzione **conformemente al suo mandato, ai sensi del presente regolamento, e a un approccio da concordarsi tra gli Stati membri nel contesto della raccomandazione della Commissione relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala.** Nell'ambito di questa funzione **potrebbe** raccogliere le informazioni pertinenti e agire come facilitatore tra la rete di CSIRT e la comunità tecnica e i responsabili decisionali nella gestione delle crisi. Inoltre, potrebbe sostenere la gestione degli incidenti dal punto di vista tecnico, agevolando lo scambio di soluzioni tecniche tra gli Stati membri e contribuendo alla comunicazione pubblica. L'Agenzia dovrebbe sostenere il processo provando le modalità di tale cooperazione attraverso esercitazioni [...]**periodiche** di cibersicurezza.

(20) [...]**Nel sostenere la cooperazione** operativa[...], l'Agenzia dovrebbe avvalersi delle competenze **tecniche e operative** disponibili della CERT-UE attraverso una cooperazione strutturata[...]. [...]Se del caso, dovrebbero essere conclusi appositi accordi tra le due organizzazioni per definire l'attuazione pratica di tale cooperazione **ed evitare la duplicazione delle attività**.

(21) Conformemente ai suoi compiti [...]**di sostegno della cooperazione operativa nell'ambito della rete di CSIRT**, l'Agenzia dovrebbe essere in grado di assistere gli Stati membri **su loro richiesta**, ad esempio fornendo consulenza **su come migliorare le loro capacità di prevenzione e rilevazione degli incidenti e di risposta agli stessi, [...]agevolando la gestione** [...]tecnica **di incidenti aventi un impatto rilevante o sostanziale**[...], o assicurando l'analisi di minacce e incidenti. **Nel quadro dell'agevolazione della gestione tecnica di incidenti aventi un impatto rilevante o sostanziale, l'ENISA dovrebbe in particolare sostenere la condivisione volontaria di soluzioni tecniche tra gli Stati membri o produrre informazioni tecniche combinate, quali soluzioni tecniche volontariamente condivise dagli Stati membri.** Nella sua raccomandazione relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala, la Commissione raccomanda agli Stati membri di cooperare in buona fede e di condividere tra loro e con l'ENISA senza indebiti ritardi le informazioni su tali incidenti e crisi. Tali informazioni dovrebbero aiutare ulteriormente l'ENISA nel [...]**sostegno alla cooperazione operativa**.

(22) Nell'ambito della costante cooperazione a livello tecnico per sostenere la conoscenza situazionale dell'Unione, l'Agenzia dovrebbe elaborare periodicamente **e in stretta cooperazione con gli Stati membri** la relazione sulla situazione tecnica della cibersicurezza nell'UE in merito alle minacce e agli incidenti, sulla base delle informazioni pubblicamente disponibili, della propria analisi e delle relazioni trasmesse dai CSIRT degli Stati membri [...]o dai punti di contatto unici istituiti dalla direttiva NIS **(in entrambi i casi su base volontaria)**, dal Centro europeo per la lotta alla criminalità informatica (EC3) presso Europol, dalla CERT-UE e, ove necessario, dal Centro dell'UE di analisi dell'intelligence (INTCEN) presso il Servizio europeo per l'azione esterna (SEAE). La relazione dovrebbe essere messa a disposizione delle istanze competenti del Consiglio, della Commissione, dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza e della rete di CSIRT.

(23) **Il sostegno dell'Agenzia, [...]su richiesta [...]degli [...]Stati membri interessati. alle indagini** tecniche ex post [...]sugli incidenti aventi un impatto significativo dovrebbe essere incentrato sulla prevenzione degli incidenti futuri[...]. **Gli Stati membri interessati dovrebbero fornire le informazioni necessarie per consentire all'Agenzia di sostenere efficacemente l'indagine tecnica.**

(24) [...]

(25) Gli Stati membri possono invitare le imprese interessate dall'incidente a collaborare fornendo le informazioni e l'assistenza necessarie all'Agenzia, fatto salvo il loro diritto di tutelare le informazioni sensibili sul piano commerciale.

(26) Per comprendere meglio le sfide nel campo della cibersicurezza e al fine di fornire consulenza strategica a lungo termine agli Stati membri e alle istituzioni dell'Unione, l'Agenzia ha bisogno di analizzare i rischi attuali e quelli emergenti. A tal fine, in cooperazione con gli Stati membri e se del caso con gli istituti di statistica e con altri organismi, l'Agenzia dovrebbe raccogliere le informazioni pertinenti **pubblicamente disponibili o volontariamente condivise**, analizzare le tecnologie emergenti e fornire valutazioni su temi specifici in relazione agli impatti previsti dal punto di vista sociale, giuridico, economico e regolamentare delle innovazioni tecnologiche sulla sicurezza delle reti e dell'informazione, in particolare sulla cibersicurezza. L'Agenzia dovrebbe inoltre assistere gli Stati membri e le istituzioni, le agenzie e gli organismi dell'Unione nell'individuazione delle tendenze emergenti e nella prevenzione[...] degli **incidenti** connessi alla cibersicurezza attraverso l'analisi di minacce e incidenti.

(27) Al fine di aumentare la resilienza dell'Unione, l'Agenzia dovrebbe sviluppare l'eccellenza in materia di **cyber**sicurezza delle **infrastrutture su cui poggiano in particolare i settori di cui all'allegato II della direttiva NIS e di quelle utilizzate dai fornitori di servizi digitali elencati nell'allegato III di tale direttiva**[...], fornendo consulenza, orientamenti e migliori pratiche. Allo scopo di agevolare l'accesso a informazioni meglio strutturate sui rischi connessi alla cibersicurezza e sulle possibili soluzioni, l'Agenzia dovrebbe sviluppare e mantenere il "polo d'informazione" dell'Unione, un portale che gli utenti possano utilizzare come sportello unico per accedere alle informazioni sulla cibersicurezza provenienti dalle istituzioni, dalle agenzie e dagli organismi dell'UE e nazionali.

(28) L'Agenzia dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla cibersicurezza e fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini e organizzazioni. Dovrebbe altresì contribuire a promuovere migliori pratiche e soluzioni a livello di singoli individui e organizzazioni mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione di relazioni finalizzate a fornire orientamenti a imprese e cittadini e a migliorare il livello complessivo di preparazione e resilienza. L'Agenzia dovrebbe inoltre organizzare regolarmente, in cooperazione con le istituzioni, le agenzie [...] **e gli organismi** degli Stati membri e dell'Unione campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali, allo scopo di promuovere comportamenti online individuali più sicuri e di accrescere la consapevolezza circa le potenziali minacce del ciberspazio, compresa la criminalità informatica, ad esempio phishing, botnet, frodi finanziarie e bancarie, nonché di promuovere consigli in materia di autenticazione di base e protezione dei dati. L'Agenzia dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi.

(29) Al fine di sostenere le imprese operanti nel settore della cibersicurezza, come pure gli utilizzatori delle soluzioni di cibersicurezza, l'Agenzia dovrebbe sviluppare e mantenere un "osservatorio del mercato" mediante l'esecuzione di analisi periodiche e la diffusione di informazioni sulle principali tendenze del mercato della cibersicurezza, sul versante sia della domanda che dell'offerta.

(30) Per conseguire appieno i propri obiettivi, l'Agenzia dovrebbe instaurare rapporti con le istituzioni, le agenzie e gli organismi pertinenti, compresi la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, l'Agenzia europea per la difesa (AED), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), l'Agenzia europea per la sicurezza aerea (EASA), **l'Agenzia dei sistemi globali di navigazione satellitare europei (Agenzia del GNSS)**, e tutte le agenzie dell'UE coinvolte nella sicurezza informatica. Dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo permanente di portatori di interessi dell'Agenzia. Nei contatti con le autorità di contrasto sugli aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di tali autorità, l'Agenzia dovrebbe avvalersi dei canali di informazione e delle reti esistenti.

(31) L'Agenzia, **nel suo ruolo**[...] di segretariato della rete di CSIRT, dovrebbe sostenere i CSIRT degli Stati membri e la CERT-UE nella cooperazione operativa, così come in tutte le pertinenti funzioni della rete di CSIRT, secondo quanto stabilito dalla direttiva NIS. Inoltre, l'Agenzia dovrebbe promuovere e sostenere la cooperazione tra i CSIRT interessati in caso di incidenti, attacchi o perturbazioni delle reti o delle infrastrutture della cui gestione o protezione sono responsabili i CSIRT e nei quali siano o possano essere coinvolti almeno due CSIRT, tenendo debitamente conto delle procedure operative standard della rete di CSIRT.

(32) Al fine di rafforzare la preparazione dell'Unione nel rispondere agli incidenti di cibersicurezza, l'Agenzia dovrebbe organizzare[...] esercitazioni **periodiche** di cibersicurezza a livello di Unione e, su loro richiesta, assistere le istituzioni, le agenzie e gli organismi dell'UE e degli Stati membri nell'organizzazione delle esercitazioni.

(33) L'Agenzia dovrebbe sviluppare ulteriormente e mantenere le proprie competenze in materia di certificazione della cibersicurezza al fine di sostenere la politica dell'UE in questo campo. Essa dovrebbe promuovere la diffusione della certificazione della cibersicurezza nell'Unione, anche contribuendo all'istituzione e al mantenimento di un apposito quadro di certificazione a livello di Unione, al fine di aumentare la trasparenza dell'affidabilità dei prodotti e dei servizi TIC in termini di cibersicurezza e di rafforzare in tal modo la fiducia nel mercato unico digitale.

(34) Strategie efficaci in materia di cibersicurezza dovrebbero essere basate su buoni metodi di valutazione dei rischi, sia nel settore pubblico che in quello privato. I metodi di valutazione dei rischi sono utilizzati a diversi livelli, e non esiste una prassi comune per quanto riguarda le modalità per una loro applicazione efficiente. La promozione e lo sviluppo di migliori pratiche per la valutazione dei rischi e per soluzioni interoperabili per la loro gestione nelle organizzazioni del settore pubblico e del settore privato aumenteranno il livello di cibersicurezza nell'Unione. A tal fine, l'Agenzia dovrebbe sostenere la cooperazione tra i portatori di interessi a livello di Unione, facilitando il loro impegno nella definizione e nella diffusione di standard europei e internazionali in materia di gestione dei rischi e di sicurezza misurabile di prodotti elettronici, sistemi, reti e servizi che, insieme ai software, costituiscono le reti e i sistemi informativi.

(35) L'Agenzia dovrebbe incoraggiare gli Stati membri e i fornitori di servizi a innalzare i loro standard di sicurezza generale in modo che tutti gli utenti di internet possano adottare le misure necessarie a garantire la propria cibersicurezza. In particolare, i fornitori di servizi e i fabbricanti di prodotti dovrebbero ritirare o riciclare i prodotti e i servizi non conformi alle norme in materia di cibersicurezza. In collaborazione con le autorità competenti, l'ENISA può diffondere informazioni sul livello di cibersicurezza dei prodotti e dei servizi offerti nel mercato interno e rivolgere avvertimenti ai fornitori e ai fabbricanti imponendo loro di migliorare la sicurezza, ivi inclusa la cibersicurezza, dei loro prodotti.

(36) L'Agenzia dovrebbe tenere pienamente conto delle attività di ricerca, sviluppo e valutazione tecnologica già in atto, in particolare quelle condotte nell'ambito delle varie iniziative di ricerca dell'Unione per fornire consulenza alle istituzioni, alle agenzie [...] e **agli organismi** dell'Unione e ove opportuno agli Stati membri, su loro richiesta, sulle esigenze in materia di ricerca nel settore della[...] cibersicurezza. **Per individuare le esigenze e priorità in materia di ricerca, l'Agenzia dovrebbe inoltre consultare i pertinenti gruppi di utenti.**

(37) [...]**Le minacce alla** cibersicurezza sono questioni globali. È necessaria una più stretta cooperazione internazionale per migliorare gli standard di **ciber**sicurezza, anche definendo norme di comportamento comuni, condividendo le informazioni e promuovendo una più celere cooperazione internazionale nel fornire una risposta alle questioni relative alla sicurezza delle reti e dell'informazione nonché un approccio globale comune a tali questioni. A tale scopo l'Agenzia dovrebbe sostenere una partecipazione e una cooperazione maggiori dell'Unione con i paesi terzi e le organizzazioni internazionali fornendo, se del caso, le competenze e le analisi necessarie alle istituzioni, alle agenzie [...] **e agli organismi** dell'Unione competenti.

(38) L'Agenzia dovrebbe essere in grado di rispondere alle richieste specifiche di consulenza e di assistenza inoltrate dagli Stati membri e dalle istituzioni, dalle agenzie e dagli organismi dell'UE che rientrano nei suoi obiettivi.

(39) È necessario applicare taluni principi per quanto riguarda la gestione dell'Agenzia al fine di rispettare la dichiarazione congiunta e l'approccio comune concordati nel luglio 2012 dal gruppo di lavoro interistituzionale sulle agenzie decentrate dell'Unione, con l'obiettivo di razionalizzare le attività delle agenzie e di migliorare la loro efficacia. La dichiarazione congiunta e l'approccio comune dovrebbero riflettersi, se del caso, nei programmi di lavoro dell'Agenzia, nelle sue valutazioni e nelle sue prassi di informazione e amministrazione.

(40) Il consiglio di amministrazione, composto dagli Stati membri e dalla Commissione, dovrebbe definire l'orientamento generale delle operazioni dell'Agenzia e garantire che questa svolga i propri compiti conformemente al presente regolamento. Il consiglio di amministrazione dovrebbe godere dei poteri necessari per formare il bilancio, verificarne l'esecuzione, adottare l'opportuna regolamentazione finanziaria, stabilire procedure di lavoro trasparenti per l'iter decisionale dell'Agenzia, adottare il documento unico di programmazione dell'Agenzia, adottare il proprio regolamento interno, nominare il direttore esecutivo e decidere in merito all'estensione del suo mandato e in merito alla sua conclusione.

(41) Per garantire il funzionamento corretto ed efficace dell'Agenzia, la Commissione e gli Stati membri dovrebbero assicurare che le persone da nominare nel consiglio di amministrazione dispongano di competenze ed esperienze professionali adeguate nelle aree funzionali. La Commissione e gli Stati membri dovrebbero inoltre sforzarsi di limitare l'avvicendamento dei loro rispettivi rappresentanti nel consiglio di amministrazione, per assicurarne la continuità dei lavori.

(42) Il corretto funzionamento dell'Agenzia esige che il direttore esecutivo sia nominato in base ai meriti e alla comprovata esperienza amministrativa e manageriale, nonché alla competenza e all'esperienza acquisita in materia di cibersicurezza, e che le funzioni del direttore esecutivo siano svolte in completa indipendenza. Previa consultazione della Commissione, il direttore esecutivo dovrebbe elaborare una proposta di programma di lavoro dell'Agenzia e adottare tutte le misure necessarie a garantire l'adeguata esecuzione del programma. Il direttore esecutivo dovrebbe redigere una relazione annuale **che includa l'attuazione del programma di lavoro annuale dell'Agenzia** da trasmettere al consiglio di amministrazione, fornire un progetto di stato di previsione delle entrate e delle spese dell'Agenzia e dare esecuzione al bilancio. Inoltre, è opportuno che il direttore esecutivo abbia la possibilità di istituire gruppi di lavoro ad hoc per affrontare questioni specifiche, in particolare di natura tecnico-scientifica, giuridica o socio-economica. Il direttore esecutivo dovrebbe garantire che i membri dei gruppi di lavoro ad hoc siano scelti secondo i più elevati standard di competenza, tenendo in debito conto la necessità di garantire un equilibrio tra le parti rappresentate, in base alle questioni specifiche, tra gli amministratori pubblici degli Stati membri, le istituzioni dell'Unione e il settore privato, compresi le imprese, gli utilizzatori e gli esperti del mondo accademico in materia di sicurezza delle reti e dell'informazione.

(43) Il comitato esecutivo dovrebbe contribuire al funzionamento efficace del consiglio di amministrazione. Nel quadro dei lavori preparatori relativi alle decisioni del consiglio di amministrazione, esso dovrebbe esaminare dettagliatamente le informazioni pertinenti, valutare le opzioni disponibili e fornire consulenza e soluzioni per la preparazione delle decisioni pertinenti del consiglio di amministrazione.

(44) È opportuno che l'Agenzia disponga di un gruppo permanente di portatori di interessi come organo consultivo, per garantire un dialogo regolare con il settore privato, le organizzazioni di consumatori e gli altri soggetti interessati. Il gruppo permanente di portatori di interessi, istituito dal consiglio di amministrazione su proposta del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'Agenzia. La composizione del gruppo permanente di portatori di interessi e i compiti assegnati a tale gruppo, da consultare in particolare in merito al progetto [...] di programma [...] di **lavoro**, dovrebbero garantire un'adeguata rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dall'Agenzia.

(45) L'Agenzia dovrebbe disporre di norme relative alla prevenzione e alla gestione dei conflitti di interessi. L'Agenzia dovrebbe applicare le disposizioni pertinenti dell'Unione in materia di accesso del pubblico ai documenti stabilite dal regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio[12]. Il trattamento dei dati personali da parte dell'Agenzia dovrebbe avvenire in conformità al regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati[13]. È opportuno che l'Agenzia si conformi alle disposizioni applicabili alle istituzioni dell'Unione e alla legislazione nazionale in materia di gestione delle informazioni, in particolare delle informazioni sensibili non classificate e delle informazioni classificate dell'UE.

---

[12] Regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione (GU L 145 del 31.5.2001, pag. 43).

[13] GU L 8 del 12.1.2001, pag. 1.

(46) Per garantire all'Agenzia piena autonomia e indipendenza e consentirle di svolgere nuovi compiti aggiuntivi, compresi compiti urgenti imprevisti, è opportuno che essa sia dotata di un bilancio congruo e autonomo le cui entrate siano essenzialmente costituite da un contributo dell'Unione e da contributi provenienti da paesi terzi che partecipano alle attività dell'Agenzia. La maggior parte del personale dell'Agenzia dovrebbe essere impiegata nell'attuazione operativa del suo mandato. Allo Stato membro ospitante, o a qualsiasi altro Stato membro, dovrebbe essere consentito di contribuire volontariamente alle entrate dell'Agenzia. La procedura di bilancio dell'Unione dovrebbe restare applicabile a qualsiasi sovvenzione a carico del bilancio generale dell'Unione. Inoltre, ai fini della trasparenza e della rendicontabilità, la revisione contabile dell'Agenzia dovrebbe essere svolta dalla Corte dei conti.

(47) [...]

(48) La certificazione della cibersicurezza riveste un ruolo importante nel rafforzare la sicurezza di prodotti e servizi TIC e nell'accrescere la fiducia negli stessi. Il mercato unico digitale, e in particolare l'economia dei dati e l'internet degli oggetti, possono prosperare solo se i cittadini sono convinti che tali prodotti e servizi offrono un determinato livello di affidabilità in termini di cibersicurezza. Le automobili connesse e automatizzate, i dispositivi medici elettronici, i sistemi di controllo per l'automazione industriale e le reti elettriche intelligenti sono solo alcuni esempi di settori in cui la certificazione è già ampiamente utilizzata o sarà probabilmente utilizzata in un prossimo futuro. La certificazione della cibersicurezza riveste un'importanza fondamentale anche nei settori disciplinati dalla direttiva NIS.

(49) Nella comunicazione del 2016 dal titolo "Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza" la Commissione ha sottolineato la necessità di prodotti e soluzioni di alta qualità, a costi contenuti e interoperabili. L'offerta di prodotti e servizi TIC nel mercato unico resta molto frammentata dal punto di vista geografico. La causa di tale frammentazione va ravvisata nel fatto che il settore della cibersicurezza in Europa si è sviluppato soprattutto in risposta alla domanda pubblica nazionale. Inoltre, l'assenza di soluzioni interoperabili (norme tecniche), di pratiche e di meccanismi UE di certificazione è un'altra delle lacune che influisce sul mercato unico della cibersicurezza. Ciò incide negativamente sulla competitività delle imprese europee a livello nazionale, europeo e mondiale e allo stesso tempo limita la gamma di tecnologie di cibersicurezza valide e utilizzabili a cui cittadini e imprese hanno accesso. Anche nella revisione intermedia dell'attuazione della strategia per il mercato unico digitale, la Commissione ha evidenziato la necessità di prodotti e sistemi connessi sicuri e ha dichiarato che la creazione di un quadro europeo di sicurezza delle TIC che definisca norme su come organizzare la certificazione della sicurezza delle TIC nell'Unione potrebbe sia preservare la fiducia nei confronti di internet sia permettere di affrontare l'attuale frammentazione del mercato della cibersicurezza.

(50) Attualmente la certificazione della cibersicurezza di **processi**, prodotti e servizi TIC è utilizzata solo in misura limitata. Quando esiste, è disponibile prevalentemente a livello di Stato membro o nell'ambito di sistemi promossi dall'industria. In tale contesto, un certificato rilasciato da un'autorità nazionale per la cibersicurezza non è, in linea di principio, riconosciuto dagli altri Stati membri. Le imprese pertanto potrebbero dover certificare i loro prodotti e servizi nei diversi Stati membri in cui operano, ad esempio ai fini della partecipazione a procedure nazionali di aggiudicazione degli appalti. Inoltre, stanno emergendo nuovi sistemi ma non sembra esservi un approccio coerente e olistico per quanto riguarda le questioni orizzontali relative alla cibersicurezza, ad esempio nel settore dell'internet degli oggetti. I sistemi esistenti presentano notevoli carenze e differenze in termini di copertura dei prodotti, livelli di affidabilità, criteri sostanziali e utilizzo effettivo.

(51) In passato sono stati compiuti sforzi finalizzati al reciproco riconoscimento dei certificati in Europa. Il loro successo tuttavia è stato solo parziale. L'esempio più importante in tal senso è l'accordo sul reciproco riconoscimento (ARR) del gruppo di alti funzionari competente in materia di sicurezza dei sistemi di informazione (SOG-IS). Sebbene rappresenti il più importante modello di cooperazione e di riconoscimento reciproco nel campo della certificazione della sicurezza, [...] il SOG-IS comprende solo una parte degli Stati membri dell'Unione. Ciò ha limitato l'efficacia dell'ARR del SOG-IS dal punto di vista del mercato interno.

(52) In considerazione di quanto precede, è necessario definire un quadro europeo di certificazione della cibersicurezza che stabilisca i principali requisiti orizzontali per i sistemi europei di certificazione della cibersicurezza da sviluppare e che consenta di riconoscere e utilizzare i certificati e le **dichiarazioni UE di conformità** per i prodotti e servizi TIC in tutti gli Stati membri. Il quadro europeo dovrebbe avere un duplice obiettivo: da un lato dovrebbe contribuire ad aumentare la fiducia nei prodotti e nei servizi TIC che sono stati certificati in base a detti sistemi. Dall'altro lato dovrebbe evitare il proliferare di certificazioni nazionali della cibersicurezza confliggenti o sovrapposte e ridurre così i costi per le imprese operanti nel mercato unico digitale. I sistemi dovrebbero essere non discriminatori e basati su norme [...] internazionali e/o **europee**, a meno che tali norme non siano inefficaci o inadeguate ai fini del conseguimento dei legittimi obiettivi dell'UE in tale ambito.

(53) La Commissione dovrebbe avere la facoltà di adottare sistemi europei di certificazione della cibersicurezza relativi a gruppi specifici di **processi,** prodotti e servizi TIC. Tali sistemi dovrebbero essere attuati e supervisionati dalle autorità nazionali di [...] certificazione **della cibersicurezza** e i certificati rilasciati nel loro ambito dovrebbero essere validi e riconosciuti in tutta l'Unione. I sistemi di certificazione gestiti dall'industria o da altre organizzazioni private non dovrebbero rientrare nel campo di applicazione del regolamento. Tuttavia, gli organismi che li gestiscono possono proporre alla Commissione di considerarli come base per l'approvazione degli stessi come sistema europeo.

(54) Le disposizioni del presente regolamento dovrebbero lasciare impregiudicata la legislazione dell'Unione che prevede norme specifiche sulla certificazione di prodotti e servizi TIC. In particolare, il regolamento generale sulla protezione dei dati stabilisce disposizioni per l'istituzione di meccanismi di certificazione e sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità a detto regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Tali meccanismi di certificazione e sigilli e marchi di protezione dei dati dovrebbero consentire agli interessati di valutare rapidamente il livello di protezione dei dati dei prodotti e dei servizi. Il presente regolamento lascia impregiudicata la certificazione delle operazioni di trattamento dei dati, anche nel caso in cui tali operazioni siano integrate nei prodotti e nei servizi, nel quadro del regolamento generale sulla protezione dei dati.

(55) Lo scopo dei sistemi europei di certificazione della cibersicurezza dovrebbe essere quello di assicurare che i **processi,** prodotti e servizi TIC certificati nel loro ambito siano conformi ai requisiti specificati **[...] che** mirano a [...] **proteggere** la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti o accessibili tramite tali prodotti, processi, servizi e sistemi **per tutto il loro ciclo di vita** ai sensi del presente regolamento. Non è possibile definire dettagliatamente nel presente regolamento i requisiti di cibersicurezza per tutti i **processi,** prodotti e servizi TIC. I **processi,** prodotti e i servizi TIC e le relative esigenze di cibersicurezza sono talmente diversi che risulta molto difficile formulare requisiti generali in materia di cibersicurezza che siano validi in tutti i casi. È pertanto necessario adottare una nozione ampia e generale di cibersicurezza ai fini della certificazione, integrata da una serie di obiettivi di cibersicurezza specifici da prendere in considerazione al momento dell'elaborazione dei sistemi europei di certificazione della cibersicurezza. Le modalità con cui tali obiettivi saranno conseguiti nei **processi,** prodotti e servizi TIC specifici dovrebbero quindi essere ulteriormente specificate dettagliatamente per ogni singolo sistema di certificazione adottato dalla Commissione, ad esempio facendo riferimento a norme o specifiche tecniche **in assenza di norme appropriate.**

(55 bis) Le specifiche tecniche da usare in un sistema europeo di certificazione della cibersicurezza dovrebbero essere individuate nel rispetto dei principi stabiliti all'allegato II del regolamento (UE) n. 1025/2012. In casi debitamente giustificati, tuttavia, si potrebbe ritenere necessario discostarsi da detti principi qualora le specifiche tecniche siano da usare in un sistema europeo di certificazione della cibersicurezza che fa riferimento a un livello di affidabilità elevato. Le motivazioni di tali scostamenti devono essere rese pubbliche.

(55 ter) La valutazione certificata della conformità è il processo che consiste nel valutare se siano stati rispettati i requisiti specifici connessi a un processo, prodotto o servizio TIC. Questa procedura è effettuata da un soggetto terzo indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. Il rilascio del certificato segue l'esito positivo della procedura di valutazione di un processo, prodotto o servizio TIC. Dovrebbe essere considerato la conferma che la corrispondente valutazione è stata correttamente effettuata. In funzione dal livello di affidabilità, il sistema europeo di cibersicurezza dovrebbe specificare se il certificato è rilasciato da un organismo pubblico o privato. La valutazione della conformità e la certificazione non possono garantire di per sé la cibersicurezza dei prodotti e servizi TIC certificati. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme tecniche.

(55 quater) La scelta, da parte degli utenti dei certificati, del livello appropriato di certificazione e dei relativi requisiti di sicurezza dovrebbe fondarsi su un'analisi del rischio per quanto riguarda l'uso di un processo, prodotto o servizio TIC. Il livello di affidabilità dovrebbe quindi essere commisurato al livello di rischio associato al previsto uso di un processo, prodotto o servizio TIC.

(55 quinquies) Un sistema europeo di certificazione della cibersicurezza potrebbe prevedere che la valutazione della conformità sia effettuata sotto la sola responsabilità del fabbricante o del fornitore di prodotti e servizi TIC (autovalutazione della conformità). In tal caso è sufficiente che il fabbricante o il fornitore effettui direttamente tutti i controlli per garantire che i processi, prodotti o servizi TIC siano conformi al sistema di certificazione. Questo tipo di valutazione della conformità dovrebbe essere considerato idoneo per prodotti o servizi TIC a bassa complessità (ad es. progetto e meccanismo di produzione semplici) che presentano un basso livello di rischio per l'interesse pubblico. Inoltre, solo i prodotti e i servizi TIC corrispondenti al livello di affidabilità di base potrebbero essere oggetto di autovalutazione della conformità.

(55 sexies) Un sistema europeo di certificazione della cibersicurezza potrebbe prevedere sia la certificazione che l'autovalutazione della conformità di prodotti e servizi TIC. In questo caso, il sistema dovrebbe comprendere mezzi chiari e comprensibili che consentano ai consumatori o altri utenti di distinguere tra i prodotti e servizi valutati sotto la responsabilità del fabbricante o del fornitore e i prodotti e servizi certificati da una parte terza.

(55 septies) I fabbricanti o fornitori di prodotti e servizi TIC che effettuano un'autovalutazione della conformità dovrebbero redigere e firmare la dichiarazione UE di conformità nell'ambito della procedura di valutazione della conformità. La dichiarazione UE di conformità è il documento che attesta che un determinato prodotto o servizio TIC è conforme ai requisiti del sistema. Redigendo e firmando la dichiarazione UE di conformità, il fabbricante o fornitore si assume la responsabilità della conformità del prodotto o servizio TIC con i requisiti di legge del sistema. Una copia della dichiarazione UE di conformità dovrebbe essere trasmessa all'autorità nazionale di certificazione della cibersicurezza e all'ENISA.

(55 octies) Il fabbricante o fornitore di prodotti e servizi TIC dovrebbe tenere a disposizione della competente autorità nazionale di certificazione della cibersicurezza, per un periodo definito nello specifico sistema europeo di certificazione della cibersicurezza, la dichiarazione UE di conformità e la documentazione tecnica di tutte le informazioni pertinenti relative alla conformità dei prodotti e servizi TIC a un sistema. La documentazione tecnica dovrebbe precisare i requisiti applicabili e includere, se necessario ai fini della valutazione, il progetto, la fabbricazione e il funzionamento del prodotto o servizio TIC. La documentazione tecnica dovrebbe essere compilata in modo da permettere la valutazione della conformità di un prodotto o servizio TIC ai requisiti applicabili.

(55 nonies) Gli Stati membri e le organizzazioni dei portatori di interesse dovrebbero poter sottoporre al Gruppo europeo per la certificazione della cibersicurezza la preparazione di una proposta di sistema. Le organizzazioni dei portatori di interesse sono l'industria o le organizzazioni dei rappresentanti dei consumatori, compresi i rappresentanti delle organizzazioni delle PMI che nutrono un valido interesse nello sviluppo di un particolare sistema europeo di certificazione della cibersicurezza. Tali proposte dovrebbero essere esaminate alla luce dei criteri elaborati dal Gruppo europeo per la certificazione della cibersicurezza per mezzo di orientamenti basati sui principi di trasparenza, apertura, imparzialità, consenso, efficacia, pertinenza e coerenza.

(56) La Commissione **e il Gruppo** dovrebbero avere la facoltà di incaricare l'ENISA di preparare **senza indebiti ritardi** proposte di sistemi per **processi,** prodotti o servizi TIC specifici. La Commissione, sulla base dei sistemi proposti dall'ENISA, dovrebbe quindi essere autorizzata ad adottare il sistema europeo di certificazione della cibersicurezza mediante atti di esecuzione. Tenendo conto dell'obiettivo generale e degli obiettivi di sicurezza individuati nel presente regolamento, i sistemi europei di certificazione della cibersicurezza adottati dalla Commissione dovrebbero specificare una serie minima di elementi riguardanti l'oggetto, l'ambito di applicazione e il funzionamento di ogni singolo sistema. Questi dovrebbero includere, tra l'altro, l'ambito di applicazione e l'oggetto della certificazione della cibersicurezza, compresi le categorie di **processi,** prodotti e servizi TIC, l'indicazione particolareggiata dei requisiti di cibersicurezza, ad esempio con riferimenti a norme o specifiche tecniche, i criteri e i metodi di valutazione specifici e il livello di affidabilità desiderato, di base, sostanziale e/o elevato, **nonché i livelli di valutazione ove applicabili**.

(56 bis) L'affidabilità di un sistema europeo di certificazione rappresenta la base per creare fiducia nel fatto che un processo, prodotto o servizio TIC soddisfa i requisiti di sicurezza di uno specifico sistema europeo di certificazione della cibersicurezza. Allo scopo di garantire la coerenza del quadro relativo ai processi, prodotti e servizi TIC certificati, un sistema europeo di certificazione della cibersicurezza potrebbe specificare i livelli di affidabilità dei certificati europei della cibersicurezza e delle dichiarazioni UE di conformità rilasciati nell'ambito di detto sistema. Ciascun certificato potrebbe far riferimento a uno dei livelli di affidabilità - di base, sostanziale o elevato - mentre la dichiarazione UE di conformità potrebbe far riferimento solo al livello di affidabilità di base. Ogni livello di affidabilità coincide con un determinato livello corrispondente di sforzi compiuti per la valutazione [...]; Tali livelli sono caratterizzati in riferimento alle specifiche, norme e procedure tecniche connesse, tra cui i controlli tecnici, il cui obiettivo è attenuare o prevenire gli incidenti di cibersicurezza. Ciascun livello di affidabilità dovrebbe essere coerente nei vari settori in cui la certificazione si applica.

(56 ter) Un sistema europeo di certificazione della cibersicurezza potrebbe precisare vari livelli di valutazione in funzione del rigore e della specificità della metodologia usata per la valutazione che dovrebbero corrispondere a uno dei livelli di affidabilità ed essere associati a un'idonea combinazione di componenti dell'affidabilità. Per tutti i livelli di affidabilità, il prodotto o servizio TIC dovrebbe contenere alcune funzioni sicure, definite nel sistema, che possono comprendere una configurazione sicura già predisposta in fabbrica, un codice firmato, aggiornamenti sicuri e tecniche utilizzate per ostacolare lo sfruttamento delle vulnerabilità (exploit mitigation) nonché piena protezione della memoria a impilaggio e della memoria heap. Dette funzioni dovrebbero essere soggette a sviluppo e manutenzione utilizzando approcci allo sviluppo centrati sulla sicurezza e strumenti ad essi associati onde assicurare che meccanismi efficaci (sia di software che di hardware) siano inclusi in maniera affidabile. Per il livello di affidabilità di base, la valutazione dovrebbe essere guidata almeno dai seguenti componenti di affidabilità: dovrebbe comprendere almeno un riesame della documentazione tecnica del prodotto o servizio TIC da parte dell'organismo di valutazione della conformità. Se la certificazione comprende processi TIC, il riesame tecnico dovrebbe vertere anche sul processo usato per il progetto, lo sviluppo e la manutenzione del prodotto o servizio TIC. Se un sistema europeo di certificazione della cibersicurezza prevede un'autovalutazione della conformità, dovrebbe essere sufficiente che il fabbricante o fornitore abbia effettuato un'autovalutazione della conformità del processo, prodotto o servizio TIC al sistema di certificazione. Per il livello di affidabilità sostanziale, la valutazione dovrebbe essere guidata, oltre che dai criteri previsti per il livello di base, almeno dalla verifica della conformità delle funzionalità di sicurezza del prodotto o servizio TIC alla documentazione tecnica ad esso relativa. Per il livello di affidabilità elevato, la valutazione dovrebbe essere guidata, oltre che dai criteri previsti per il livello sostanziale, almeno da un test di efficacia che accerti la resistenza delle funzionalità di sicurezza di un prodotto o servizio TIC nei confronti di coloro che effettuano complessi ciberattacchi disponendo di competenze e risorse significative.

(56 quater) All'atto di preparare una proposta di sistema, l'ENISA dovrebbe consultare tutti i pertinenti portatori di interesse, quali gli organismi europei di normazione, le competenti autorità nazionali, le organizzazioni costituite ai sensi di accordi di reciproco riconoscimento, ad esempio l'ARR del SOG-IS, le PMI, le organizzazioni dei consumatori e le parti interessate in campo ambientale e sociale.

(56 quinquies) L'ENISA dovrebbe avere un sito web che fornisca informazioni in merito ai sistemi europei di certificazione della cibersicurezza, e che pubblicizzi detti sistemi, in cui figurino, tra l'altro, le richieste di preparazione di una proposta di sistema europeo di certificazione della cibersicurezza e il riscontro ricevuto nella procedura di consultazione effettuata dall'ENISA durante la fase di preparazione. Tale sito web dovrebbe anche fornire informazioni sui certificati e le dichiarazioni UE di conformità rilasciati ai sensi del presente regolamento.

(57) Il ricorso alla certificazione europea della cibersicurezza **e alla dichiarazione UE di conformità** dovrebbe restare volontario, salvo disposizioni contrarie della legislazione dell'Unione o **di quella** nazionale **adottata in conformità alla legislazione dell'Unione**. **In mancanza di una legislazione armonizzata, gli Stati membri possono adottare regolamentazioni tecniche nazionali in virtù della direttiva (UE) 2015/1535 in cui è prevista una certificazione obbligatoria nel quadro di un sistema europeo di certificazione della cibersicurezza. Gli Stati membri potrebbero anche ricorrere alla certificazione europea della cibersicurezza nell'ambito degli appalti pubblici e della direttiva 2014/24/UE.**[...]

(57 bis) Al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere dalla data stabilita dalla Commissione mediante un atto di esecuzione. Inoltre, gli Stati membri non dovrebbero introdurre nuovi sistemi nazionali di certificazione per la certificazione della cibersicurezza di prodotti e servizi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza in vigore. Non si dovrebbe tuttavia impedire agli Stati membri di adottare o mantenere in vigore sistemi nazionali di certificazione per motivi di sicurezza nazionale.

(58) In seguito all'adozione di un sistema europeo di certificazione della cibersicurezza, i fabbricanti di prodotti TIC o i fornitori di servizi TIC dovrebbero essere in grado di presentare una domanda di certificazione dei loro prodotti o servizi a un organismo di valutazione della conformità di propria scelta. Se soddisfano determinati requisiti stabiliti nel presente regolamento, gli organismi di valutazione della conformità dovrebbero essere accreditati da un organismo di accreditamento. L'accreditamento dovrebbe essere concesso per un periodo massimo di cinque anni, con la possibilità di rinnovarlo alle stesse condizioni, purché l'organismo di valutazione della conformità soddisfi i requisiti. Gli organismi di accreditamento dovrebbero **limitare, sospendere o** revocare l'accreditamento di un organismo di valutazione della conformità se le condizioni per l'accreditamento non sono, o non sono più, soddisfatte o se le azioni intraprese da un organismo di valutazione della conformità sono contrarie alle disposizioni del presente regolamento.

(59) [...] Gli Stati membri **dovrebbero** [...] designare una **o più** autorità di [...] certificazione della cibersicurezza per vigilare sulla conformità **agli obblighi derivanti dal presente regolamento**. **Qualora lo ritengano appropriato, gli Stati membri possono attribuire questi compiti anche ad autorità già esistenti. Gli Stati membri dovrebbero altresì avere facoltà di decidere, di comune accordo con un altro Stato membro, di designare una o più autorità di vigilanza nel territorio di tale altro Stato membro. In particolare l'autorità dovrebbe monitorare e far applicare gli obblighi che incombono al fabbricante o al fornitore di prodotti e servizi TIC stabilito nel suo territorio in relazione alla dichiarazione UE di conformità, assistere gli organismi nazionali di accreditamento nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità mettendo a loro disposizione le proprie competenze e le pertinenti informazioni, autorizzare gli organismi di valutazione della conformità a svolgere i suoi compiti quando soddisfano i requisiti supplementari previsti in un sistema e monitorare i pertinenti sviluppi nel settore della certificazione della cibersicurezza** [...]. Le autorità nazionali di [...] certificazione **della cibersicurezza** dovrebbero trattare i reclami presentati dalle persone fisiche o giuridiche in relazione ai certificati **che sono da loro** rilasciati **o dei certificati rilasciati dagli organismi di valutazione della conformità in relazione al livello di affidabilità elevato** [...], svolgere le indagini opportune sull'oggetto del reclamo e informare il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole. Esse dovrebbero inoltre cooperare con le altre autorità nazionali di [...] certificazione **della cibersicurezza** o con altre autorità pubbliche, anche mediante lo scambio di informazioni sugli eventuali prodotti e servizi TIC non conformi ai requisiti del presente regolamento o di specifici sistemi di cibersicurezza.

(60) Al fine di garantire un'applicazione coerente del quadro europeo di certificazione della cibersicurezza, dovrebbe essere costituito un gruppo europeo per la certificazione della cibersicurezza (di seguito il "gruppo") costituito **dai rappresentanti delle** autorità nazionali di [...] certificazione della cibersicurezza **o di altre autorità nazionali competenti**. I compiti principali del gruppo dovrebbero essere consigliare e assistere la Commissione nelle attività volte ad assicurare un'attuazione e un'applicazione coerenti del quadro europeo di certificazione della cibersicurezza; assistere e cooperare strettamente con l'Agenzia nella preparazione delle proposte di sistemi di certificazione della cibersicurezza; raccomandare alla Commissione di incaricare l'Agenzia di preparare una proposta di sistema europeo di certificazione della cibersicurezza; adottare pareri indirizzati **all'Agenzia in merito alle proposte di sistemi e** alla Commissione relativi al mantenimento e alla revisione degli attuali sistemi europei di certificazione della cibersicurezza.

(60 bis) Il gruppo dovrebbe agevolare lo scambio di buone prassi e di competenze tra le autorità nazionali di certificazione della cibersicurezza responsabili dell'autorizzazione degli organismi di valutazione della conformità e del rilascio dei certificati. Il gruppo dovrebbe sostenere lo sviluppo di un meccanismo di valutazione inter pares nell'ambito della preparazione di una proposta di sistema e la sua attuazione per gli organismi che rilasciano certificati europei di cibersicurezza per il livello di affidabilità elevato. Dette valutazioni inter pares dovrebbero in particolare valutare se gli organismi in questione dispongono delle competenze adeguate e svolgono i rispettivi compiti in maniera armonizzata. I risultati delle valutazioni inter pares dovrebbero essere resi pubblici. Gli organismi interessati possono adottare le opportune misure per adeguare le proprie prassi e competenze.

(61) Al fine di accrescere la consapevolezza e facilitare l'accettazione dei futuri sistemi di cibersicurezza dell'UE, la Commissione europea può emanare orientamenti generali o settoriali in materia di cibersicurezza, ad esempio orientamenti sulle buone pratiche o sul comportamento responsabile in tale ambito, sottolineando l'effetto positivo dell'utilizzo di prodotti e servizi TIC certificati.

(61 bis) Allo scopo di agevolare ulteriormente gli scambi e riconoscendo il carattere globale delle catene dell'offerta di TIC, l'Unione può concludere, conformemente all'articolo 218 del TFUE, accordi per il reciproco riconoscimento relativamente ai certificati rilasciati nell'ambito di sistemi istituiti in virtù del quadro europeo di certificazione della cibersicurezza. La Commissione, tenuto conto del parere dell'ENISA e del gruppo europeo per la certificazione della cibersicurezza, può raccomandare l'apertura dei negoziati pertinenti. Ciascun sistema dovrebbe prevedere condizioni specifiche per il reciproco riconoscimento con i paesi terzi.

(62) [...]

(63) [...]

(64) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, dovrebbero essere attribuite alla Commissione competenze di esecuzione ove previsto dal presente regolamento. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011.

(65) La procedura d'esame dovrebbe essere utilizzata per l'adozione degli atti di esecuzione sui sistemi europei di certificazione della cibersicurezza per i prodotti e i servizi TIC; sulle modalità di conduzione delle indagini da parte dell'Agenzia; sulle circostanze, sui formati e sulle procedure delle notifiche degli organismi di valutazione della conformità accreditati da parte delle autorità nazionali di [...] certificazione **della cibersicurezza** alla Commissione.

(66) L'operato dell'Agenzia dovrebbe essere valutato in maniera indipendente. La valutazione dovrebbe tenere conto del conseguimento degli obiettivi da parte dell'Agenzia, delle sue pratiche di lavoro e della pertinenza dei suoi compiti. Dovrebbe altresì valutare l'impatto, l'efficacia e l'efficienza del quadro europeo di certificazione della cibersicurezza.

(67) Il regolamento (UE) n. 526/2013 dovrebbe essere abrogato.

(68) Poiché gli obiettivi del presente regolamento non possono essere conseguiti in misura sufficiente dagli Stati membri e possono dunque essere conseguiti 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 necessario per conseguire tali scopi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

TITOLO I
DISPOSIZIONI GENERALI

Articolo 1

Oggetto e ambito di applicazione

1. Allo scopo di garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione, il presente regolamento:

a) stabilisce gli obiettivi, i compiti e gli aspetti organizzativi dell'ENISA, l'"Agenzia dell'[...]**Unione europea per la cibersicurezza**", di seguito denominata "l'Agenzia" e

b) stabilisce un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza **dei processi,** prodotti e servizi TIC nell'Unione. Tale quadro si applica fatte salve le disposizioni specifiche in materia di certificazione volontaria o obbligatoria in altri atti dell'Unione.

2. **Il presente regolamento fa salve le competenze degli Stati membri per quanto riguarda la cibersicurezza e, in ogni caso, fa salve le attività nel settore della pubblica sicurezza, della difesa, della sicurezza nazionale e le attività dello Stato nell'ambito del diritto penale.**

Articolo 2

Definizioni

Ai fini del presente regolamento si intende per:

1) "cibersicurezza", l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, i loro utenti e le persone interessate dalle minacce informatiche;

2) "rete e sistema informativo", un sistema ai sensi dell'articolo 4, punto 1, della direttiva (UE) 2016/1148;

3) "strategia nazionale per la sicurezza della rete e dei sistemi informativi", un quadro ai sensi dell'articolo 4, punto 3, della direttiva (UE) 2016/1148;

4) "operatore di servizi essenziali", un soggetto pubblico o privato ai sensi dell'articolo 4, punto 4, della direttiva (UE) 2016/1148;

5) "fornitore di servizio digitale", qualsiasi persona giuridica che fornisce un servizio digitale ai sensi dell'articolo 4, punto 6, della direttiva (UE) 2016/1148;

6) "incidente", qualsiasi evento che corrisponda alla definizione di cui all'articolo 4, punto 7, della direttiva (UE) 2016/1148;

7) "gestione dell'incidente", qualsiasi procedura che corrisponda alla definizione di cui all'articolo 4, punto 8, della direttiva (UE) 2016/1148;

8) "minaccia informatica", qualsiasi circostanza o evento che potrebbe **danneggiare, perturbare** o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sui loro utenti e sulle persone interessate;

9) "sistema europeo di certificazione della cibersicurezza", la serie completa di norme, requisiti tecnici, norme tecniche e procedure definiti a livello di Unione che si applicano alla certificazione **o alla valutazione della conformità dei processi,** dei prodotti e dei servizi nell'ambito delle tecnologie dell'informazione e della comunicazione (TIC) che rientrano nell'ambito di applicazione del sistema;

9 bis) "sistema nazionale di certificazione della cibersicurezza", una serie completa di norme, requisiti tecnici, norme tecniche e procedure elaborati e adottati da un'autorità pubblica nazionale, che si applicano alla certificazione o alla valutazione della conformità dei processi, prodotti e servizi TIC che rientrano nell'ambito di applicazione del sistema;

10) "certificato europeo di cibersicurezza", un documento [...] che attesta che un determinato processo, prodotto o servizio TIC [...]**è stato oggetto di una valutazione di conformità con** i requisiti **di sicurezza** specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;

11) "prodotto [...] TIC", qualsiasi elemento o gruppo di elementi della rete e dei sistemi informativi;

11 bis) "servizio TIC", qualsiasi servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo della rete e dei sistemi informativi;

11 ter) "processo TIC", l'insieme delle attività svolte per progettare, sviluppare, fornire e mantenere un prodotto o servizio TIC;

12) "accreditamento", l'accreditamento quale definito all'articolo 2, punto 10, del regolamento (CE) n. 765/2008;

13) "organismo nazionale di accreditamento", un organismo nazionale di accreditamento ai sensi dell'articolo 2, punto 11, del regolamento (CE) n. 765/2008;

14) "valutazione della conformità", la valutazione della conformità ai sensi dell'articolo 2, punto 12, del regolamento (CE) n. 765/2008;

15) "organismo di valutazione della conformità", un organismo di valutazione della conformità ai sensi dell'articolo 2, punto 13, del regolamento (CE) n. 765/2008;

16) "norma tecnica", una norma tecnica ai sensi dell'articolo 2, punto 1, del regolamento (UE) n. 1025/2012**;**

16 bis) "specifica tecnica", un documento che prescrive i requisiti tecnici che un prodotto, un processo o un servizio TIC deve soddisfare;

16 ter) "livello di affidabilità", base per creare fiducia nel fatto che un processo, prodotto o servizio TIC soddisfi i requisiti di sicurezza di uno specifico sistema europeo di certificazione della cibersicurezza e dichiari a quale livello è stato valutato; il livello di affidabilità non misura la sicurezza intrinseca di un processo, prodotto o servizio TIC.

TITOLO II

ENISA – l'*"Agenzia dell'[...]Unione europea per la cibersicurezza"*

CAPO I

MANDATO E OBIETTIVI *[...]*

Articolo 3

Mandato

1. L'Agenzia svolge i compiti che le sono attribuiti dal presente regolamento allo scopo di contribuire a un elevato livello di cibersicurezza [...]**in tutta** l'Unione**, in particolare sostenendo le istituzioni, le agenzie e gli organismi degli Stati membri e dell'Unione nel miglioramento della cibersicurezza**. **L'Agenzia funge da punto di riferimento per pareri e competenze in materia di cibersicurezza per le istituzioni, le agenzie e gli organismi dell'Unione.**

2. L'Agenzia svolge i compiti che le sono attribuiti dagli atti dell'Unione che stabiliscono le misure per il ravvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri relative alla cibersicurezza.

2 bis. Nello svolgimento dei suoi compiti, l'Agenzia agisce in maniera indipendente e tiene nella massima considerazione le competenze nazionali delle autorità pertinenti degli Stati membri, evitando nel contempo la duplicazione delle attività.

3. [...]

Articolo 4

Obiettivi

1. L'Agenzia opera come centro di competenze nel settore della cibersicurezza grazie alla sua indipendenza, alla qualità scientifica e tecnica delle consulenze e dell'assistenza fornite e delle informazioni che mette a disposizione, alla trasparenza delle procedure e dei metodi operativi utilizzati e alla diligenza nell'esecuzione dei suoi compiti.

2. L'Agenzia assiste le istituzioni, le agenzie e gli organismi dell'Unione, come pure gli Stati membri, nell'elaborazione e nell'attuazione di politiche **dell'Unione** relative alla cibersicurezza**, ivi comprese le politiche settoriali in materia di cibersicurezza**.

3. L'Agenzia sostiene lo sviluppo della capacità e la preparazione nell'Unione, assistendo **le istituzioni, le agenzie e gli organismi** dell'Unione, **nonché** gli Stati membri e i portatori di interessi del settore pubblico e privato nel miglioramento della protezione delle loro reti e dei loro sistemi informativi, nello sviluppo **e nel miglioramento delle capacità di ciberresilienza e di risposta, nonché nello sviluppo** di abilità e competenze nel campo della cibersicurezza [...].

4. L'Agenzia promuove la cooperazione e il coordinamento a livello di Unione tra gli Stati membri, le istituzioni, le agenzie e gli organismi dell'Unione e i portatori di interessi [...] **del settore pubblico e privato** su questioni relative alla cibersicurezza.

5. L'Agenzia **contribuisce a rafforzare** [...] le capacità di cibersicurezza a livello di Unione per [...] **assistere gli** Stati membri nella prevenzione delle minacce informatiche e nella reazione alle stesse, in particolare in caso di incidenti transfrontalieri.

6. L'Agenzia promuove l'uso della certificazione **con l'obiettivo di evitare la frammentazione dei sistemi di certificazione nell'UE. In particolare, l'Agenzia contribuisce** [...] all'istituzione e al mantenimento di un apposito quadro di certificazione della cibersicurezza a livello di Unione, conformemente al titolo III del presente regolamento, al fine di aumentare la trasparenza dell'affidabilità dei prodotti e dei servizi TIC in termini di cibersicurezza e di rafforzare in tal modo la fiducia nel mercato unico digitale.

7. L'Agenzia promuove un elevato livello di consapevolezza dei cittadini e delle imprese sulle questioni relative alla cibersicurezza.

CAPO I BIS

COMPITI

Articolo 5

[...] ***Sviluppo e attuazione delle politiche e della normativa dell'Unione***

L'Agenzia contribuisce allo sviluppo e all'attuazione delle politiche e della normativa dell'Unione:

1. fornendo assistenza e consulenza, in particolare fornendo un parere indipendente e lavori preparatori, per lo sviluppo e la revisione delle politiche e della normativa dell'Unione nel settore della cibersicurezza, nonché delle iniziative legislative e politiche settoriali che presentano una correlazione con le questioni relative alla cibersicurezza;

2. assistendo gli Stati membri nell'attuazione uniforme delle politiche e della normativa dell'Unione in materia di cibersicurezza, in particolare in relazione alla direttiva (UE) 2016/1148, anche mediante pareri, orientamenti, consigli e migliori pratiche su questioni quali la gestione del rischio, la segnalazione degli incidenti e la condivisione delle informazioni, e agevolando lo scambio di migliori pratiche tra le autorità competenti in materia;

3. contribuendo ai lavori del gruppo di cooperazione di cui all'articolo 11 della direttiva (UE) 2016/1148, mettendo a disposizione le proprie competenze e fornendo assistenza;

4. sostenendo:

    1) lo sviluppo e l'attuazione della politica dell'Unione nel settore dell'identificazione elettronica e dei servizi fiduciari, in particolare fornendo consulenza e orientamenti tecnici e agevolando lo scambio di migliori pratiche tra le autorità competenti;

    2) la promozione di un livello di sicurezza più elevato delle comunicazioni elettroniche, anche fornendo competenze e consulenza e agevolando lo scambio delle migliori pratiche tra le autorità competenti;

5. sostenendo il riesame periodico delle attività politiche dell'Unione attraverso una relazione annuale sullo stato di attuazione del relativo quadro giuridico per quanto riguarda:

    a) le notifiche degli incidenti degli Stati membri trasmesse dal punto di contatto unico al gruppo di cooperazione, a norma dell'articolo 10, paragrafo 3, della direttiva (UE) 2016/1148;

    b) le notifiche di violazioni della sicurezza e perdita di integrità pervenute dai prestatori di servizi fiduciari, trasmesse dagli organismi di vigilanza all'Agenzia, a norma dell'articolo 19, paragrafo 3, del regolamento (UE) n. 910/2014;

    c) le notifiche relative a [...] **incidenti di** sicurezza trasmesse dalle imprese che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, trasmesse dalle autorità competenti all'Agenzia, a norma dell'articolo 40 della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche].

Articolo 6

*[...]**Sviluppo delle capacità***

1. L'Agenzia assiste:

a) gli Stati membri nell'impegno a migliorare la prevenzione, la rilevazione e l'analisi delle [...] **minacce e degli incidenti informatici**, come pure la capacità di reazione agli stessi, fornendo loro le conoscenze e le competenze necessarie;

b) le istituzioni, [...] **le agenzie e gli organismi** dell'Unione nel loro impegno a migliorare la prevenzione, la rilevazione e l'analisi delle [...] **minacce e degli incidenti informatici**, come pure la capacità di reazione agli stessi, **in particolare** tramite un sostegno adeguato alla squadra CERT delle istituzioni, delle agenzie e degli organismi dell'Unione (CERT-UE);

c) gli Stati membri, su loro richiesta, nello sviluppo di gruppi di intervento nazionali per la sicurezza informatica in caso di incidente (CSIRT), a norma dell'articolo 9, paragrafo 5, della direttiva (UE) 2016/1148;

d) gli Stati membri, su loro richiesta, nello sviluppo di strategie nazionali in materia di sicurezza delle reti e dei sistemi informativi, a norma dell'articolo 7, paragrafo 2, della direttiva (UE) 2016/1148; l'Agenzia promuove inoltre la diffusione **e segue l'**attuazione di tali strategie [...] in tutta l'Unione allo scopo di promuovere le migliori pratiche;

e) le istituzioni dell'Unione nello sviluppo e nella revisione di strategie dell'Unione in materia di cibersicurezza, nella promozione della loro diffusione e nel monitoraggio dei progressi compiuti nella loro attuazione;

f) i CSIRT nazionali e dell'Unione nell'innalzare il livello delle loro capacità, anche attraverso la promozione del dialogo e dello scambio di informazioni, al fine di assicurare che, tenuto conto dello stato dell'arte, tutti i CSIRT soddisfino una serie comune di capacità minime e operino secondo le migliori pratiche;

g) gli Stati membri, mediante l'organizzazione delle esercitazioni **periodiche** di cibersicurezza [...] a livello di Unione di cui all'articolo 7, paragrafo 6, e la formulazione di raccomandazioni politiche basate sul processo di valutazione delle esercitazioni e sugli insegnamenti tratti da queste ultime;

h) i pertinenti enti pubblici, attraverso l'offerta di formazione sulla cibersicurezza, se del caso in cooperazione con i portatori di interessi;

i) il gruppo di cooperazione, attraverso lo scambio di migliori pratiche, in particolare per quanto riguarda l'identificazione degli operatori di servizi essenziali da parte degli Stati membri, anche in relazione alle dipendenze transfrontaliere, riguardo a rischi e incidenti, a norma dell'articolo 11, paragrafo 3, lettera l), della direttiva (UE) 2016/1148.

2. L'Agenzia **sostiene la condivisione delle informazioni intra e intersettoriale** [...], in particolare nei settori che figurano nell'allegato II della direttiva (UE) 2016/1148, fornendo migliori pratiche e orientamenti sugli strumenti disponibili, sulla procedura da seguire e su come affrontare le questioni regolamentari connesse allo scambio di informazioni.

Articolo 7

[...] ***Cooperazione operativa a livello di Unione***

1. L'Agenzia sostiene la cooperazione operativa tra gli **Stati membri, le istituzioni, le agenzie e gli organismi dell'Unione** [...] e tra i portatori di interessi.

2. L'Agenzia coopera a livello operativo e stabilisce sinergie con le istituzioni, [...] le agenzie **e gli organismi** dell'Unione, compresi la CERT-UE, i servizi che si occupano della criminalità informatica e le autorità di vigilanza che si occupano della tutela della vita privata e della protezione dei dati personali, al fine di affrontare questioni di interesse comune, anche:

a) scambiando conoscenze e migliori pratiche;

b) fornendo consulenza e orientamenti sulle questioni pertinenti relative alla cibersicurezza;

c) predisponendo, previa consultazione della Commissione, le disposizioni pratiche per l'esecuzione di compiti specifici.

3. L'Agenzia svolge le funzioni di segretariato della rete di CSIRT, a norma dell'articolo 12, paragrafo 2, della direttiva (UE) 2016/1148, **e in tale veste agevola** [...] la condivisione delle informazioni e la cooperazione tra i suoi membri.

4. L'Agenzia **sostiene la** [...] cooperazione operativa nell'ambito della rete di CSIRT fornendo sostegno agli Stati membri **, su loro richiesta,** mediante:

a) consigli su come migliorare le loro capacità di prevenzione e rilevazione degli incidenti e di risposta agli stessi;

b) [...] **l'agevolazione della gestione tecnica di** [...] incidenti aventi un impatto rilevante o sostanziale, **ivi compreso in particolare il sostegno alla condivisione volontaria di soluzioni tecniche tra gli Stati membri**;

c) l'analisi delle vulnerabilità, [...] e degli incidenti**;**

c bis) il sostegno a indagini tecniche ex post sugli incidenti aventi un impatto significativo o rilevante ai sensi della direttiva (UE) 2016/1148.

Nello svolgimento di questi compiti, l'Agenzia e la CERT-UE intraprendono una cooperazione strutturata al fine di beneficiare delle sinergie **ed evitare la duplicazione delle attività**[...].,

5. [...]

[...]

6. L'Agenzia organizza esercitazioni **periodiche**[...] di cibersicurezza a livello di Unione e, su loro richiesta, sostiene gli Stati membri e le istituzioni, le agenzie e gli organismi dell'UE nell'organizzazione di esercitazioni. **Tali esercitazioni a livello di Unione possono includere elementi tecnici, operativi o strategici** [...]. **Ogni due anni è organizzata un'esercitazione su vasta scala comprendente tutti gli elementi di cui sopra.** L'Agenzia inoltre contribuisce e aiuta ad organizzare, se del caso, esercitazioni di cibersicurezza settoriali insieme [...]**alle organizzazioni pertinenti, che possono** partecipare anche alle esercitazioni di cibersicurezza a livello di Unione.

7. L'Agenzia elabora periodicamente**, in stretta cooperazione con gli Stati membri,** una relazione sulla situazione tecnica della cibersicurezza nell'UE in merito agli incidenti e alle minacce, sulla base delle informazioni pubblicamente disponibili, della propria analisi e delle relazioni condivise, tra l'altro: dai CSIRT degli Stati membri [...] o dai punti di contatto unici istituiti dalla direttiva NIS [...] **(in entrambi i casi su base volontaria)**; dal Centro europeo per la lotta alla criminalità informatica (EC3) presso Europol e dalla CERT-UE.

8. L'Agenzia contribuisce a sviluppare una risposta cooperativa, a livello di Unione e di Stati membri, agli incidenti o alle crisi transfrontalieri su vasta scala connessi alla cibersicurezza, soprattutto:

   a) aggregando le relazioni delle fonti nazionali **condivise su base volontaria** al fine di contribuire a creare una conoscenza situazionale comune;

   b) assicurando un flusso di informazioni efficiente e la disponibilità di meccanismi di attivazione tra la rete di CSIRT e i responsabili delle decisioni politiche e tecniche a livello di Unione;

c) [...]**agevolando, su richiesta degli Stati membri,** la gestione tecnica di un incidente o di una crisi, **in particolare** [...] **sostenendo** la condivisione **volontaria** di soluzioni tecniche tra gli Stati membri;

d) sostenendo **le istituzioni, le agenzie e gli organismi dell'UE e, su richiesta, gli Stati membri nella** comunicazione pubblica in merito all'incidente o alla crisi;

e) **sostenendo gli Stati membri, su loro richiesta, nella verifica dei** [...] piani di cooperazione per rispondere a detti incidenti o crisi.

Articolo 8

[...]Mercato, certificazione della cibersicurezza e normazione

L'Agenzia:

a) sostiene e promuove lo sviluppo e l'attuazione della politica dell'Unione in materia di certificazione della cibersicurezza **dei processi,** dei prodotti e dei servizi TIC, come stabilito al titolo III del presente regolamento:

1) preparando proposte di sistemi europei di certificazione della cibersicurezza per **i processi,** i prodotti e i servizi TIC, in cooperazione con l'industria e conformemente all'articolo 44 del presente regolamento;

2) assistendo la Commissione nel provvedere alle funzioni di segretariato del gruppo europeo per la certificazione della cibersicurezza a norma dell'articolo 53 del presente regolamento;

3) elaborando e pubblicando orientamenti e sviluppando buone pratiche in merito ai requisiti di cibersicurezza dei prodotti e dei servizi TIC, in cooperazione con le autorità nazionali di [...] certificazione **della cibersicurezza** e con l'industria;

3 bis) raccomandando adeguate specifiche tecniche ai fini dello sviluppo dei sistemi europei di certificazione della cibersicurezza di cui all'articolo 47, paragrafo 1, lettera b), nei casi in cui non siano disponibili norme tecniche;

3 ter) contribuendo a uno sviluppo sufficiente delle capacità relative ai processi di valutazione e certificazione mediante l'elaborazione e la pubblicazione di orientamenti, nonché fornendo sostegno agli Stati membri su loro richiesta;

b) facilitando la definizione e l'adozione di norme europee e internazionali in materia di gestione dei rischi e di sicurezza **dei processi,** dei prodotti [...] e dei servizi TIC;

b bis) redige, in collaborazione con gli Stati membri, pareri e linee guida riguardanti i settori tecnici relativi ai requisiti di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali e concernenti altresì le norme tecniche già esistenti, comprese le norme tecniche nazionali degli Stati membri, a norma dell'articolo 19, paragrafo 2, della direttiva (UE) 2016/1148;

c) effettua regolarmente, diffondendone poi i risultati, analisi delle principali tendenze del mercato della cibersicurezza sul versante della domanda e dell'offerta, al fine di promuovere tale mercato nell'Unione.

Articolo 9

*[...]**Conoscenze* e *informazioni***[...]

L'Agenzia:

a) esegue analisi delle tecnologie emergenti e fornisce valutazioni su temi specifici in relazione agli impatti previsti, dal punto di vista sociale, giuridico, economico e regolamentare, delle innovazioni tecnologiche sulla cibersicurezza;

b) effettua analisi strategiche a lungo termine delle minacce e degli incidenti di cibersicurezza al fine di individuare le tendenze emergenti e contribuire a prevenire [...]**gli incidenti di** cibersicurezza;

c) fornisce, in cooperazione con esperti delle autorità degli Stati membri, consulenza, orientamenti e migliori pratiche per la sicurezza delle reti e dei sistemi informativi, in particolare per quanto riguarda la sicurezza delle infrastrutture [...] su cui poggiano i settori di cui all'allegato II della direttiva (UE) 2016/1148 **e di quelle utilizzate dai fornitori di servizi digitali elencati nell'allegato III di tale direttiva**;

d) raggruppa, organizza e mette a disposizione del pubblico, tramite un portale dedicato, informazioni sulla cibersicurezza, fornite dalle istituzioni, dalle agenzie e dagli organismi dell'Unione **nonché, su base volontaria, dagli Stati membri e dai portatori di interessi del settore pubblico e privato**;

e) [...]

f) raccoglie e analizza le informazioni pubblicamente disponibili sugli incidenti rilevanti e redige relazioni al fine di fornire orientamenti alle imprese e ai cittadini in tutta l'Unione.

g) [...].

Articolo 9 bis

Sensibilizzazione e istruzione

L'Agenzia:

a) sensibilizza l'opinione pubblica sui rischi connessi alla cibersicurezza e fornisce orientamenti in materia di buone pratiche per i singoli utenti destinate a cittadini e organizzazioni;

b) organizza regolarmente, in collaborazione con gli Stati membri, con le istituzioni, le agenzie e gli organismi dell'Unione e con l'industria, campagne di sensibilizzazione al fine di rafforzare la cibersicurezza e la sua visibilità nell'Unione;

c) assiste gli Stati membri nei loro sforzi di sensibilizzazione e promuove l'istruzione in materia di cibersicurezza;

d) incoraggia un miglior coordinamento e scambio di migliori pratiche tra gli Stati membri per l'istruzione e la sensibilizzazione in materia di cibersicurezza agevolando la creazione e il mantenimento di una rete di punti di contatto nazionali in materia di istruzione.

Articolo 10

*[...]**Ricerca e innovazione***

Per quanto riguarda la ricerca e l'innovazione, l'Agenzia:

a) fornisce consulenza all'Unione e agli Stati membri sulle esigenze e le priorità in materia di ricerca nel settore della cibersicurezza, al fine di consentire di reagire in maniera efficace ai rischi e alle minacce attuali ed emergenti, anche per quanto riguarda le tecnologie dell'informazione e della comunicazione nuove ed emergenti, e di utilizzare efficacemente le tecnologie per la prevenzione dei rischi;

b) partecipa, qualora la Commissione le abbia delegato i pertinenti poteri, alla fase di attuazione dei programmi di finanziamento per la ricerca e l'innovazione o in qualità di beneficiario.

Articolo 11

[...]Cooperazione internazionale

L'Agenzia contribuisce all'impegno dell'Unione nella cooperazione con i paesi terzi e le organizzazioni internazionali per promuovere la cooperazione internazionale sulle questioni connesse alla cibersicurezza:

a) impegnandosi, ove opportuno, in qualità di osservatore e nell'organizzazione delle esercitazioni internazionali, nonché analizzando i risultati di tali esercitazioni e comunicandoli al consiglio di amministrazione;

b) agevolando, [...] **all'interno dei pertinenti quadri di cooperazione internazionale**, lo scambio di migliori pratiche[...];

c) fornendo competenze specialistiche alla Commissione su richiesta**;**

c bis) fornendo, in collaborazione con il gruppo europeo per la certificazione della cibersicurezza di cui all'articolo 53, consulenza e assistenza alla Commissione su questioni concernenti gli accordi per il riconoscimento reciproco dei certificati di cibersicurezza con i paesi terzi.

CAPO II

ORGANIZZAZIONE DELL'AGENZIA

Articolo 12

Struttura

La struttura amministrativa e di gestione dell'Agenzia è composta da:

a) un consiglio di amministrazione, che esercita le funzioni di cui all'articolo 14;

b) un comitato esecutivo, che esercita le funzioni di cui all'articolo 18;

c) un direttore esecutivo, che esercita le funzioni di cui all'articolo 19;[...]

d) un gruppo permanente di portatori di interessi che esercita le funzioni di cui all'articolo 20**;**

d bis) una rete dei funzionari nazionali di collegamento, che esercita le funzioni di cui all'articolo 20 bis;

SEZIONE 1

CONSIGLIO DI AMMINISTRAZIONE

Articolo 13

Composizione del consiglio di amministrazione

1. Il consiglio di amministrazione è composto da un rappresentante per ciascuno Stato membro e due rappresentanti nominati dalla Commissione. Tutti i rappresentanti hanno diritto di voto.

2. Ciascun membro del consiglio di amministrazione ha un supplente che lo rappresenta in sua assenza.

3. I membri del consiglio di amministrazione e i loro supplenti sono nominati in base alle loro conoscenze in materia di cibersicurezza, tenendo conto delle pertinenti competenze gestionali, amministrative e di bilancio. La Commissione e gli Stati membri si sforzano di limitare l'avvicendamento dei loro rappresentanti nel consiglio di amministrazione, al fine di assicurarne la continuità dei lavori. La Commissione e gli Stati membri mirano a conseguire una rappresentanza equilibrata tra uomini e donne nel consiglio di amministrazione.

4. La durata del mandato dei membri del consiglio di amministrazione e dei loro supplenti è di quattro anni. Il mandato è rinnovabile.

Articolo 14

Funzioni del consiglio di amministrazione

1. Il consiglio di amministrazione:

a) definisce gli orientamenti generali del funzionamento dell'Agenzia e assicura che operi secondo le norme e i principi stabiliti dal presente regolamento. Assicura inoltre la coerenza del lavoro dell'Agenzia con le attività svolte dagli Stati membri e a livello di Unione;

b) adotta il progetto di documento unico di programmazione dell'Agenzia di cui all'articolo 21 prima che venga trasmesso alla Commissione per parere;

c) adotta, tenendo conto del parere della Commissione, il documento unico di programmazione dell'Agenzia a maggioranza dei due terzi dei membri e conformemente all'articolo 17;

c bis) vigila sull'attuazione della programmazione annuale e pluriennale contenuta nel documento unico di programmazione;

d) adotta, a maggioranza dei due terzi dei membri, il bilancio annuale dell'Agenzia ed esercita altre funzioni in relazione al bilancio dell'Agenzia a norma del capo III;

e) valuta e adotta la relazione annuale consolidata sulle attività dell'Agenzia e trasmette, entro il 1° luglio dell'anno successivo, sia la relazione che la sua valutazione al Parlamento europeo, al Consiglio, alla Commissione e alla Corte dei conti. La relazione annuale include i conti e descrive in che modo l'Agenzia ha conseguito i propri indicatori di risultato. La relazione annuale è resa pubblica;

f) adotta la regolamentazione finanziaria applicabile all'Agenzia in conformità dell'articolo 29;

g) adotta una strategia antifrode, proporzionata ai rischi di frode, tenendo conto dei costi e dei benefici delle misure da attuare;

h) adotta norme di prevenzione e gestione dei conflitti di interesse in relazione ai suoi membri;

i) garantisce un seguito adeguato alle risultanze e alle raccomandazioni derivanti dalle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e dalle relazioni di revisione contabile e valutazioni interne o esterne.

j) adotta il proprio regolamento interno;

k) a norma del paragrafo 2, esercita, nei confronti del personale dell'Agenzia, i poteri conferiti dallo statuto dei funzionari all'autorità che ha il potere di nomina e dal regime applicabile agli altri agenti dell'Unione europea all'autorità abilitata a concludere i contratti di assunzione ("poteri dell'autorità che ha il potere di nomina");

l) adotta le norme di esecuzione dello statuto dei funzionari e del regime applicabile agli altri agenti secondo la procedura di cui all'articolo 110 dello statuto dei funzionari;

m) nomina il direttore esecutivo e, se del caso, ne proroga il mandato o lo rimuove dall'incarico, a norma dell'articolo 33 del presente regolamento;

n) nomina un contabile, che può essere il contabile della Commissione, che opera in piena indipendenza nell'esercizio delle sue funzioni;

o) prende tutte le decisioni sull'istituzione delle strutture interne dell'Agenzia e, se necessario, sulla relativa modifica, in considerazione delle necessità per l'attività dell'Agenzia e secondo una gestione di bilancio sana;

p) autorizza la conclusione di accordi operativi conformemente agli articoli 7 e 39.

2. Il consiglio di amministrazione adotta, in conformità dell'articolo 110 dello statuto dei funzionari, una decisione basata sull'articolo 2, paragrafo 1, dello statuto dei funzionari e sull'articolo 6 del regime applicabile agli altri agenti, con cui delega al direttore esecutivo i poteri di autorità che ha il potere di nomina e stabilisce le condizioni di sospensione della delega di poteri. Il direttore esecutivo è autorizzato a subdelegare tali poteri.

3. Qualora circostanze eccezionali lo richiedano, il consiglio di amministrazione può, mediante decisione, sospendere temporaneamente la delega dei poteri di autorità che ha il potere di nomina delegati al direttore esecutivo e quelli subdelegati da quest'ultimo ed esercitarli esso stesso o delegarli a uno dei suoi membri o a un membro del personale diverso dal direttore esecutivo.

Articolo 15

Presidente del consiglio di amministrazione

Il consiglio di amministrazione elegge tra i propri membri, a maggioranza dei due terzi dei membri, un presidente e un vicepresidente con un mandato di quattro anni, rinnovabile una sola volta. Tuttavia, qualora il presidente o il vicepresidente cessino di far parte del consiglio di amministrazione in un qualsiasi momento in corso di mandato, questo giunge automaticamente a termine alla stessa data. Il vicepresidente sostituisce ex officio il presidente nel caso in cui quest'ultimo non sia in grado di svolgere i propri compiti.

Articolo 16

Riunioni del consiglio di amministrazione

1. Il consiglio di amministrazione si riunisce su convocazione del suo presidente.

2. Il consiglio di amministrazione tiene almeno due riunioni ordinarie l'anno. Si riunisce inoltre in seduta straordinaria su richiesta del presidente, della Commissione o di almeno un terzo dei suoi membri.

3. Il direttore esecutivo partecipa, senza diritto di voto, alle riunioni del consiglio di amministrazione.

4. I membri del gruppo permanente di portatori di interessi, su invito del presidente, possono partecipare senza diritto di voto alle riunioni del consiglio di amministrazione.

5. I membri del consiglio di amministrazione e i loro supplenti possono farsi assistere da consulenti o esperti, fatte salve le disposizioni del regolamento interno.

6. L'Agenzia provvede alle funzioni di segretariato del consiglio di amministrazione.

Articolo 17

Modalità di voto del consiglio di amministrazione

1. Il consiglio di amministrazione adotta le proprie decisioni a maggioranza dei suoi membri.

2. La maggioranza di due terzi di tutti i membri del consiglio di amministrazione è necessaria per il documento unico di programmazione, il bilancio annuale, la nomina del direttore esecutivo, la proroga del suo mandato o la sua rimozione dall'incarico.

3. Ogni membro dispone di un voto. In assenza di un membro, il supplente è abilitato a esercitare il suo diritto di voto.

4. Il presidente partecipa al voto.

5. Il direttore esecutivo non partecipa al voto.

6. Il regolamento interno del consiglio di amministrazione stabilisce le regole dettagliate concernenti la votazione, in particolare le circostanze in cui un membro può agire per conto di un altro.

SEZIONE 2
COMITATO ESECUTIVO

Articolo 18

Comitato esecutivo

1. Il consiglio direttivo è assistito da un comitato esecutivo.

2. Il comitato esecutivo:

   a) prepara le decisioni che dovranno essere adottate dal consiglio di amministrazione;

   b) insieme con il consiglio di amministrazione, garantisce un seguito adeguato alle risultanze e alle raccomandazioni derivanti dalle indagini svolte dall'OLAF, nonché dalle relazioni di revisione contabile e valutazioni interne ed esterne;

   c) fatte salve le responsabilità del direttore esecutivo quali stabilite all'articolo 19, fornisce assistenza e consulenza al direttore esecutivo nell'attuazione delle decisioni del consiglio di amministrazione sulle questioni amministrative e di bilancio di cui all'articolo 19.

3. Il comitato esecutivo consta di cinque membri designati tra i membri del consiglio di amministrazione, tra cui figurano il presidente del consiglio di amministrazione, il quale può anche presiedere il comitato esecutivo, e un rappresentante della Commissione. Il direttore esecutivo partecipa alle riunioni del comitato esecutivo senza diritto di voto.

4. La durata del mandato dei membri del consiglio di amministrazione è di quattro anni. Il mandato è rinnovabile.

5. Il comitato esecutivo si riunisce almeno una volta ogni tre mesi. Il presidente del comitato esecutivo convoca riunioni supplementari su richiesta dei suoi membri.

6. Il consiglio di amministrazione stabilisce il regolamento interno del comitato esecutivo.

7. [...]

SEZIONE 3
DIRETTORE ESECUTIVO

Articolo 19

Compiti del direttore esecutivo

1. L'Agenzia è diretta dal suo direttore esecutivo che è indipendente nell'espletamento delle sue funzioni. Il direttore esecutivo risponde al consiglio di amministrazione.

2. Su richiesta, il direttore esecutivo riferisce al Parlamento europeo sull'esercizio delle sue funzioni. Il Consiglio può invitare il direttore esecutivo a riferire sull'esercizio delle sue funzioni.

3. Il direttore esecutivo ha la responsabilità di:

a) provvedere all'amministrazione corrente dell'Agenzia;

b) attuare le decisioni adottate dal consiglio di amministrazione;

c) preparare il documento unico di programmazione e presentarlo al consiglio di amministrazione per approvazione prima di trasmetterlo alla Commissione;

d) attuare il documento unico di programmazione e riferire in merito al consiglio di amministrazione;

e) elaborare la relazione annuale consolidata sulle attività dell'Agenzia, **compresa l'attuazione del programma di lavoro annuale,** e presentarla al consiglio di amministrazione per valutazione e adozione;

f) predisporre un piano d'azione per dare seguito alle conclusioni delle valutazioni retrospettive e riferire ogni due anni alla Commissione sui progressi compiuti;

g) predisporre un piano d'azione a seguito delle conclusioni delle relazioni di revisione contabile interne ed esterne e delle indagini dell'Ufficio europeo per la lotta antifrode (OLAF) e riferire due volte l'anno sui progressi compiuti alla Commissione e periodicamente al consiglio di amministrazione;

h) predisporre il progetto della regolamentazione finanziaria applicabile all'Agenzia;

i) predisporre il progetto di stato di previsione delle entrate e delle spese dell'Agenzia e l'esecuzione del bilancio;

j) proteggere gli interessi finanziari dell'Unione mediante l'applicazione di misure preventive contro la frode, la corruzione e qualsiasi altra attività illecita, mediante controlli efficaci e, in caso di irregolarità rilevate, mediante il recupero degli importi erroneamente versati e, se del caso, mediante sanzioni amministrative e pecuniarie efficaci, proporzionate e dissuasive;

k) elaborare una strategia antifrode dell'Agenzia e presentarla al consiglio di amministrazione per approvazione;

l) sviluppare e mantenere i contatti con le imprese e le organizzazioni dei consumatori per assicurare un dialogo regolare con i portatori di interessi;

l bis) comunicare periodicamente con le istituzioni, le agenzie e gli organismi dell'Unione riguardo alle loro attività in materia di cibersicurezza, al fine di garantire la coerenza nello sviluppo e nell'attuazione delle politiche dell'UE;

m) svolgere gli altri compiti attribuiti al direttore esecutivo dal presente regolamento.

4. In base alle esigenze e nell'ambito del mandato dell'Agenzia, e conformemente ai suoi obiettivi e compiti, il direttore esecutivo può istituire gruppi di lavoro ad hoc composti da esperti, anche inviati dalle autorità competenti degli Stati membri. Il consiglio di amministrazione ne è informato in anticipo. Le procedure relative in particolare alla composizione dei gruppi di lavoro, alla nomina degli esperti dei gruppi di lavoro da parte del direttore esecutivo e il funzionamento dei gruppi di lavoro sono specificati nel regolamento interno dell'Agenzia.

5. **Se necessario, per svolgere i compiti dell'Agenzia in maniera efficiente ed efficace e in base a un'adeguata analisi costi-benefici, il direttore esecutivo può decidere [...] di istituire uno o più uffici locali in uno o più Stati membri.** Prima di decidere di istituire un ufficio locale, il direttore esecutivo **chiede il parere dello Stato membro o degli Stati membri interessati, compreso lo Stato membro che ospita la sede dell'Agenzia, e** ottiene il consenso della Commissione **e** del consiglio di amministrazione. **In caso di disaccordo durante il processo di consultazione tra il direttore esecutivo e gli Stati membri interessati, la questione è sottoposta all'esame del Consiglio.** La decisione precisa la gamma di attività che devono essere espletate presso l'ufficio locale al fine di evitare costi inutili e duplicazioni di funzioni amministrative dell'Agenzia.[...] **Il numero del personale in tutti gli uffici locali è ridotto al minimo e non supera in totale il 40% del numero del personale nello Stato membro che ospita la sede dell'Agenzia. Il numero del personale in ciascuno degli uffici locali non supera il 10% del numero [...] del personale nello Stato membro che ospita la sede dell'Agenzia.**

SEZIONE 4
GRUPPO PERMANENTE DEI PORTATORI DI INTERESSI

Articolo 20

Gruppo permanente dei portatori di interessi

1. Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce un gruppo permanente di portatori di interessi composto da esperti riconosciuti che rappresentano i portatori di interessi, quali il settore delle TIC, i fornitori delle reti o dei servizi di comunicazione elettronica accessibili al pubblico, **gli operatori di servizi essenziali,** le organizzazioni dei consumatori, gli esperti universitari in materia di cibersicurezza e i rappresentanti delle autorità competenti notificati a norma della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche], nonché le autorità di contrasto e le autorità di controllo preposte alla protezione dei dati.

2. Le procedure per il gruppo permanente di portatori di interessi, in particolare per quanto riguarda il numero, la composizione e la nomina dei membri da parte del consiglio di amministrazione, la proposta del direttore esecutivo e il funzionamento del gruppo sono specificati nel regolamento interno dell'Agenzia e resi pubblici.

3. Il gruppo permanente di portatori di interessi è presieduto dal direttore esecutivo o da qualsiasi altra persona nominata dal direttore esecutivo caso per caso.

4. Il mandato dei membri del gruppo permanente di portatori di interessi è di due anni e mezzo. I membri del consiglio di amministrazione non possono essere membri del gruppo permanente di portatori di interessi. Gli esperti della Commissione e degli Stati membri sono autorizzati a presenziare alle riunioni del gruppo permanente di portatori di interessi e a partecipare alle sue attività. I rappresentanti di altri organismi considerati pertinenti dal direttore esecutivo che non sono membri del gruppo permanente di portatori di interessi possono essere invitati a partecipare alle riunioni di tale gruppo e alle sue attività.

5. Il gruppo permanente di portatori di interessi fornisce consulenza all'Agenzia relativamente allo svolgimento delle sue attività. In particolare, esso consiglia il direttore esecutivo ai fini della stesura della proposta relativa al programma di lavoro dell'Agenzia e della comunicazione con i relativi portatori di interessi su tutte le questioni inerenti al programma di lavoro.

5 bis. Il gruppo permanente dei portatori di interessi informa periodicamente il consiglio di amministrazione sulle sue attività.

SEZIONE 4 BIS

RETE DEI FUNZIONARI NAZIONALI DI COLLEGAMENTO

Articolo 20 bis

Rete dei funzionari nazionali di collegamento

1. Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce una rete dei funzionari nazionali di collegamento composta da rappresentanti degli Stati membri.

2. La rete dei funzionari nazionali di collegamento è composta dai rappresentanti di tutti gli Stati membri. Ciascuno Stato membro designa un rappresentante. Le riunioni della rete possono svolgersi in diverse composizioni di esperti.

3. In particolare, la rete dei funzionari nazionali di collegamento agevola lo scambio di informazioni tra l'ENISA e gli Stati membri. Essa sostiene in particolare l'ENISA nella diffusione, in tutta l'UE, tra le pertinenti parti interessate delle attività, dei risultati e delle raccomandazioni che la riguardano.

4. I funzionari nazionali di collegamento fungono da punti di contatto specifici a livello nazionale per agevolare la cooperazione tra l'ENISA e gli esperti nazionali nel contesto dell'attuazione del programma di lavoro dell'ENISA.

5. Mentre i funzionari nazionali di collegamento dovrebbero cooperare strettamente con i rappresentanti del consiglio di amministrazione dei rispettivi paesi, la rete in sé non duplica il lavoro né del consiglio di amministrazione né di altri organismi dell'UE.

6. Le funzioni e le procedure relative alla rete dei funzionari nazionali di collegamento sono specificate nel regolamento interno dell'Agenzia e rese pubbliche.

SEZIONE 5
FUNZIONAMENTO

Articolo 21

Documento unico di programmazione

1. L'Agenzia svolge la sua attività in conformità di un documento unico di programmazione contenente la programmazione annuale e pluriennale, che include tutte le attività pianificate.

2. Ogni anno il direttore esecutivo, tenendo conto degli orientamenti stabiliti della Commissione, predispone un progetto di documento unico di programmazione contenente la pianificazione delle risorse umane e finanziarie corrispondenti, secondo quanto previsto all'articolo 32 del regolamento delegato (UE) n. 1271/2013 della Commissione[14].

3. Entro il 30 novembre di ogni anno il consiglio di amministrazione adotta il documento unico di programmazione di cui al paragrafo 1 e lo trasmette al Parlamento europeo, al Consiglio e alla Commissione entro il 31 gennaio dell'anno successivo, nonché eventuali versioni aggiornate di tale documento.

4. Il documento unico di programmazione diventa definitivo dopo l'approvazione definitiva del bilancio generale dell'Unione e, se necessario, è adeguato di conseguenza.

5. Il programma di lavoro annuale comprende gli obiettivi dettagliati e i risultati attesi, compresi gli indicatori di risultato. Esso contiene inoltre una descrizione delle azioni da finanziare e un'indicazione delle risorse finanziarie e umane assegnate a ciascuna azione, conformemente ai principi di formazione del bilancio per attività e gestione per attività. Il programma di lavoro annuale è coerente con il programma di lavoro pluriennale di cui al paragrafo 7. Indica chiaramente i compiti aggiunti, modificati o soppressi rispetto all'esercizio finanziario precedente.

---

[14] Regolamento delegato (UE) n. 1271/2013 della Commissione, del 30 settembre 2013, che stabilisce il regolamento finanziario quadro degli organismi di cui all'articolo 208 del regolamento (UE, Euratom) n. 966/2012 del Parlamento europeo e del Consiglio (GU L 328 del 7.12.2013, pag. 42).

6. Quando all'Agenzia è assegnato un nuovo compito, il consiglio di amministrazione modifica il programma di lavoro annuale adottato. Le modifiche sostanziali del programma di lavoro annuale sono adottate con la stessa procedura di quella applicabile al programma di lavoro annuale iniziale. Il consiglio di amministrazione può delegare al direttore esecutivo il potere di apportare modifiche non sostanziali al programma di lavoro annuale.

7. Il programma di lavoro pluriennale definisce la programmazione strategica generale, compresi gli obiettivi, i risultati attesi e gli indicatori di prestazione. Riporta inoltre la programmazione delle risorse, compresi il bilancio pluriennale e il personale.

8. La programmazione delle risorse è aggiornata ogni anno. La programmazione strategica è aggiornata secondo necessità, in particolare per adattarla all'esito della valutazione di cui all'articolo 56.

Articolo 22

Dichiarazione di interessi

1. I membri del consiglio di amministrazione, il direttore esecutivo, come pure i funzionari distaccati dagli Stati membri a titolo temporaneo, rendono ciascuno una dichiarazione di impegni e una dichiarazione con la quale indicano l'assenza o la presenza di interessi diretti o indiretti che possano essere considerati in contrasto con la loro indipendenza. Le dichiarazioni sono precise e complete, presentate ogni anno per iscritto e aggiornate ogniqualvolta sia necessario.

2. I membri del consiglio di amministrazione, il direttore esecutivo e gli esperti esterni che partecipano ai gruppi di lavoro ad hoc dichiarano ciascuno in modo preciso e completo, al più tardi all'inizio di ogni riunione, qualsiasi interesse che possa essere considerato in contrasto con la loro indipendenza in relazione ai punti all'ordine del giorno e si astengono dal partecipare alle discussioni e alle votazioni inerenti tali punti.

3. L'Agenzia stabilisce nel proprio regolamento interno le disposizioni pratiche per le norme sulle dichiarazioni di interessi di cui ai paragrafi 1 e 2.

Articolo 23

Trasparenza

1. L'Agenzia svolge le proprie attività con un livello elevato di trasparenza e nel rispetto dell'articolo 25.

2. L'Agenzia provvede a che il pubblico e le parti interessate dispongano di informazioni appropriate, obiettive, affidabili e facilmente accessibili, in particolare sui risultati del suo lavoro. Inoltre, rende pubbliche le dichiarazioni di interessi rese a norma dell'articolo 22.

3. Il consiglio di amministrazione, su proposta del direttore esecutivo, può autorizzare le parti interessate a presenziare in qualità di osservatori allo svolgimento di alcune attività dell'Agenzia.

4. L'Agenzia stabilisce nel proprio regolamento interno le disposizioni pratiche per l'attuazione delle regole di trasparenza di cui ai paragrafi 1 e 2.

Articolo 24

Riservatezza

1. Fatto salvo l'articolo 25, l'Agenzia non rivela a terzi le informazioni da essa trattate o ricevute in relazione alle quali è stata presentata una richiesta motivata di trattamento riservato, integralmente o in parte.

2. I membri del consiglio di amministrazione, il direttore esecutivo, i membri del gruppo permanente di portatori di interessi, gli esperti esterni che partecipano ai gruppi di lavoro ad hoc e il personale dell'Agenzia, compresi i funzionari distaccati dagli Stati membri a titolo temporaneo, rispettano gli obblighi di riservatezza di cui all'articolo 339 del trattato sul funzionamento dell'Unione europea (TFUE) anche dopo la cessazione delle proprie funzioni.

3. L'Agenzia stabilisce nel proprio regolamento interno le disposizioni pratiche per l'attuazione delle regole di riservatezza di cui ai paragrafi 1 e 2.

4. Se necessario ai fini dell'esecuzione dei compiti dell'Agenzia, il consiglio di amministrazione decide di consentire all'Agenzia di trattare informazioni riservate. In questo caso, il consiglio di amministrazione, in accordo con i servizi della Commissione, adotta un regolamento interno che applichi i principi di sicurezza enunciati nelle decisioni (UE, Euratom) 2015/443[15] e 2015/444[16] della Commissione. Tale regolamento disciplina, tra l'altro, lo scambio, il trattamento e la conservazione di informazioni classificate.

---

15 Decisione (UE, Euratom) 2015/443 della Commissione, del 13 marzo 2015, sulla sicurezza nella Commissione (GU L 72 del 17.3.2015, pag. 41).

16 Decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per proteggere le informazioni classificate UE (GU L 72 del 17.3.2015, pag. 53).

Articolo 25

Accesso ai documenti

1. Il regolamento (CE) n. 1049/2001 si applica ai documenti detenuti dall'Agenzia.

2. Entro sei mesi dall'istituzione dell'Agenzia, il consiglio di amministrazione adotta disposizioni per l'attuazione del regolamento (CE) n. 1049/2001.

3. Le decisioni adottate dall'Agenzia a norma dell'articolo 8 del regolamento (CE) n. 1049/2001 possono formare oggetto di una denuncia presentata al Mediatore europeo a norma dell'articolo 228 TFUE o di un ricorso dinanzi alla Corte di giustizia dell'Unione europea a norma dell'articolo 263 TFUE.

CAPO III
FORMAZIONE E STRUTTURA DEL BILANCIO

Articolo 26

Formazione del bilancio

1. Ogni anno il direttore esecutivo redige un progetto di stato di previsione delle entrate e delle spese dell'Agenzia per l'esercizio finanziario successivo e lo trasmette al consiglio di amministrazione, corredato di un progetto di tabella dell'organico. Le entrate e le spese risultano in pareggio.

2. Ogni anno il consiglio di amministrazione elabora, sulla base del progetto di stato di previsione delle entrate e delle spese di cui al paragrafo 1, lo stato di previsione delle entrate e delle spese dell'Agenzia per l'esercizio finanziario successivo.

3. Entro il 31 gennaio di ogni anno il consiglio di amministrazione invia lo stato di previsione di cui al paragrafo 2, come parte integrante del progetto di documento unico di programmazione, alla Commissione e ai paesi terzi con cui l'Unione ha concluso accordi a norma dell'articolo 39.

4. Sulla base di tale stato di previsione, la Commissione iscrive le stime che ritiene necessarie per quanto concerne la tabella dell'organico e l'importo del contributo a carico del bilancio generale nel progetto di bilancio dell'Unione che sottopone al Parlamento europeo e al Consiglio conformemente all'articolo 314 TFUE.

5. Il Parlamento europeo e il Consiglio autorizzano gli stanziamenti a titolo del contributo destinato all'Agenzia.

6. Il Parlamento europeo e il Consiglio adottano la tabella dell'organico dell'Agenzia.

7. Insieme al documento unico di programmazione, il consiglio di amministrazione adotta il bilancio dell'Agenzia. Esso diventa definitivo dopo l'adozione definitiva del bilancio generale dell'Unione. Se del caso, il consiglio di amministrazione modifica il bilancio e il documento unico di programmazione dell'Agenzia per conformarli al bilancio generale dell'Unione.

Articolo 27

Struttura del bilancio

1. Fatte salve altre risorse, le entrate dell'Agenzia comprendono:

   a) un contributo dal bilancio dell'Unione;

   b) entrate con destinazione specifica volte a finanziare spese specifiche conformemente alla regolamentazione finanziaria di cui all'articolo 29;

   c) finanziamenti dell'Unione sotto forma di accordi di delega o di sovvenzioni ad hoc secondo la regolamentazione finanziaria di cui all'articolo 29 e le disposizioni dei pertinenti strumenti di sostegno alle politiche dell'Unione;

d) contributi dei paesi terzi che partecipano ai lavori dell'Agenzia a norma dell'articolo 39;

e) eventuali contributi volontari degli Stati membri, in denaro o in natura; Gli Stati membri che versano contributi volontari non possono rivendicare alcun diritto o servizio specifico per effetto di tale contributo.

2. Le spese dell'Agenzia comprendono la retribuzione del personale, l'assistenza amministrativa e tecnica, le spese infrastrutturali e di esercizio, nonché quelle conseguenti a contratti stipulati con terzi.

Articolo 28

Esecuzione del bilancio

1. Il direttore esecutivo è responsabile dell'esecuzione del bilancio dell'Agenzia.

2. Il revisore contabile interno della Commissione esercita nei confronti dell'Agenzia le stesse competenze di cui dispone nei confronti dei servizi della Commissione.

3. Entro il 1° marzo successivo alla chiusura dell'esercizio (1° marzo dell'anno N + 1), il contabile dell'Agenzia comunica i conti provvisori al contabile della Commissione e alla Corte dei conti.

4. In seguito al ricevimento delle osservazioni della Corte dei conti sui conti provvisori dell'Agenzia, il contabile dell'Agenzia redige i conti definitivi sotto la propria responsabilità.

5. Il direttore esecutivo li presenta al consiglio di amministrazione per parere.

6. Entro il 31 marzo dell'anno N + 1, il direttore esecutivo trasmette la relazione sulla gestione di bilancio e finanziaria al Parlamento europeo, al Consiglio, alla Commissione e alla Corte dei conti.

7. Entro il 1° luglio dell'anno N + 1, il contabile trasmette i conti definitivi, accompagnati dal parere del consiglio di amministrazione, al Parlamento europeo, al Consiglio, al contabile della Commissione e alla Corte dei conti.

8. Allo scadere del termine previsto per la trasmissione dei conti definitivi, il contabile trasmette altresì alla Corte dei conti, e in copia al contabile della Commissione, una dichiarazione ad essi relativa.

9. Il direttore esecutivo pubblica i conti definitivi entro il 15 novembre dell'anno successivo.

10. Entro il 30 settembre dell'anno N + 1 il direttore esecutivo invia alla Corte dei conti una risposta alle osservazioni da essa formulate e ne trasmette copia al consiglio di amministrazione e alla Commissione.

11. Il direttore esecutivo presenta al Parlamento europeo, su richiesta di quest'ultimo, tutte le informazioni necessarie al corretto svolgimento della procedura di discarico per l'esercizio in oggetto, conformemente all'articolo 165, paragrafo 3, del regolamento finanziario.

12. Il Parlamento europeo, su raccomandazione del Consiglio, concede il discarico al direttore esecutivo, entro il 15 maggio dell'anno N + 2, per l'esecuzione del bilancio dell'esercizio N.

Articolo 29

Regolamentazione finanziaria

La regolamentazione finanziaria applicabile all'Agenzia è adottata dal consiglio di amministrazione previa consultazione della Commissione. Essa si discosta dal regolamento (UE) n. 1271/2013 solo per esigenze specifiche di funzionamento dell'Agenzia e previo accordo della Commissione.

Articolo 30

Lotta antifrode

1. Per facilitare la lotta contro la frode, la corruzione e altre attività illecite ai sensi del regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio[17], entro sei mesi dalla data in cui diventa operativa l'Agenzia aderisce all'accordo interistituzionale del 25 maggio 1999 relativo alle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e adotta le opportune disposizioni valide per l'insieme dei dipendenti dell'Agenzia, utilizzando i modelli riportati nell'allegato di tale accordo.

2. La Corte dei conti ha il potere di revisione contabile, esercitabile sulla base di documenti e sul posto, su tutti i beneficiari di sovvenzioni, contraenti e subcontraenti cui l'Agenzia ha concesso finanziamenti dell'Unione.

[17] Regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio, dell'11 settembre 2013, relativo alle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e che abroga il regolamento (CE) n. 1073/1999 del Parlamento europeo e del Consiglio e il regolamento (Euratom) n. 1074/1999 del Consiglio (GU L 248 del 18.9.2013, pag. 1).

3. L'OLAF può eseguire indagini, compresi controlli e verifiche sul posto, in conformità delle disposizioni e delle procedure stabilite dal regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio e dal regolamento (Euratom, CE) n. 2185/96 del Consiglio[18], dell'11 novembre 1996, relativo ai controlli e alle verifiche sul posto effettuati dalla Commissione ai fini della tutela degli interessi finanziari dell'Unione contro le frodi e altre irregolarità, per accertare casi di frode, corruzione o altre attività illecite lesive degli interessi finanziari dell'Unione in relazione a sovvenzioni o contratti finanziati dall'Agenzia.

4. Fatti salvi i paragrafi 1, 2 e 3, gli accordi di cooperazione con paesi terzi e organizzazioni internazionali, i contratti, le convenzioni di sovvenzione e le decisioni di sovvenzione dell'Agenzia contengono disposizioni che autorizzano esplicitamente la Corte dei conti e l'OLAF a procedere a tali revisioni contabili e indagini conformemente alle loro rispettive competenze.

CAPO IV
PERSONALE DELL'AGENZIA

Articolo 31

Disposizioni generali

Al personale dell'Agenzia si applicano lo statuto dei funzionari, il regime applicabile agli altri agenti e le norme adottate di comune accordo dalle istituzioni dell'Unione per dare applicazione a detto statuto.

---

18 Regolamento (Euratom, CE) n 2185/96 del Consiglio, dell'11 novembre 1996, relativo ai controlli e alle verifiche sul posto effettuati dalla Commissione ai fini della tutela degli interessi finanziari delle Comunità europee contro le frodi e altre irregolarità (GU L 292 del 15.11.1996, pag. 2).

Articolo 32

Privilegi e immunità

All'Agenzia e al suo personale si applica il protocollo n. 7 sui privilegi e sulle immunità dell'Unione europea allegato al trattato sull'Unione europea e al TFUE.

Articolo 33

Direttore esecutivo

1. Il direttore esecutivo è assunto come agente temporaneo dell'Agenzia ai sensi dell'articolo 2, lettera a), del regime applicabile agli altri agenti.

2. Il direttore esecutivo è nominato dal consiglio di amministrazione in base a un elenco di candidati proposto dalla Commissione, secondo una procedura di selezione aperta e trasparente.

3. Ai fini della conclusione del contratto del direttore esecutivo, l'Agenzia è rappresentata dal presidente del consiglio di amministrazione.

4. Prima di essere nominato, il candidato selezionato dal consiglio di amministrazione è invitato a fare una dichiarazione dinanzi alla commissione competente del Parlamento europeo e a rispondere alle domande dei deputati.

5. La durata del mandato del direttore esecutivo è di **quattro** [...] anni. Entro la fine di tale periodo, la Commissione esegue una valutazione che tiene conto della prestazione del direttore esecutivo e dei compiti e delle sfide futuri dell'Agenzia.

6. Il consiglio di amministrazione adotta le decisioni riguardanti la nomina del direttore esecutivo, la proroga del suo mandato e la sua rimozione dall'incarico a maggioranza di due terzi dei suoi membri con diritto di voto.

7. Agendo su proposta della Commissione, la quale tiene conto della valutazione di cui al paragrafo 5, il consiglio di amministrazione può prorogare il mandato del direttore esecutivo una sola volta, per non più di **quattro** [...] anni.

8. Il consiglio di amministrazione informa il Parlamento europeo dell'intenzione di prorogare il mandato del direttore esecutivo. Entro i tre mesi che precedono tale proroga, il direttore esecutivo, se invitato, fa una dichiarazione davanti alla commissione competente del Parlamento europeo e risponde alle domande dei deputati.

9. Un direttore esecutivo il cui mandato sia stato prorogato non può partecipare a un'altra procedura di selezione per lo stesso posto.

10. Il direttore esecutivo può essere rimosso dal suo incarico solo su decisione del consiglio di amministrazione [...].

Articolo 34

Esperti nazionali distaccati e altro personale

1. L'Agenzia può avvalersi di esperti nazionali distaccati o di altro personale non alle sue dipendenze. Lo statuto dei funzionari e il regime applicabile agli altri agenti non si applicano a tale personale.

2. Il consiglio di amministrazione adotta una decisione che stabilisce le norme relative al distacco di esperti nazionali presso l'Agenzia.

CAPO V
DISPOSIZIONI GENERALI

Articolo 35

Status giuridico dell'Agenzia

1. L'Agenzia è un organismo dell'Unione ed è dotata di personalità giuridica.

2. L'Agenzia gode, in ciascuno Stato membro, della più ampia capacità giuridica riconosciuta alle persone giuridiche dalla legislazione nazionale. In particolare, essa può acquistare o alienare beni mobili e immobili e può stare in giudizio.

3. L'Agenzia è rappresentata dal direttore esecutivo.

Articolo 36

Responsabilità dell'Agenzia

1. La responsabilità contrattuale dell'Agenzia è disciplinata dalla normativa applicabile al contratto.

2. La Corte di giustizia dell'Unione europea è competente a giudicare in virtù di clausole compromissorie contenute nel contratto concluso dall'Agenzia.

3. In materia di responsabilità extracontrattuale, l'Agenzia è obbligata, secondo i principi generali comuni agli ordinamenti degli Stati membri, al risarcimento dei danni cagionati da essa o dai suoi agenti nell'esercizio delle loro funzioni.

4. La Corte di giustizia dell'Unione europea è competente a conoscere delle controversie relative al risarcimento di tali danni.

5. La responsabilità personale degli agenti nei confronti dell'Agenzia è disciplinata dalle disposizioni pertinenti che si applicano al personale dell'Agenzia.

Articolo 37

Regime linguistico

1. All'Agenzia si applicano le disposizioni previste dal regolamento n. 1 del Consiglio[19]. Gli Stati membri e gli altri organismi da essi designati possono rivolgersi all'Agenzia e ottenere la risposta in una delle lingue ufficiali delle istituzioni dell'Unione di loro scelta.

2. I servizi di traduzione necessari per il funzionamento dell'Agenzia sono forniti dal Centro di traduzione degli organismi dell'Unione europea.

Articolo 38

Protezione dei dati personali

1. Il trattamento dei dati personali da parte dell'Agenzia è soggetto al regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio[20].

2. Il consiglio di amministrazione adotta le misure di attuazione di cui all'articolo 24, paragrafo 8, del regolamento (CE) n. 45/2001. Il consiglio di amministrazione può adottare misure aggiuntive necessarie per l'applicazione del regolamento (CE) n. 45/2001 da parte dell'Agenzia.

---

19 Regolamento n. 1 che stabilisce il regime linguistico della Comunità economica europea (GU 17 del 6.10.1958, pag. 401).

20 Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

Articolo 39

Cooperazione con paesi terzi e organizzazioni internazionali

1. Se necessario ai fini del conseguimento degli obiettivi stabiliti nel presente regolamento, l'Agenzia può cooperare con le autorità competenti di paesi terzi, con le organizzazioni internazionali o con entrambi. A tal fine l'Agenzia può, previa approvazione da parte della Commissione, istituire accordi di lavoro con le autorità dei paesi terzi e con le organizzazioni internazionali. Detti accordi non creano obblighi giuridici per l'Unione e gli Stati membri.

2. L'Agenzia è aperta alla partecipazione di paesi terzi che hanno concluso con l'Unione accordi in tal senso. Nell'ambito delle pertinenti disposizioni di tali accordi, sono elaborate disposizioni che specificano, in particolare, la natura, la portata e le modalità di partecipazione di detti paesi ai lavori dell'Agenzia, comprese le disposizioni sulla partecipazione alle iniziative intraprese dall'Agenzia, sui contributi finanziari e sul personale. In materia di personale, tali disposizioni rispettano in ogni caso lo statuto dei funzionari.

3. Il consiglio di amministrazione adotta una strategia per le relazioni con paesi terzi o organizzazioni internazionali riguardo a questioni che rientrano tra le competenze dell'Agenzia. La Commissione garantisce che l'Agenzia operi nell'ambito del proprio mandato e del quadro istituzionale vigente stipulando un accordo di lavoro adeguato con il direttore esecutivo dell'Agenzia.

Articolo 40

Norme di sicurezza per la protezione delle informazioni classificate e delle informazioni sensibili non classificate

In consultazione con la Commissione, l'Agenzia adotta le proprie norme di sicurezza applicando i principi di sicurezza contenuti nelle norme di sicurezza della Commissione per la protezione delle informazioni classificate UE (ICUE) e delle informazioni sensibili non classificate di cui alle decisioni (UE, Euratom) 2015/443 e 2015/444 della Commissione. Esse riguardano, tra l'altro, le disposizioni che disciplinano lo scambio, il trattamento e la conservazione di tali informazioni.

Articolo 41

Accordo sulla sede e condizioni operative

1. Le necessarie disposizioni relative all'insediamento dell'Agenzia nello Stato membro ospitante e alle strutture che quest'ultimo deve mettere a disposizione nonché le norme specifiche applicabili in tale Stato membro al direttore esecutivo, ai membri del consiglio di amministrazione, al personale dell'Agenzia e ai membri delle rispettive famiglie sono fissate in un accordo di sede concluso, previa approvazione del consiglio di amministrazione ed entro [due anni dall'entrata in vigore del presente regolamento].

2. Lo Stato membro che ospita l'Agenzia fornisce le [...] condizioni [...] volte a garantire il corretto funzionamento dell'Agenzia, compresi l'accessibilità della sede, l'esistenza di strutture scolastiche adeguate per i figli del personale, un accesso adeguato al mercato del lavoro, alla sicurezza sociale e alle cure mediche per i figli e i coniugi.

Articolo 42

Controllo amministrativo

L'operato dell'Agenzia è sottoposto al controllo del Mediatore in conformità dell'articolo 228 TFUE.

TITOLO III
QUADRO DI CERTIFICAZIONE DELLA CIBERSICUREZZA

Articolo 43

Quadro [...] ***europeo di certificazione della cibersicurezza***

1. **Il quadro europeo di certificazione della cibersicurezza, istituito al fine di migliorare le condizioni di funzionamento del mercato interno aumentando il livello di cibersicurezza all'interno dell'Unione, instaura una governance che rende possibile, a livello di UE, un approccio armonizzato dei sistemi europei di certificazione della cibersicurezza, allo scopo di creare un mercato unico digitale per i processi, i prodotti e i servizi TIC.**

2. **Il quadro europeo di certificazione della cibersicurezza definisce il meccanismo volto a istituire** [...] i sistemi europei di certificazione della cibersicurezza **e ad** attesta**re** che i **processi,** prodotti e servizi TIC [...] **valutati** nel loro ambito sono 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, processi **e** servizi [...] o accessibili tramite essi **per tutto il loro ciclo di vita**.

Articolo 44

Preparazione e adozione di un sistema europeo di certificazione della cibersicurezza

1. A seguito di una richiesta della Commissione **o del gruppo europeo per la certificazione della cibersicurezza (di seguito il "gruppo") istituito a norma dell'articolo 53**, l'ENISA prepara una proposta di sistema europeo di certificazione della cibersicurezza che soddisfi i requisiti di cui agli articoli 45, 46 e 47 del presente regolamento.

1 bis. La preparazione di una proposta di sistema europeo di certificazione della cibersicurezza può essere sottoposta al gruppo dagli Stati membri o dalle organizzazioni dei portatori di interesse. Il gruppo valuta tali proposte rispetto a criteri da esso definiti mediante orientamenti, in conformità dell'articolo 53, paragrafo 3, lettera c bis), e può chiedere all'ENISA di preparare una proposta di sistema europeo di certificazione della cibersicurezza.

2. Nella preparazione delle proposte di sistemi di cui al paragrafo 1, l'ENISA consulta tutti i pertinenti portatori di interessi **mediante procedure di consultazione trasparenti** e coopera strettamente con il gruppo. Il gruppo fornisce all'ENISA assistenza e consulenza specialistica [...]in relazione alla preparazione della proposta di sistema **e adotta un parere su tale proposta prima che sia presentata alla Commissione** [...]. **L'ENISA assicura la coerenza delle proposte di sistema rispetto alle norme armonizzate applicabili utilizzate per l'accreditamento dell'organismo di valutazione della conformità.**

3. L'ENISA **tiene nella massima considerazione il parere del gruppo prima di trasmettere** [...] alla Commissione il sistema [...] preparato in conformità del paragrafo 2.

4. La Commissione, sulla base del sistema proposto dall'ENISA, può adottare atti di esecuzione in conformità dell'articolo 55, paragrafo 2, prevedendo sistemi europei di certificazione della cibersicurezza per **i processi,** i prodotti e i servizi TIC che soddisfano i requisiti di cui agli articoli 45, 46 e 47 del presente regolamento.

5. [...]

Articolo 44 bis

Mantenimento di un sistema europeo di certificazione della cibersicurezza

1. L'Agenzia gestisce un apposito sito web che fornisce informazioni sui sistemi europei di certificazione della cibersicurezza, sui certificati e sulle dichiarazioni UE di conformità rilasciate a norma dell'articolo 47 bis, e li pubblicizza.

2. Almeno ogni cinque anni l'Agenzia riesamina, in stretta cooperazione con il gruppo, i sistemi europei di certificazione della cibersicurezza adottati, tenendo conto del riscontro ricevuto dalle parti interessate. Se ritenuto necessario, la Commissione o il gruppo possono chiedere all'Agenzia di avviare il processo di sviluppo di una proposta riveduta di sistema in conformità dell'articolo 44, paragrafi 2 e 3.

Articolo 45

Obiettivi di sicurezza dei sistemi europei di certificazione della cibersicurezza

I sistemi europei di certificazione della cibersicurezza sono progettati in modo tale da [...] **conseguire**, se del caso, **almeno** i seguenti obiettivi di sicurezza:

a) proteggere i dati conservati, trasmessi o altrimenti trattati dall'archiviazione, dal trattamento, dall'accesso o dalla divulgazione accidentali o non autorizzati **durante l'intero ciclo di vita del processo, prodotto o servizio**;

b) proteggere i dati conservati, trasmessi o altrimenti trattati dalla distribuzione accidentale o non autorizzata, dalla perdita [...] o dall'alterazione**, oppure dalla mancanza di disponibilità durante l'intero ciclo di vita del processo, prodotto o servizio**;

c) [...] le persone, i programmi o le macchine autorizzati possono accedere esclusivamente ai dati, ai servizi o alle funzioni per i quali dispongono dei diritti di accesso;

d) registrare **a** quali dati, funzioni o servizi [...] **è stato effettuato l'accesso e quali sono stati utilizzati o altrimenti trattati**, in quale momento e da chi;

e) [...] è possibile verificare quali sono i dati, i servizi o le funzioni a cui è stato effettuato l'accesso**,** [...] che sono stati utilizzati **o altrimenti trattati**, in quale momento e da chi;

f) ripristinare la disponibilità e l'accesso ai dati, ai servizi e alle funzioni in modo tempestivo in caso di incidente fisico o tecnico;

g) [...] il software **e l'hardware dei processi,** dei prodotti e dei servizi TIC **sono** aggiornat**i** e non contengono vulnerabilità **pubblicamente** note e [...] tali **processi,** prodotti e servizi dispongono di meccanismi per effettuare aggiornamenti [...] protetti**;**

g bis) i processi, i prodotti e i servizi TIC sono sviluppati, fabbricati e forniti in conformità dei requisiti di sicurezza enunciati nel sistema in questione.

Articolo 46

Livelli di affidabilità dei sistemi europei di certificazione della cibersicurezza

1. I sistemi europei di certificazione della cibersicurezza possono specificare per **i processi,** i prodotti e i servizi TIC [...] uno o più dei seguenti livelli di affidabilità: di base, sostanziale e/o elevato. **Il livello di affidabilità è commisurato al livello di rischio associato al previsto uso di un processo, prodotto o servizio TIC.**

2. I livelli di affidabilità di base, sostanziale e elevato [...] **si riferiscono a un certificato o a una dichiarazione UE di conformità rilasciati nell'ambito di un sistema europeo di certificazione della cibersicurezza che prevede, per ciascun livello di affidabilità, i relativi requisiti di sicurezza, comprese le funzionalità di sicurezza, e il corrispondente livello di azioni compiute per la valutazione di un processo, prodotto o servizio TIC. Il certificato o la dichiarazione UE di conformità sono caratterizzati in riferimento a specifiche, norme e procedure tecniche ad esso connesse, tra cui i controlli tecnici, il cui obiettivo è ridurre il rischio di incidenti di cibersicurezza, o prevenirli, come segue:**

a) **un certificato europeo della cibersicurezza o una dichiarazione UE di conformità che si riferisce al** livello di affidabilità **"**di base**" assicura che i processi, prodotti e servizi TIC rispettino i relativi requisiti di sicurezza, comprese le funzionalità di sicurezza, e che siano stati valutati a un livello che mira a ridurre al minimo i rischi di base noti di incidenti e attacchi informatici. Le attività di valutazione comprendono almeno un riesame della documentazione tecnica; qualora ciò non sia possibile, includono attività sostitutive di effetto equivalente** [...];

b) **un certificato europeo della cibersicurezza che si riferisce al** livello di affidabilità **"**sostanziale**" assicura che i processi, prodotti e servizi TIC rispettino i relativi requisiti di sicurezza, comprese le funzionalità di sicurezza, e che siano stati valutati a un livello che mira a ridurre al minimo i rischi, gli incidenti e gli attacchi informatici noti causati da attori che dispongono di competenze e risorse limitate. Le attività di valutazione comprendono almeno un riesame della non applicabilità delle vulnerabilità pubblicamente note e un test che confermi che i processi, prodotti o servizi TIC attuano correttamente le necessarie funzionalità di sicurezza; qualora ciò non sia possibile, includono attività sostitutive di effetto equivalente** [...];

c) **un certificato europeo della cibersicurezza che si riferisce al** livello di affidabilità "elevato**" assicura che i processi, prodotti e servizi TIC rispettino i relativi requisiti di sicurezza, comprese le funzionalità di sicurezza, e che siano stati valutati a un livello che mira a ridurre al minimo il rischio di attacchi informatici avanzati commessi da attori che dispongono di competenze e risorse significative. Le attività di valutazione comprendono almeno un riesame della non applicabilità delle vulnerabilità pubblicamente note, un test che confermi che i processi, prodotti o servizi TIC attuano correttamente le necessarie funzionalità di sicurezza, allo stato più avanzato della tecnica, e una valutazione della loro resistenza agli attacchi commessi da autori qualificati mediante test di penetrazione; qualora ciò non sia possibile, includono attività sostitutive di effetto equivalente** [...].

2 bis. I sistemi europei di certificazione della cibersicurezza possono precisare vari livelli di valutazione in funzione del rigore e della specificità della metodologia di valutazione. Ciascun livello di valutazione corrisponde a uno dei livelli di affidabilità ed è definito da un'idonea combinazione di componenti dell'affidabilità.

Articolo 47

Elementi dei sistemi europei di certificazione della cibersicurezza

1. Un sistema europeo di certificazione della cibersicurezza comprende **almeno** i seguenti elementi:

a) l'oggetto e l'ambito di applicazione del **sistema di** certificazione, compresi il tipo o le categorie di **processi,** prodotti e servizi TIC coperti**, nonché una spiegazione che illustri in che modo il sistema di certificazione risponde alle esigenze dei gruppi interessati previsti**;

b) [...] **un** riferimento a**lle** norme [...] internazionali**, europee o nazionali applicate nella valutazione. Laddove non vi siano norme disponibili, si fa riferimento alle** [...] specifiche tecniche **che rispettano le prescrizioni di cui all'allegato II del regolamento n. 1025/2012 oppure, se non disponibili, alle specifiche tecniche o ad altri requisiti di cibersicurezza definiti nel sistema**;

c) se del caso, uno o più livelli di affidabilità;

c bis) se del caso, requisiti specifici o supplementari applicabili agli organismi di valutazione della conformità al fine di garantire che abbiano la competenza tecnica per valutare i requisiti di cibersicurezza;

d) i criteri e i metodi di valutazione specifici utilizzati, compresi i tipi di valutazione, al fine di dimostrare che gli obiettivi specifici di cui all'articolo 45 sono stati conseguiti;

e) **se del caso,** le informazioni necessarie per la certificazione che un richiedente deve fornire agli organismi di valutazione della conformità **o che deve altrimenti mettere a loro disposizione**;

f) le condizioni alle quali possono essere utilizzati gli eventuali marchi o etichette previsti dal sistema;

g) [...] le norme per il controllo della conformità dei certificati **o delle dichiarazioni UE di conformità** ai requisiti, compresi i meccanismi per dimostrare il mantenimento della conformità ai requisiti di cibersicurezza specificati;

h) **se del caso,** le condizioni per il rilascio **e il rinnovo di un certificato**, **nonché** il mantenimento, la prosecuzione e l'estensione della certificazione **o** la riduzione del suo campo di applicazione;

i) le regole riguardanti le conseguenze della non conformità dei prodotti e servizi TIC certificati **o autovalutati** ai requisiti [...] **del sistema**;

j) le regole riguardanti il modo in cui segnalare e trattare le vulnerabilità della cibersicurezza nei **processi,** prodotti e servizi TIC precedentemente non rilevate;

k) **se del caso,** le regole riguardanti la conservazione delle registrazioni da parte degli organismi di valutazione della conformità;

l) l'individuazione dei sistemi nazionali **o internazionali** di certificazione della cibersicurezza relativi allo stesso tipo o alle stesse categorie di **processi,** prodotti e servizi TIC**, requisiti di sicurezza e criteri e metodi di valutazione**;

m) il contenuto del certificato rilasciato **o la dichiarazione UE di conformità;**

m bis) il periodo di conservazione della dichiarazione UE di conformità e la documentazione tecnica di tutte le informazioni pertinenti da parte del fabbricante o fornitore di prodotti e servizi TIC;

m ter[...]) il periodo massimo di validità dei certificati;

m quater[...]) la politica di divulgazione dei certificati concessi, modificati e revocati;

m quinquies[...]) le condizioni per il riconoscimento reciproco dei sistemi di certificazione con i paesi terzi;

m sexies[...]) se del caso, le regole riguardanti un meccanismo di valutazione inter pares per gli organismi che rilasciano certificati europei di cibersicurezza per il livell[...]o di affidabilità elevato a norma dell'articolo 48, paragrafo 4 bis.

2. I requisiti specificati del sistema non sono in contrasto con gli obblighi di legge applicabili, in particolare quelli derivanti dalla normativa armonizzata dell'Unione.

3. Se un atto specifico dell'Unione lo prevede, la certificazione **o la dichiarazione UE di conformità** nell'ambito di un sistema europeo di certificazione della cibersicurezza può essere utilizzata per dimostrare la presunzione di conformità agli obblighi imposti da tale atto.

4. In assenza di una normativa armonizzata dell'Unione, anche la legislazione degli Stati membri può disporre che un sistema europeo di certificazione della cibersicurezza può essere utilizzato per stabilire la presunzione di conformità agli obblighi di legge.

Articolo 47 bis

Autovalutazione della conformità

1. Un sistema europeo di certificazione della cibersicurezza può consentire lo svolgimento di una valutazione della conformità sotto la sola responsabilità del fabbricante o del fornitore di prodotti e servizi TIC. Tale valutazione della conformità è applicabile unicamente ai prodotti e servizi TIC a basso rischio corrispondenti al livello di affidabilità di base.

2. Il fabbricante o fornitore di prodotti e servizi TIC può rilasciare una dichiarazione UE di conformità in cui afferma che è stato dimostrato il rispetto dei requisiti previsti nel sistema. Redigendo tale dichiarazione, il fabbricante o fornitore di prodotti e servizi TIC si assume la responsabilità della conformità del prodotto o servizio TIC ai requisiti previsti nel sistema.

3. Il fabbricante o fornitore di prodotti e servizi TIC tiene a disposizione dell'autorità nazionale di certificazione della cibersicurezza di cui all'articolo 50, paragrafo 1, per un periodo definito nel corrispondente sistema europeo di certificazione della cibersicurezza, la dichiarazione UE di conformità e la documentazione tecnica di tutte le informazioni pertinenti relative alla conformità dei prodotti e servizi TIC a un sistema. Una copia della dichiarazione UE di conformità è trasmessa all'autorità nazionale di certificazione della cibersicurezza e all'ENISA.

4. Il rilascio di una dichiarazione UE di conformità è volontario, salvo diversamente specificato nel diritto dell'Unione o degli Stati membri.

5. Le dichiarazioni UE di conformità rilasciate a norma del presente articolo sono riconosciute in tutti gli Stati membri.

Articolo 48

Certificazione della cibersicurezza

1. I **processi, i** prodotti e i servizi TIC certificati ricorrendo a un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 44 sono considerati conformi ai requisiti di tale sistema.

2. La certificazione è volontaria, salvo diversamente specificato nel diritto dell'Unione **o degli Stati membri**.

3. Un certificato europeo della cibersicurezza ai sensi del presente articolo **che fa riferimento a un livello di affidabilità di base o sostanziale** è rilasciato dagli organismi di valutazione della conformità di cui all'articolo 51 sulla base dei criteri previsti dal sistema europeo di certificazione della cibersicurezza, adottato a norma dell'articolo 44.

4. In deroga al paragrafo 3, in casi debitamente giustificati un determinato sistema europeo **di certificazione** della cibersicurezza può prevedere che un certificato europeo della cibersicurezza derivante da tale sistema possa essere rilasciato da un ente pubblico. Detto ente [...] è uno dei seguenti:

a) un'autorità nazionale di [...] certificazione **della cibersicurezza** ai sensi dell'articolo 50, paragrafo 1;

b) un organismo **pubblico** accreditato come organismo di valutazione della conformità a norma dell'articolo 51, paragrafo 1[...]

c) [...].

4 bis. Nei casi in cui un sistema europeo di certificazione della cibersicurezza a norma dell'articolo 44 richieda un livello di affidabilità elevato, il certificato può essere rilasciato solo da un'autorità nazionale di certificazione della cibersicurezza di cui all'articolo 50, paragrafo 1, oppure, alle seguenti condizioni, da un organismo di valutazione della conformità di cui all'articolo 51:

a) previa approvazione dell'autorità nazionale di certificazione della cibersicurezza per ogni singolo certificato rilasciato da un organismo di valutazione della conformità; o

b) previa delega generale di tale compito a un organismo di valutazione della conformità da parte dell'autorità nazionale di certificazione della cibersicurezza.

5. La persona fisica o giuridica che presenta i suoi **processi,** prodotti o servizi TIC al meccanismo di certificazione [...] **mette a disposizione de**ll'organismo di valutazione della conformità di cui all'articolo 51 **o dell'autorità nazionale di certificazione della cibersicurezza di cui all'articolo 50, qualora tale autorità sia l'organismo che rilascia il certificato,** tutte le informazioni necessarie a espletare la procedura di certificazione.

5 bis. Il titolare di un certificato informa l'organismo che rilascia il certificato delle eventuali vulnerabilità o irregolarità successivamente rilevate in relazione alla sicurezza dei processi, prodotti o servizi TIC certificati che possono incidere sui requisiti relativi alla certificazione. L'organismo trasmette tali informazioni senza indebiti ritardi all'autorità nazionale di certificazione della cibersicurezza.

6. I certificati sono rilasciati per [...] **il periodo definito dallo specifico sistema di certificazione** e possono essere rinnovati [...] purché continuino a essere soddisfatti i requisiti pertinenti.

7. I certificati europei della cibersicurezza rilasciati a norma del presente articolo sono riconosciuti in tutti gli Stati membri.

Articolo 49

Sistemi nazionali di certificazione della cibersicurezza e certificati nazionali della cibersicurezza

1. Fatto salvo il paragrafo 3, i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per **i processi,** i prodotti e i servizi TIC 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 44, paragrafo 4. I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i **processi,** prodotti e servizi TIC non coperti da un sistema europeo di certificazione della cibersicurezza continuano ad esistere.

2. Gli Stati membri non introducono nuovi sistemi nazionali di certificazione della cibersicurezza per i **processi,** prodotti e servizi TIC coperti da un sistema europeo di certificazione della cibersicurezza in vigore.

3. I certificati esistenti rilasciati nell'ambito di sistemi nazionali di certificazione della cibersicurezza **e coperti da un sistema europeo di certificazione della cibersicurezza** restano validi fino alla loro data di scadenza.

Articolo 50

***Autorità nazionali di [...] certificazione* della cibersicurezza**

1. Ciascuno Stato membro [...] **designa una o più** autorità **nazionali** di [...] certificazione **della cibersicurezza nel suo territorio oppure, di comune accordo con un altro Stato membro, designa una o più autorità stabilite in tale altro Stato membro affinché siano responsabili dei compiti di vigilanza nello Stato membro designante**.

2. Ciascuno Stato membro comunica alla Commissione l'identità delle autorità [...] **designate e i compiti loro assegnati**.

3. **Fatti salvi l'articolo 48, paragrafo 4, lettera a), e l'articolo 48, paragrafo 4 bis,** [...]**c**iascuna autorità nazionale di [...] certificazione **della cibersicurezza**, per quanto riguarda la sua organizzazione, le decisioni di finanziamento, la struttura giuridica e il processo decisionale, è indipendente dai soggetti sui quali vigila.

3 bis. Gli Stati membri assicurano che le attività delle autorità nazionali di certificazione della cibersicurezza relative al rilascio di certificati in conformità dell'articolo 48, paragrafo 4, lettera a), e dell'articolo 48, paragrafo 4 bis, si attengano a una rigorosa separazione dei ruoli e delle responsabilità con le attività di vigilanza di cui al presente articolo e operino in modo indipendente le une dalle altre.

4. Gli Stati membri provvedono affinché le autorità nazionali di [...] certificazione **della cibersicurezza** dispongano di risorse adeguate per l'esercizio dei loro poteri e l'esecuzione efficiente ed efficace dei compiti loro assegnati.

5. Ai fini dell'effettiva attuazione del regolamento, è opportuno che dette autorità partecipino in modo attivo, efficace, efficiente e sicuro al gruppo europeo per la certificazione della cibersicurezza istituito a norma dell'articolo 53.

6. Le autorità nazionali di [...] certificazione **della cibersicurezza**:

a) [...]

a bis) monitorano e fanno applicare gli obblighi fissati nell'articolo 47 bis, paragrafi 2 e 3, e nel corrispondente sistema europeo di certificazione della cibersicurezza, che incombono al fabbricante o al fornitore di prodotti e servizi TIC stabiliti nei rispettivi territori;

b) [...] **fatto salvo l'articolo 51, paragrafo 1 ter, assistono gli organismi nazionali di accreditamento nel monitoraggio e nella vigilanza del**le attività degli organismi di valutazione della conformità ai fini del presente regolamento [...];

b bis) monitorano e supervisionano le attività degli enti di cui all'articolo 48, paragrafo 4;

b ter) autorizzano gli organismi di valutazione della conformità di cui all'articolo 51, paragrafo 1 ter, e limitano, sospendono o revocano l'autorizzazione esistente nei casi di inosservanza dei requisiti di cui al presente regolamento;

c) trattano i reclami presentati dalle persone fisiche o giuridiche in relazione ai certificati rilasciati [...] **dall'autorità nazionale di certificazione della cibersicurezza o, in conformità dell'articolo 48, paragrafo 4 bis, dagli organismi di valutazione della conformità**, svolgono le indagini opportune sull'oggetto del reclamo e informano il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole;

d) cooperano con le altre autorità nazionali di [...] certificazione **della cibersicurezza** o con altre autorità pubbliche, anche mediante lo scambio di informazioni sugli eventuali **processi,** prodotti e servizi TIC non conformi ai requisiti del presente regolamento o di specifici sistemi europei di certificazione della cibersicurezza;

e) sorvegliano gli sviluppi che presentano un interesse nel campo della certificazione della cibersicurezza.

7. Ciascuna autorità nazionale di [...] certificazione **della cibersicurezza** dispone almeno dei seguenti poteri:

a) richiedere agli organismi di valutazione della conformità**,** [...] ai titolari di certificati europei della cibersicurezza **e agli emittenti di dichiarazioni UE di conformità** di fornire le eventuali informazioni necessarie all'esecuzione dei suoi compiti;

b) condurre indagini, sotto forma di verifiche contabili, nei confronti degli organismi di valutazione della conformità, [...] dei titolari dei certificati europei della cibersicurezza **e degli emittenti di dichiarazioni UE di conformità** allo scopo di verificare l'osservanza delle disposizioni di cui al titolo III;

c) adottare misure appropriate, nel rispetto della legislazione nazionale, al fine di accertare che gli organismi di valutazione della conformità**,** [...] i titolari di certificati **e gli emittenti di dichiarazioni UE di conformità** si conformino al presente regolamento o a un sistema europeo di certificazione della cibersicurezza;

d) ottenere accesso a tutti i locali degli organismi di valutazione della conformità e dei titolari dei certificati europei della cibersicurezza al fine di espletare le indagini in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri;

e) revocare, in conformità del diritto nazionale, i certificati **rilasciati dalle autorità nazionali di certificazione della cibersicurezza o, conformemente all'articolo 48, paragrafo 4 bis, dagli organismi di valutazione della conformità** non conformi al presente regolamento o a un sistema europeo di certificazione della cibersicurezza;

f) irrogare sanzioni a norma dell'articolo 54, conformemente al diritto nazionale, e chiedere la cessazione immediata delle violazioni degli obblighi di cui al presente regolamento.

8. Le autorità nazionali di [...] certificazione **della cibersicurezza** cooperano tra di loro e con la Commissione e, in particolare, si scambiano informazioni, esperienze e buone pratiche per quanto concerne la certificazione della cibersicurezza e le questioni tecniche riguardanti la cibersicurezza di **processi,** prodotti e servizi TIC.

Articolo 51

Organismi di valutazione della conformità

1. Gli organismi di valutazione della conformità sono accreditati dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008 solo se soddisfano i requisiti indicati nell'allegato del presente regolamento.

1 bis. Nei casi in cui il certificato europeo della cibersicurezza è rilasciato da un'autorità nazionale di certificazione della cibersicurezza a norma dell'articolo 48, paragrafo 4, lettera a), e dell'articolo 48, paragrafo 4 bis, l'organismo di certificazione dell'autorità nazionale di certificazione della cibersicurezza è accreditato come organismo di valutazione della conformità a norma del paragrafo 1.

1 ter. Se del caso, l'autorità nazionale di certificazione della cibersicurezza autorizza gli organismi di valutazione della conformità a svolgere i suoi compiti quando soddisfano i requisiti specifici o supplementari previsti nel sistema europeo di certificazione ai sensi dell'articolo 47, paragrafo 1, lettera c bis).

2. L'accreditamento è rilasciato per un periodo massimo di cinque anni e può essere rinnovato alle stesse condizioni purché l'organismo di valutazione della conformità soddisfi i requisiti di cui al presente articolo. **Entro un termine ragionevole, g**li organismi di accreditamento **adottano tutte le misure necessarie per limitare, sospendere o** revoca**re** l'accreditamento di un organismo di valutazione della conformità di cui al paragrafo 1 se le condizioni per l'accreditamento non sono, o non sono più, soddisfatte o se le azioni intraprese da un organismo di valutazione della conformità sono contrarie alle disposizioni del presente regolamento.

Articolo 52

Notifica

1. Per ciascun sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 44, le autorità nazionali di [...] certificazione **della cibersicurezza** notificano alla Commissione gli organismi di valutazione della conformità accreditati **e, se del caso, autorizzati a norma dell'articolo 51, paragrafo 1 ter,** a rilasciare i certificati a determinati livelli di affidabilità di cui all'articolo 46 e, senza indebiti ritardi, ogni successiva modifica degli stessi.

2. Un anno dopo l'entrata in vigore di un sistema europeo di certificazione della cibersicurezza, la Commissione pubblica nella Gazzetta ufficiale un elenco degli organismi di valutazione della conformità notificati.

3. Se la Commissione riceve una notifica dopo lo scadere del periodo di cui al paragrafo **2**[...], pubblica nella Gazzetta ufficiale dell'Unione europea le modifiche dell'elenco di cui al paragrafo 2 entro due mesi dalla data di ricevimento di tale notifica.

4. Un'autorità nazionale di [...] certificazione **della cibersicurezza** può presentare alla Commissione una richiesta di rimozione di un organismo di valutazione della conformità notificato dall'autorità stessa dall'elenco di cui al paragrafo 2. La Commissione pubblica nella Gazzetta ufficiale dell'Unione europea le corrispondenti modifiche dell'elenco entro un mese dalla data di ricevimento della richiesta dell'autorità nazionale di [...] certificazione **della cibersicurezza**.

5. La Commissione può, mediante atti di esecuzione, definire le circostanze, i formati e le procedure delle notifiche di cui al paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 55, paragrafo 2.

Articolo 53

Gruppo europeo per la certificazione della cibersicurezza

1. È istituito il gruppo europeo per la certificazione della cibersicurezza (di seguito il "gruppo").

2. Il gruppo è composto da**i rappresentanti de**lle autorità nazionali di [...] certificazione **della cibersicurezza o dai rappresentanti di altre autorità nazionali competenti**. [...] **Ogni membro del gruppo può rappresentare non più di un altro Stato membro**.

3. Il gruppo ha i seguenti compiti:

a) consigliare e coadiuvare la Commissione nelle sue attività volte a garantire un'attuazione e un'applicazione coerenti delle disposizioni del presente titolo, in particolare per quanto riguarda le questioni relative alla politica in materia di certificazione della cibersicurezza, al coordinamento degli approcci politici e alla preparazione dei sistemi europei di certificazione della cibersicurezza;

b) assistere, consigliare e collaborare con l'ENISA in relazione alla preparazione di una proposta di sistema conformemente all'articolo 44 del presente regolamento;

b bis) adottare un parere sulla proposta di sistema ai sensi dell'articolo 44 del presente regolamento;

c) [...] chiedere all'Agenzia di preparare una proposta di sistema europeo di certificazione della cibersicurezza conformemente all'articolo 44 del presente regolamento;

c bis) sviluppare e adottare orientamenti sui criteri di valutazione delle proposte finalizzate alla preparazione di una proposta di sistema presentate [...] al gruppo a norma dell'articolo 44, paragrafo 1 bis;

d) adottare pareri indirizzati alla Commissione relativi al mantenimento e alla revisione degli attuali sistemi europei di certificazione della cibersicurezza.

e) esaminare gli sviluppi che presentano un interesse in materia di certificazione della cibersicurezza e scambio di buone pratiche sui sistemi di certificazione della cibersicurezza;

f) agevolare la cooperazione tra le autorità nazionali di [...] certificazione **della cibersicurezza** di cui al presente titolo attraverso **lo sviluppo della capacità,** lo scambio di informazioni, in particolare mediante la definizione di metodi per un efficiente scambio di informazioni in relazione a tutti gli aspetti riguardanti la certificazione della cibersicurezza**;**

f bis) sostenere l'attuazione del meccanismo di valutazione inter pares in conformità delle norme fissate da un sistema europeo di certificazione della cibersicurezza ai sensi dell'articolo 47, paragrafo 1, lettera m quinquies), del presente regolamento.

4. La Commissione presiede **in veste di moderatore** il gruppo, per il quale svolge le funzioni di segretariato, con l'assistenza dell'ENISA conformemente all'articolo 8, lettera a).

Articolo 53 bis

***Diritto di presentare un reclamo all'autorità nazionale di [...] certificazione* della cibersicurezza**

1. Le persone fisiche o giuridiche hanno il diritto di presentare un reclamo all'autorità nazionale di certificazione della cibersicurezza in relazione a un certificato rilasciato dalla stessa autorità o, conformemente all'articolo 48, paragrafo 4 bis, da organismi di valutazione della conformità.

2. L'autorità nazionale di certificazione della cibersicurezza a cui è stato presentato il reclamo informa il reclamante dello stato e dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 53 ter.

Articolo 53 ter

Diritto a un ricorso giurisdizionale effettivo

1. Le persone fisiche o giuridiche hanno diritto a un ricorso giurisdizionale effettivo nei confronti di una decisione giuridicamente vincolante adottata da un'autorità nazionale di certificazione della cibersicurezza al loro riguardo.

2. Le persone fisiche o giuridiche hanno diritto a un ricorso giurisdizionale effettivo qualora l'autorità nazionale di certificazione della cibersicurezza non tratti un reclamo.

3. I procedimenti nei confronti di un'autorità nazionale di certificazione della cibersicurezza sono presentati dinanzi ai tribunali dello Stato membro in cui è stabilita tale autorità.

Articolo 54

Sanzioni

Gli Stati membri stabiliscono le norme sulle sanzioni da irrogare in caso di violazione del presente titolo e dei sistemi europei di certificazione della cibersicurezza e prendono tutti i provvedimenti necessari per la loro applicazione. Le sanzioni previste sono efficaci, proporzionate e dissuasive. Gli Stati membri notificano [entro il …/senza indugio] tali norme e misure alla Commissione, nonché eventuali successive modifiche delle stesse.

TITOLO IV
DISPOSIZIONI FINALI

Articolo 55

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo **5, paragrafo 4, lettera b),** del regolamento (UE) n. 182/2011.

Articolo 56

Valutazione e riesame

1. Entro cinque anni dalla data di cui all'articolo 58, e successivamente ogni cinque anni, la Commissione valuta l'impatto, l'efficacia e l'efficienza dell'Agenzia e delle sue prassi di lavoro, come pure l'eventuale necessità di modificarne il mandato e le conseguenti implicazioni finanziarie. La valutazione tiene conto di qualsiasi riscontro pervenuto all'Agenzia in relazione alle sue attività. Se ritiene che il mantenimento dell'Agenzia non sia più giustificato rispetto agli obiettivi, al mandato e ai compiti che le sono stati assegnati, la Commissione può proporre di modificare il presente regolamento in relazione alle disposizioni che riguardano l'Agenzia.

2. La valutazione esamina inoltre l'impatto, l'efficacia e l'efficienza delle disposizioni del titolo III per quanto riguarda gli obiettivi di garantire un livello adeguato di cibersicurezza dei prodotti e servizi TIC nell'Unione e di migliorare il funzionamento del mercato interno.

3. La Commissione trasmette la relazione di valutazione unitamente alle sue conclusioni al Parlamento europeo, al Consiglio e al consiglio di amministrazione. I risultati della valutazione sono resi pubblici.

Articolo 57

Abrogazione e sostituzione

1. Il regolamento (CE) n. 526/2013 è abrogato con effetto a decorrere dal [….].

2. I riferimenti al regolamento (CE) n. 526/2013 e all'ENISA si intendono fatti al presente regolamento e all'Agenzia.

3. L'Agenzia sostituisce l'Agenzia istituita dal regolamento (CE) n. 526/2013 per quanto riguarda diritti di proprietà, accordi, obblighi di legge, contratti di lavoro, impegni finanziari e responsabilità. Tutte le decisioni già prese dal consiglio di amministrazione e dal comitato esecutivo restano valide, purché non siano in conflitto con le disposizioni del presente regolamento.

4. L'Agenzia è istituita per un periodo di tempo indeterminato a decorrere dal […].

5. Il direttore esecutivo nominato a norma dell'articolo 24, paragrafo 4, del regolamento (CE) n. 526/2013 è il direttore esecutivo dell'Agenzia per la restante durata del mandato.

6. I membri del consiglio di amministrazione e i loro supplenti nominati a norma dell'articolo 6 del regolamento (CE) n. 526/2013 sono i membri e i rispettivi supplenti del consiglio di amministrazione dell'Agenzia per la restante durata del mandato.

Articolo 58

Entrata in vigore

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea.

1 bis. Il presente regolamento si applica a decorrere dal […], fatta eccezione per gli articoli 50, 51, 52, 53 bis, 53 ter e 54 che si applicano da [24 mesi dopo la pubblicazione nella Gazzetta ufficiale dell'Unione europea].

2. Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*

ALLEGATO

REQUISITI CHE GLI ORGANISMI DI VALUTAZIONE DELLA CONFORMITÀ DEVONO SODDISFARE

Gli organismi di valutazione della conformità che desiderano essere accreditati devono soddisfare i seguenti requisiti:

1. L'organismo di valutazione della conformità è stabilito a norma del diritto interno e ha personalità giuridica.

2. L'organismo di valutazione della conformità è un organismo terzo, indipendente dall'organizzazione o dai prodotti o servizi TIC 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 o dei servizi TIC che esso 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. L'organismo di valutazione della conformità, i suoi alti dirigenti e il personale addetto 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 dei prodotti o servizi TIC sottoposti alla sua valutazione, né il rappresentante autorizzato di uno di questi soggetti. Non è per questo precluso l'uso dei prodotti valutati che sono necessari per il funzionamento dell'organismo di valutazione della conformità o il loro uso per scopi privati.

5. Un organismo di valutazione della conformità, i suoi alti dirigenti e il personale addetto alla valutazione della conformità non intervengono direttamente nella progettazione, fabbricazione o costruzione, nella commercializzazione, nell'installazione, nell'uso o nella manutenzione dei prodotti o servizi TIC, né rappresentano i soggetti impegnati in tali attività. Essi non devono intraprendere attività alcuna che possa essere in conflitto con la loro indipendenza di giudizio o integrità riguardo alle attività di valutazione della conformità per cui sono notificati. Ciò vale in particolare per i servizi di consulenza.

6. Gli organismi di valutazione della conformità garantiscono che le attività delle loro affiliate o dei loro subappaltatori non abbiano effetti negativi sulla riservatezza, sull'obiettività o sull'imparzialità delle loro attività di valutazione della conformità.

7. Gli organismi di valutazione della conformità e il loro personale eseguono le attività di valutazione della conformità con il massimo dell'integrità professionale e della competenza tecnica e sono liberi da qualsivoglia pressione e incentivo, anche di natura finanziaria, che possa influenzare il loro giudizio o i risultati delle loro attività di valutazione, in particolare da persone o gruppi di persone interessati ai risultati di tali attività.

8. Un organismo di valutazione della conformità è in grado di effettuare tutti i compiti di valutazione della conformità ad esso assegnati dal presente regolamento, indipendentemente dal fatto che tali compiti siano eseguiti dall'organismo stesso o per suo conto e sotto la sua responsabilità.

9. In ogni momento, per ogni procedura di valutazione della conformità e per ogni tipo, categoria o sottocategoria di prodotti e servizi TIC, l'organismo di valutazione della conformità dispone:

a) di personale avente conoscenze tecniche ed esperienza sufficiente e appropriata per eseguire i compiti di valutazione della conformità;

b) di descrizioni delle procedure in base alle quali si svolge la valutazione della conformità, garantendo la trasparenza di tali procedure e la possibilità di essere riprodotte. Predispone una politica e procedure appropriate che distinguano i compiti che svolge in qualità di organismo notificato dalle altre attività;

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 o del servizio TIC in questione e della natura di massa o seriale del processo produttivo.

10. L'organismo di valutazione della conformità dispone dei mezzi necessari per eseguire i compiti tecnici e amministrativi connessi alle attività di valutazione della conformità in modo appropriato e ha accesso a tutti gli strumenti e impianti occorrenti.

11. Il personale che effettua le attività di valutazione della conformità dispone di quanto segue:

a) una formazione tecnica e professionale solida che includa tutte le attività di valutazione della conformità;

b) soddisfacenti conoscenze delle prescrizioni relative alle valutazioni che esegue e un'adeguata autorità per eseguire tali valutazioni;

c) una conoscenza e una comprensione adeguate dei requisiti e delle norme tecniche di prova applicabili;

d) la capacità di elaborare certificati, registri e relazioni a dimostrazione del fatto che le valutazioni sono state effettuate.

12. È garantita l'imparzialità dell'organismo di valutazione della conformità, dei suoi alti dirigenti e del personale addetto alle valutazioni.

13. La remunerazione degli alti dirigenti e del personale addetto alle valutazioni di un organismo di valutazione della conformità non dipende dal numero di valutazioni eseguite o dai risultati di tali valutazioni.

14. Gli organismi di valutazione della conformità sottoscrivono un contratto di assicurazione per la responsabilità civile, a meno che detta responsabilità non sia direttamente coperta dallo Stato a norma del diritto nazionale o che lo Stato membro stesso non sia direttamente responsabile della valutazione della conformità.

15. Il personale di un organismo di valutazione della conformità è tenuto al segreto professionale per tutto ciò di cui viene a conoscenza nell'esercizio delle sue funzioni a norma del presente regolamento o di qualsiasi disposizione esecutiva di diritto interno, tranne nei confronti delle autorità competenti degli Stati membri in cui esercita le sue attività.

16. Gli organismi di valutazione della conformità sono conformi ai requisiti della norma **pertinente armonizzata conformemente al regolamento (CE) n. 765/2008 per quanto riguarda l'accreditamento degli organismi di valutazione della conformità che effettuano la certificazione dei processi, prodotti o servizi** [...].

17. 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 norma **pertinente armonizzata conformemente al regolamento (CE) n. 765/2008 per quanto riguarda l'accreditamento dei laboratori che effettuano prove** [...].