Gazzetta ufficiale dell'Unione europea

C 191

Edizione in lingua italiana

Comunicazioni e informazioni

64° anno

18 maggio 2021

Sommario

IT

III

(Atti preparatori)

CONSIGLIO

POSIZIONE (UE) N. 18/2021 DEL CONSIGLIO IN PRIMA LETTURA

in vista dell'adozione del regolamento del Parlamento europeo e del Consiglio che istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento

Adottata dal Consiglio il 20 aprile 2021

(2021/C 191/01)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 173, paragrafo 3, e l'articolo 188, primo comma,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

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

deliberando secondo la procedura legislativa ordinaria [2],

considerando quanto segue:

(1) La maggior parte della popolazione dell'Unione è collegata a Internet. La vita quotidiana delle persone e le economie dipendono sempre di più dalle tecnologie digitali. I cittadini e le imprese sono sempre più esposti a gravi incidenti di cibersicurezza e ogni anno molte imprese europee subiscono almeno un incidente di questo tipo. Ciò evidenzia la necessità di resilienza, di potenziamento delle capacità tecnologiche e industriali, e del ricorso a standard elevati e soluzioni olistiche in materia di cibersicurezza che coinvolgano le persone, i prodotti, i processi e le tecnologie dell'Unione, nonché di una leadership dell'Unione negli ambiti della cibersicurezza e dell'autonomia digitale. La cibersicurezza può essere migliorata anche attraverso la sensibilizzazione in merito alle minacce rivolte alla stessa e lo sviluppo di competenze, capacità e abilità in tutta l'Unione, tenendo pienamente conto delle implicazioni e preoccupazioni sociali ed etiche.

(2) L'Unione ha costantemente intensificato le sue attività per far fronte alle crescenti sfide in materia di cibersicurezza, in conformità della strategia per la cibersicurezza presentata dalla Commissione e dall'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza (alto rappresentante) nella comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni del 7 febbraio 2013 dal titolo «Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro» («strategia per la cibersicurezza del 2013»). La strategia per la cibersicurezza del 2013 era intesa a promuovere un ecosistema cibernetico affidabile, sicuro e aperto. Nel 2016 l'Unione ha adottato le prime misure nel settore della cibersicurezza attraverso la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio [3] sulla sicurezza delle reti e dei sistemi informativi.

[1] GU C 159 del 10.5.2019, pag. 63.

[2] Posizione del Parlamento europeo del 17 aprile 2019 (GU C 158 del 30.4.2021, pag. 850) e posizione del Consiglio in prima lettura del 20 aprile 2021. Posizione del Parlamento europeo del … (non ancora pubblicata nella Gazzetta ufficiale).

[3] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, concernente misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

(3) Nel settembre 2017 la Commissione e l'alto rappresentante hanno presentato una comunicazione congiunta al Parlamento europeo e al Consiglio dal titolo «Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE» al fine di rafforzare ulteriormente la resilienza, la deterrenza e la risposta dell'Unione agli attacchi informatici.

(4) In occasione del vertice di Tallinn sul digitale del settembre 2017, i capi di Stato e di governo hanno invitato l'Unione a diventare un leader mondiale della cibersicurezza entro il 2025, al fine di garantire la fiducia, la sicurezza e la tutela dei cittadini, dei consumatori e delle imprese online e di fare sì che Internet sia libero, più sicuro e regolamentato, e hanno dichiarato la loro intenzione di avvalersi maggiormente di soluzioni open source e di standard aperti in caso di (ri)costruzione di sistemi e soluzioni nell'ambito delle tecnologie dell'informazione e della comunicazione (TIC), in particolare per evitare di rimanere vincolati ai fornitori, compresi quelli sviluppati o promossi dai programmi dell'Unione per l'interoperabilità e la normazione, come ISA[2].

(5) Il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca sulla cibersicurezza («Centro di competenza») istituito dal presente regolamento dovrebbe contribuire ad aumentare la sicurezza delle reti e dei sistemi informativi, tra cui Internet e altre infrastrutture critiche per il funzionamento della società, come i trasporti, la sanità, l'energia, le infrastrutture digitali, l'acqua, il mercato finanziario e i sistemi bancari.

(6) Una grave perturbazione delle reti e dei sistemi informativi può ripercuotersi su singoli Stati membri e su tutta l'Unione. Un elevato livello di sicurezza delle reti e dei sistemi informativi in tutta l'Unione è quindi essenziale sia per la società che per l'economia. Al momento l'Unione dipende da fornitori di cibersicurezza non europei. Tuttavia, è nell'interesse strategico dell'Unione garantire il mantenimento e lo sviluppo di capacità di ricerca e tecnologiche essenziali in materia di cibersicurezza per tutelare le reti e i sistemi informativi dei cittadini e delle imprese, in particolare per proteggere reti e sistemi informativi critici, e per fornire servizi fondamentali di cibersicurezza.

(7) L'Unione vanta grandi competenze ed esperienza nello sviluppo industriale, nella tecnologia e nella ricerca sulla cibersicurezza, ma gli sforzi delle comunità dell'industria e della ricerca sono frammentati, disallineati e privi di una progettualità comune, il che frena la competitività e l'effettiva protezione delle reti e dei sistemi in tale ambito. Tali sforzi e competenze necessitano di essere aggregati, collegati in rete e impiegati in modo efficiente per consolidare e integrare le capacità in materia di ricerca, tecnologie e industria e le competenze esistenti a livello nazionale e di Unione. Nonostante il settore delle TIC si trovi ad affrontare sfide importanti, quali il soddisfacimento della domanda di lavoratori qualificati, esso può trarre beneficio dalla rappresentanza della diversità della società in generale e dal raggiungimento di una rappresentanza equilibrata dei generi, della diversità etnica e della non discriminazione nei confronti delle persone con disabilità, nonché dalla facilitazione dell'accesso alla conoscenza e alla formazione dei futuri esperti di cibersicurezza, compresa la loro istruzione in contesti non formali, ad esempio in progetti di software libero e aperto, progetti di tecnologia civica, start-up e microimprese.

(8) Le piccole e medie imprese (PMI) sono portatori di interessi fondamentali del settore della cibersicurezza dell'Unione e sono in grado di fornire soluzioni all'avanguardia grazie alla loro agilità. Tuttavia, le PMI che non sono specializzate nella cibersicurezza tendono anche a essere più vulnerabili agli incidenti di cibersicurezza, dati gli investimenti e le conoscenze di alto livello necessari per realizzare soluzioni efficaci in materia di cibersicurezza. È pertanto necessario che il Centro di competenza e la rete dei centri nazionali di coordinamento («rete») sostengano le PMI agevolando il loro accesso alle conoscenze e fornendo un accesso su misura ai risultati della ricerca e dello sviluppo, affinché esse possano proteggersi in misura sufficiente e in modo da consentire a coloro che le PMI che operano nel settore della cibersicurezza di essere competitive e di contribuire alla leadership dell'Unione nell'ambito della cibersicurezza.

(9) Esistono competenze al di fuori dei contesti dell'industria e della ricerca. I progetti non commerciali e precommerciali, denominati progetti di «tecnologia civica», utilizzano standard aperti, dati aperti e software liberi e aperti, nell'interesse della società e del bene pubblico.

(10) Quello della cibersicurezza è un settore diversificato. I portatori di interessi pertinenti possono includere portatori di interessi provenienti da enti pubblici, dagli Stati membri e dall'Unione, così come dall'industria, dalla società civile, per esempio dai sindacati, dalle associazioni dei consumatori, dalla comunità dei software liberi e aperti e dalla comunità accademica e della ricerca, e da altri soggetti.

(11) Nelle conclusioni adottate nel novembre 2017, il Consiglio ha invitato la Commissione a fornire rapidamente una valutazione d'impatto sulle possibili opzioni per creare una rete di centri di competenza sulla cibersicurezza e un centro europeo di ricerca e di competenza sulla cibersicurezza e a proporre entro la metà del 2018 lo strumento giuridico pertinente per la creazione di tale rete e tale centro.

(12) L'Unione non dispone ancora di sufficienti capacità e mezzi tecnologici e industriali per garantire autonomamente la sicurezza della propria economia e delle proprie infrastrutture critiche e per diventare un leader mondiale nel settore della cibersicurezza. Il livello di coordinamento e cooperazione strategici e sostenibili tra industrie, comunità di ricerca in materia di cibersicurezza e governi è insufficiente. L'Unione risente di investimenti frammentari e di un accesso limitato alle conoscenze, competenze e strutture in materia di cibersicurezza in Europa, e pochi sono i risultati europei della ricerca e dell'innovazione in materia di cibersicurezza che si traducono in soluzioni commercializzabili o di ampia diffusione in tutti i comparti economici.

(13) Istituire la rete e il Centro di competenza, con il mandato di perseguire l'attuazione di misure a supporto delle tecnologie industriali e nell'ambito della ricerca e dell'innovazione, è il miglior modo per conseguire gli obiettivi del presente regolamento e, al tempo stesso, offrire i migliori risultati in termini economici, sociali e ambientali e salvaguardare gli interessi dell'Unione.

(14) Il Centro di competenza dovrebbe costituire il principale strumento dell'Unione per concentrare gli investimenti nello sviluppo industriale, nella tecnologia e nella ricerca sulla cibersicurezza e per attuare progetti e iniziative pertinenti in collaborazione con la rete. Il Centro di competenza dovrebbe fornire il sostegno finanziario legato alla cibersicurezza e concesso dal programma Orizzonte Europa — il programma quadro di ricerca e innovazione («Orizzonte Europa») istituito dal regolamento (UE) 2021/… del Parlamento europeo e del Consiglio ([4]) ([+]) e dal programma Europa digitale istituito dal regolamento (UE) 2021/… del Parlamento europeo e del Consiglio ([5]) ([++]) e dovrebbe essere aperto ad altri programmi, ove opportuno. Questo approccio dovrebbe contribuire alla creazione di sinergie e al coordinamento del sostegno finanziario connesso alle iniziative dell'Unione nel settore dello sviluppo industriale, dell'innovazione, della tecnologia e della ricerca e dello sviluppo sulla cibersicurezza, e dovrebbe evitare inutili duplicazioni.

(15) È importante che nei progetti di ricerca in materia di cibersicurezza sostenuti dal Centro di competenza siano assicurati il rispetto dei diritti fondamentali e una condotta consapevole dal punto di vista etico.

(16) Il Centro di competenza non dovrebbe svolgere compiti operativi in materia di cibersicurezza, quali i compiti connessi ai gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), compresi il monitoraggio e la gestione degli incidenti di cibersicurezza. Tuttavia, il Centro di competenza dovrebbe poter agevolare lo sviluppo di infrastrutture TIC al servizio delle industrie, in particolare le PMI, delle comunità di ricerca, della società civile e del settore pubblico, coerentemente alla missione e agli obiettivi di cui al presente regolamento. Qualora i CSIRT e altri portatori di interessi intendano promuovere la segnalazione e la divulgazione delle vulnerabilità, il Centro di competenza e i membri della comunità delle competenze in materia di cibersicurezza («comunità») dovrebbero potere sostenere tali portatori di interessi, su richiesta degli stessi, nei limiti dei rispettivi compiti ed evitando duplicazioni con l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) istituita dal regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio ([6]).

(17) Il Centro di competenza, la comunità e la rete sono istituiti con l'intento di beneficiare dell'esperienza e dell'ampia e pertinente rappresentanza dei portatori di interessi, acquisite attraverso il partenariato pubblico-privato contrattuale sulla cibersicurezza tra la Commissione e l'Organizzazione europea per la cibersicurezza (ECSO) per la durata di Orizzonte 2020 — il programma quadro di ricerca e innovazione (2014-2020) istituito dal regolamento (UE) n. 1291/2013 del Parlamento europeo e del Consiglio ([7]), e attraverso gli insegnamenti tratti dai quattro progetti pilota avviati all'inizio del 2019 nell'ambito di Orizzonte 2020, segnatamente CONCORDIA, ECHO, SPARTA e CyberSec4Europe, nonché dal progetto pilota e dall'azione preparatoria sulle verifiche di software liberi e aperti (EU FOSSA), per la gestione e la rappresentanza della comunità all'interno del Centro di competenza.

(18) In considerazione della portata delle sfide poste dalla cibersicurezza e degli investimenti effettuati nelle capacità e abilità in materia di cibersicurezza in altre parti del mondo, l'Unione e gli Stati membri dovrebbero essere incoraggiati a incrementare il proprio sostegno finanziario alla ricerca, allo sviluppo e alla diffusione dell'innovazione in tale settore. Affinché sia possibile realizzare economie di scala e conseguire un livello di protezione comparabile in tutta l'Unione, gli Stati membri dovrebbero concentrare i propri sforzi in direzione di un quadro dell'Unione contribuendo attivamente al lavoro del Centro di competenza e della rete.

([4]) Regolamento (UE) 2021/… del Parlamento europeo e del Consiglio, del …, che istituisce Orizzonte Europa — il programma quadro di ricerca e innovazione — e ne stabilisce le norme di partecipazione e diffusione, e che abroga i regolamenti (UE) n. 1290/2013 e (UE) n. 1291/2013 (GU …).

([+]) Regolamento di cui al documento ST 7064/20.

([5]) Regolamento (UE) 2021/… del Parlamento europeo e del Consiglio, del …, che istituisce il programma Europa digitale e che abroga la decisione (UE) 2015/2240 (GU …).

([++]) Regolamento di cui al documento ST 6789/20.

([6]) Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sull'ENISA (l'Agenzia dell'Unione europea per la cibersicurezza) e sulla certificazione della cibersicurezza delle tecnologie dell'informazione e della comunicazione e che abroga il regolamento (UE) n. 526/2013 (legge sulla cibersicurezza) (GU L 151 del 7.6.2019, pag. 15).

([7]) Regolamento (UE) n. 1291/2013 del Parlamento europeo e del Consiglio, dell'11 dicembre 2013, che istituisce il programma quadro di ricerca e innovazione (2014-2020) — Orizzonte 2020 e abroga la decisione n. 1982/2006/CE (GU L 347 del 20.12.2013, pag. 104).

(19) Per favorire la competitività dell'Unione e standard elevati in materia di cibersicurezza a livello internazionale, il Centro di competenza e la comunità dovrebbero mirare a promuovere gli scambi con la comunità internazionale per quanto concerne gli sviluppi della cibersicurezza, compresi i prodotti e i processi, gli standard e le norme tecniche, ove ciò sia pertinente alla missione, agli obiettivi e ai compiti del Centro di competenza. Ai fini del presente regolamento, le norme tecniche pertinenti potrebbero comprendere la creazione di implementazioni di riferimento, incluse quelle pubblicate sulla base di licenze aperte standard.

(20) Il Centro di competenza ha sede a Bucarest.

(21) Nell'elaborare il suo programma di lavoro annuale (programma di lavoro annuale), il Centro di competenza dovrebbe informare la Commissione in merito al suo fabbisogno di cofinanziamenti sulla base dei contributi previsti dagli Stati membri a titolo di cofinanziamento per azioni congiunte, in modo tale che la Commissione possa tenere conto del contributo corrispondente dell'Unione nella preparazione del progetto di bilancio generale dell'Unione per l'esercizio successivo.

(22) Quando elabora il programma di lavoro di Orizzonte Europa per le questioni relative alla cibersicurezza, anche nel contesto del processo di consultazione dei portatori di interessi e, in special modo prima dell'adozione del programma di lavoro in questione, la Commissione dovrebbe tenere conto del contributo del Centro di competenza e condividerlo con il comitato di programma di Orizzonte Europa.

(23) Al fine di porre il Centro di competenza in grado di svolgere il suo ruolo nel settore della cibersicurezza e facilitare il coinvolgimento della rete e di dotare gli Stati membri di un forte ruolo di governance, il Centro di competenza dovrebbe essere istituito come organismo dell'Unione dotato di personalità giuridica a cui si applica il regolamento delegato (UE) 2019/715 ([8]) della Commissione. Il Centro di competenza dovrebbe svolgere un duplice ruolo assumendo compiti specifici nei settori industriale, tecnologico e della ricerca in materia di cibersicurezza, come stabilito nel presente regolamento, e gestendo contemporaneamente i finanziamenti legati alla cibersicurezza provenienti da diversi programmi, in particolare da Orizzonte Europa e dal programma Europa digitale e, se possibile, anche da altri programmi dell'Unione. Tale gestione dovrebbe essere conforme alle norme applicabili a detti programmi. Tuttavia, considerato che i finanziamenti per il funzionamento del Centro di competenza proverrebbero principalmente dal programma Europa digitale e da Orizzonte Europa, è necessario che il Centro di competenza sia considerato un partenariato ai fini dell'esecuzione del bilancio, compreso durante la fase di programmazione.

(24) Per effetto del contributo dell'Unione, l'accesso ai risultati delle attività e dei progetti del Centro di competenza deve essere il più aperto possibile e chiuso quanto necessario, e il riuso di tali risultati deve essere possibile, ove opportuno.

(25) Il Centro di competenza dovrebbe agevolare e coordinare l'attività della rete. La rete dovrebbe essere costituita da un centro nazionale di coordinamento in ciascuno Stato membro. I centri nazionali di coordinamento dei quali sia stata riconosciuta la capacità necessaria per gestire i fondi al fine di assolvere la missione e conseguire gli obiettivi di cui al presente regolamento dovrebbero ricevere il sostegno finanziario diretto dell'Unione, ivi comprese sovvenzioni concesse in assenza di un invito a presentare proposte, al fine di svolgere le loro attività in relazione al presente regolamento.

(26) I centri nazionali di coordinamento dovrebbero essere enti del settore pubblico o enti a partecipazione pubblica maggioritaria che esercitano funzioni amministrative pubbliche ai sensi del diritto nazionale, anche per delega, e dovrebbero essere selezionati dagli Stati membri. Le funzioni di un centro nazionale di coordinamento in un determinato Stato membro possono essere svolte da un ente che svolge altre funzioni prescritte dal diritto dell'Unione, ad esempio quelle di un'autorità nazionale competente, di un punto di contatto unico ai sensi della direttiva (UE) 2016/1148 o di qualsiasi altro regolamento dell'UE, oppure di un polo dell'innovazione digitale ai sensi del Regolamento (UE) 2021/… ([+]). Altri enti del settore pubblicoo enti che esercitano funzioni amministrative pubbliche in uno Stato membro dovrebbero poter assistere il centro nazionale di coordinamento in detto Stato membro nello svolgimento delle sue funzioni.

(27) I centri nazionali di coordinamento dovrebbero avere la capacità amministrativa necessaria, dovrebbero disporre di competenze in materia di cibersicurezza nell'ambito industriale, tecnologico e della ricerca in materia di cibersicurezza o potervi accedere ed essere in grado di interagire e di coordinarsi efficacemente con l'industria, il settore pubblico e la comunità della ricerca.

([8]) Regolamento delegato (UE) 2019/715 della Commissione, del 18 dicembre 2018, relativo al regolamento finanziario quadro degli organismi istituiti in virtù del TFUE e del trattato Euratom, di cui all'articolo 70 del regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio (GU L 122 del 10.5.2019, pag. 1).

([+]) Regolamento di cui al documento ST 6789/20.

(28) Il settore dell'istruzione negli Stati membri dovrebbe rispecchiare l'importanza di avere sensibilità e competenze adeguate in materia di cibersicurezza. A tal fine, tenendo conto del ruolo dell'ENISA e fatte salve le competenze degli Stati membri in materia di istruzione, i centri nazionali di coordinamento dovrebbero contribuire, accanto alle autorità pubbliche competenti e ai pertinenti portatori di interessi, alla promozione e alla diffusione di programmi didattici in materia di cibersicurezza.

(29) I centri nazionali di coordinamento dovrebbero poter ricevere sovvenzioni dal Centro di competenza al fine di fornire sostegno finanziario a terzi sotto forma di sovvenzioni. I costi diretti sostenuti dai centri nazionali di coordinamento per la fornitura e l'amministrazione del sostegno finanziario a terzi dovrebbero essere ammissibili al finanziamento a titolo dei pertinenti programmi.

(30) Il Centro di competenza, la rete e la comunità dovrebbero contribuire al progresso e alla diffusione dei prodotti, servizi e processi per la cibersicurezza. Contestualmente, il Centro di competenza e la rete dovrebbero promuovere le competenze in materia di cibersicurezza dell'industria sul versante della domanda, in particolare sostenendo sviluppatori e operatori in settori quali i trasporti, l'energia, la sanità, le finanze, l'amministrazione, le telecomunicazioni, la manifattura e lo spazio al fine di aiutare tali sviluppatori e operatori a risolvere i loro problemi di cibersicurezza, quali la messa in opera del principio della «sicurezza fin dalla progettazione ». Il Centro di competenza e la rete dovrebbero anche sostenere la normazione e la diffusione di prodotti, servizi e processi e per la cibersicurezza e promuovere al contempo, ove possibile, l'attuazione del quadro europeo di certificazione della cibersicurezza istituito dal regolamento (UE) 2019/881.

(31) Data la natura in rapido mutamento delle minacce informatiche e della cibersicurezza, l'Unione deve potersi adattare velocemente e continuamente ai nuovi sviluppi del settore. Di conseguenza, il Centro di competenza, la rete e la comunità dovrebbero essere sufficientemente flessibili da garantire la capacità necessaria di reagire a tali sviluppi. Dovrebbero agevolare progetti che aiutino gli enti a sviluppare costantemente capacità finalizzate a migliorare la loro resilienza e quella dell'Unione.

(32) Il Centro di competenza dovrebbe sostenere la comunità. Il Centro di competenza dovrebbe attuare le parti pertinenti alla cibersicurezza di Orizzonte Europa e del programma Europa digitale conformemente al programma di lavoro pluriennale del Centro di competenza (programma di lavoro pluriennale), al programma di lavoro annuale e al processo di pianificazione strategica di Orizzonte Europa assegnando sovvenzioni e altre forme di finanziamento, principalmente in seguito a un invito a presentare proposte su base competitiva. Il Centro di competenza dovrebbe altresì facilitare il trasferimento di competenze nell'ambito della rete e della comunità delle, nonché sostenere gli investimenti congiunti dell'Unione, degli Stati membri o dell'industria. Dovrebbe prestare particolare attenzione al sostegno delle PMI nel settore della cibersicurezza e alle azioni che contribuiscono a colmare il divario di competenze.

(33) L'assistenza tecnica per la preparazione dei progetti dovrebbe essere fornita in modo pienamente obiettivo e trasparente, per garantire che tutti i potenziali beneficiari ricevano le stesse informazioni, e deve evitare i conflitti di interesse.

(34) Il Centro di competenza dovrebbe stimolare e sostenere la cooperazione strategica a lungo termine e il coordinamento delle attività della comunità, coinvolgendo un gruppo vasto, aperto, interdisciplinare e diversificato di portatori di interessi europei impegnati nella tecnologia della cibersicurezza. La comunità dovrebbe includere organismi di ricerca, industrie e il settore pubblico. La comunità dovrebbe fornire il proprio contributo alle attività del Centro di competenza, al programma di lavoro pluriennale e al programma di lavoro annuale, in particolare tramite il gruppo consultivo strategico. La comunità dovrebbe altresì beneficiare delle attività di creazione di comunità del Centro di competenza e della rete, ma non dovrebbe essere privilegiata in altro modo per quanto riguarda gli inviti a presentare proposte o le gare d'appalto. La comunità dovrebbe essere costituita da organizzazioni e organi collettivi. Al contempo, per avvalersi di tutte le competenze in materia di cibersicurezza presenti nell'Unione, il Centro di competenza e i suoi organi dovrebbero potere anche ricorrere alle competenze di persone fisiche in qualità di esperti ad hoc.

(35) Il Centro di competenza dovrebbe cooperare e garantire sinergie con l'ENISA e dovrebbe ricevere da quest'ultima contributi pertinenti nella definizione delle priorità.

(36) Al fine di rispondere alle esigenze della cibersicurezza tanto sul versante della domanda quanto su quello dell'offerta, per il compito del Centro di competenza, ossia fornire alle imprese conoscenze e assistenza tecnica in tema di cibersicurezza, si dovrebbe tenere conto sia dei prodotti, dei processi e dei servizi delle TIC sia di tutti gli altri prodotti e processi tecnologici in cui occorre integrare la cibersicurezza. Se richiesto, anche il settore pubblico potrebbe beneficiare del sostegno del Centro di competenza.

(37) Al fine di procurare un ambiente della cibersicurezza sostenibile, è importante che la «sicurezza fin dalla progettazione» sia utilizzata come principio nel processo di sviluppo, manutenzione, funzionamento e aggiornamento delle infrastrutture, dei prodotti e dei servizi, in particolare sostenendo metodi di sviluppo sicuri e all'avanguardia, test di sicurezza adeguati e audit di sicurezza, mettendo a disposizione senza ritardo aggiornamenti per porre rimedio alle vulnerabilità o alle minacce note, nonché, ove possibile, consentendo a terzi di creare e fornire aggiornamenti al di là dei rispettivi limiti di vita dei prodotti. La «sicurezza fin dalla progettazione» dovrebbe essere assicurata nell'arco dell'intero ciclo di vita dei prodotti, servizi o processi TIC, nonché mediante un'evoluzione costante dei processi di sviluppo al fine di ridurre il rischio di danni derivanti da un utilizzo fraudolento.

(38) Considerando che il Centro di competenza e la rete dovrebbero cercare di rafforzare le sinergie e il coordinamento tra le dimensioni civili e di difesa della cibersicurezza, i progetti ai sensi del presente regolamento finanziati da Orizzonte Europa dovrebbero essere attuati in conformità del regolamento (UE) 2021/… (*), secondo cui le attività di ricerca e innovazione svolte nell'ambito di Orizzonte Europa devono riguardare esclusivamente le applicazioni civili.

(39) Il presente regolamento si applica principalmente in ambito civile, ma le attività degli Stati membri a norma del presente regolamento possono rispecchiare le specificità degli Stati membri nei casi in cui la politica in materia di cibersicurezza sia perseguita da autorità che esercitano sia attività in ambito civile che militare, dovrebbero mirare alla complementarità ed evitare sovrapposizioni con gli strumenti di finanziamento relativi alla difesa.

(40) Il presente regolamento dovrebbe garantire la responsabilità e la trasparenza del Centro di competenza e delle imprese che ricevono finanziamenti, in linea con i pertinenti regolamenti che istituiscono ciascun programma.

(41) L'attuazione dei progetti di diffusione, in particolare di quelli collegati alle infrastrutture e alle capacità utilizzate a livello di Unione o per mezzo di appalti congiunti, potrebbe essere suddivisa in diverse fasi di realizzazione, quali gare di appalto separate per la progettazione di hardware e architettura di software, la loro produzione, il loro funzionamento e la loro manutenzione, mentre le imprese potrebbero partecipare solo a una delle fasi e, ove opportuno, si potrebbe stabilire che i beneficiari in una o più di tali fasi soddisfino determinate condizioni per quanto riguarda la titolarità o il controllo europei.

(42) L'ENISA, tenuto conto delle sue competenze in materia di cibersicurezza e del suo mandato in quanto punto di riferimento per consulenze e competenze in materia di cibersicurezza per le istituzioni, gli organi e gli organismi dell'Unione, nonché per i pertinenti portatori di interessi dell'Unione, e tenuto conto dei contributi apportati mediante i suoi compiti, dovrebbe svolgere un ruolo attivo nelle attività del Centro di competenza, compreso lo sviluppo dell'agenda, evitando duplicazioni dei compiti in particolare grazie al suo ruolo di osservatore permanente nel consiglio di direzione del Centro di competenza. Per quanto riguarda l'elaborazione dell'agenda, il programma di lavoro annuale e il programma di lavoro pluriennale, il direttore esecutivo del Centro di competenza e il consiglio di direzione dovrebbero tenere conto di qualsiasi pertinente consulenza strategica e contributo forniti dall'ENISA, in conformità del regolamento interno del consiglio di direzione.

(43) Qualora ricevano un contributo finanziario dal bilancio generale dell'Unione, i centri nazionali di coordinamento e gli enti che fanno parte della comunità dovrebbero pubblicizzare il fatto che le rispettive attività sono intraprese nel contesto del presente regolamento.

(44) Le spese derivanti dalle attività di istituzione, amministrazione e coordinamento del Centro di competenza dovrebbero essere finanziate dall'Unione e dagli Stati membri, in proporzione ai rispettivi contributi volontari alle azioni congiunte. Al fine di evitare i doppi finanziamenti, tali attività non dovrebbero beneficiare contemporaneamente di un contributo a titolo di altri programmi dell'Unione.

(45) Il consiglio di direzione, che dovrebbe essere composto da rappresentanti degli Stati membri e della Commissione, dovrebbe definire l'orientamento generale delle operazioni del Centro di competenza e garantire che quest'ultimo svolga i propri compiti conformemente al presente regolamento. Il consiglio di direzione dovrebbe adottare l'agenda.

(46) Al consiglio di direzione dovrebbero essere conferiti i poteri necessari per formare il bilancio del Centro di competenza. Esso dovrebbe verificarne l'esecuzione, adottare le opportune regole finanziarie, e stabilire procedure operative trasparenti per l'iter decisionale del Centro di competenza, incluso per l'adozione, tenendo conto dell'agenda, del programma di lavoro annuale e del programma di lavoro pluriennale. Il consiglio di direzione dovrebbe inoltre adottare il proprio regolamento interno, nominare il direttore esecutivo e decidere in merito alla proroga e alla cessazione del mandato del direttore esecutivo.

(*) Regolamento di cui al documento ST 7064/20.

(47) Il consiglio di direzione dovrebbe esercitare una funzione di controllo sulle attività strategiche e di attuazione del Centro di competenza e assicurare l'allineamento tra di esse. Nella sua relazione annuale, il Centro di competenza dovrebbe porre in particolare l'accento sugli obiettivi strategici conseguiti e, se necessario, proporre azioni per migliorarne ulteriormente il conseguimento.

(48) Per garantire il funzionamento corretto ed efficace del Centro di competenza, la Commissione e gli Stati membri dovrebbero assicurare che le persone da nominare nel consiglio di direzione 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 direzione, per assicurare la continuità dei lavori.

(49) In considerazione dello status specifico del Centro di competenza e della sua responsabilità per quanto riguarda l'esecuzione dei fondi dell'Unione, in particolare di quelli provenienti da Orizzonte Europa e dal programma Europa digitale, la Commissione dovrebbe disporre, nell'ambito del consiglio di direzione, del 26 % dei voti totali per le decisioni che riguardano fondi dell'Unione, al fine di massimizzare il valore aggiunto dell'Unione di tali decisioni, garantendone nel contempo la legalità e l'allineamento con le priorità dell'Unione.

(50) Il corretto funzionamento del Centro di competenza esige che il direttore esecutivo sia nominato in modo trasparente in base ai meriti, alla comprovata esperienza amministrativa e manageriale, nonché alla competenza e all'esperienza acquisite in materia di cibersicurezza, e che le sue funzioni siano svolte in completa indipendenza.

(51) Il Centro di competenza dovrebbe avvalersi di un gruppo consultivo strategico. Il gruppo consultivo strategico dovrebbe fornire consulenze sulla base di un dialogo costante tra il Centro di competenza e la comunità, che dovrebbe essere formata dai rappresentanti del settore privato, delle organizzazioni dei consumatori, del mondo accademico e di altri pertinenti portatori di interessi. Il gruppo consultivo strategico dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione del consiglio di direzione e del direttore esecutivo. I compiti del gruppo consultivo strategico dovrebbero includere la fornitura di consulenze in merito all'agenda, al programma di lavoro annuale e al programma di lavoro pluriennale. La rappresentanza dei diversi portatori di interessi nel gruppo consultivo strategico dovrebbe essere equilibrata, riservando particolare attenzione alla rappresentanza delle PMI, al fine di garantire che la rappresentanza di tali portatori di interessi sia adeguatamente rappresentata nel lavoro svolto dal Centro di competenza.

(52) I contributi degli Stati membri alle risorse del Centro di competenza potrebbero essere finanziari o in natura. Ad esempio, tali contributi finanziari potrebbero consistere in una sovvenzione concessa da uno Stato membro a un beneficiario in tale Stato membro a integrazione del sostegno finanziario dell'Unione a un progetto nell'ambito del programma di lavoro annuale. Altrimenti, i contributi in natura sarebbero tipicamente forniti qualora un ente di uno Stato membro sia esso stesso beneficiario di un sostegno finanziario dell'Unione. Ad esempio, se l'Unione ha sovvenzionato un'attività di un centro nazionale di coordinamento al tasso di finanziamento del 50 %, il costo restante dell'attività sarebbe contabilizzato come un contributo in natura. Un altro caso a titolo esemplificativo potrebbe essere quello in cui qualora un ente di uno Stato membro abbia ricevuto un sostegno finanziario dell'Unione per la creazione o il miglioramento di un'infrastruttura da condividere tra i portatori di interessi in linea con il programma di lavoro annuale, i relativi costi non sovvenzionati sarebbero contabilizzati come contributi in natura.

(53) Ai sensi delle pertinenti disposizioni del regolamento delegato (UE) 2019/715 sui conflitti di interesse, il Centro di competenza dovrebbe disporre di norme relative alla prevenzione, all'individuazione, alla risoluzione e alla gestione dei conflitti di interessi che riguardino i suoi membri, i suoi organi e il suo personale, nonché il consiglio di direzione, il gruppo consultivo strategico e la comunità. Gli Stati membri dovrebbero garantire la prevenzione, l'individuazione e la risoluzione dei conflitti di interessi in relazione ai centri nazionali di coordinamento, conformemente al diritto nazionale. Il Centro di competenza dovrebbe inoltre applicare il pertinente diritto dell'Unione in materia di accesso del pubblico ai documenti stabilite dal regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio ([9]). Il trattamento dei dati personali da parte del Centro di competenza dovrebbe essere soggetto al regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([10]). È opportuno che il Centro di competenza si conformi alle disposizioni del diritto dell'Unione applicabili alle istituzioni dell'Unione e al diritto nazionale in materia di gestione delle informazioni, in particolare delle informazioni sensibili non classificate e delle informazioni classificate UE.

([9]) 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).

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

(54) È opportuno che gli interessi finanziari dell'Unione e degli Stati membri siano tutelati durante l'intero ciclo di spesa attraverso misure proporzionate, tra cui la prevenzione, l'individuazione e l'indagine delle irregolarità, il recupero dei fondi perduti, indebitamente versati o non correttamente utilizzati e, se del caso, attraverso l'applicazione di sanzioni amministrative e finanziarie, in conformità del regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio ([11]) («regolamento finanziario»).

(55) Il Centro di competenza dovrebbe operare in modo aperto e trasparente. Dovrebbe fornire tempestivamente tutte le informazioni pertinenti e promuovere le proprie attività, incluse le attività di informazione e divulgazione destinate al pubblico. Il regolamento interno del consiglio di direzione del Centro di competenza e del comitato consultivo strategico dovrebbe essere reso pubblico.

(56) È opportuno che il revisore interno della Commissione eserciti nei confronti del Centro di competenza le stesse competenze esercitate nei confronti della Commissione.

(57) La Commissione, la Corte dei conti e l'Ufficio europeo per la lotta antifrode dovrebbero avere accesso a tutte le informazioni necessarie e ai locali del Centro di competenza per eseguire audit e svolgere indagini sulle sovvenzioni, i contratti e gli accordi firmati dal Centro di competenza.

(58) Poiché gli obiettivi del presente regolamento — ossia rafforzare la competitività e le capacità dell'Unione, mantenere e sviluppare le capacità tecnologiche, industriali e di ricerca dell'Unione in materia di cibersicurezza, aumentare la competitività dell'industria della cibersicurezza dell'Unione e trasformare la cibersicurezza in un vantaggio competitivo per altri settori industriali dell'Unione — non possono essere conseguiti in misura sufficiente dai soli Stati membri, a causa della dispersione delle limitate risorse e dell'entità dell'investimento necessario ma, a motivo della necessità di evitare inutili duplicazioni degli sforzi, contribuire al raggiungimento di una massa critica di investimenti, garantire l'utilizzo ottimale dei finanziamenti pubblici, e garantire che un livello elevato di cibersicurezza sia promosso in tutti gli Stati membri, possono essere conseguiti meglio a livello di Unione, l'Unione può adottare misure in conformità del principio di sussidiarietà di cui all'articolo 5 del trattato sull'Unione europea (TUE). Il presente regolamento si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

DISPOSIZIONI GENERALI E PRINCIPI DEL CENTRO DI COMPETENZA E DELLA RETE

Articolo 1

Oggetto e ambito di applicazione

1. Il presente regolamento istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca sulla cibersicurezza («Centro di competenza») e la rete dei centri nazionali di coordinamento («rete»). Stabilisce le modalità di designazione dei centri nazionali di coordinamento e le norme per l'istituzione della comunità delle competenze in materia di cibersicurezza («comunità»).

2. Il Centro di competenza svolge un ruolo essenziale nell'attuazione della parte relativa alla cibersicurezza del Programma Europa digitale, in particolare riguardo delle azioni di cui all'articolo 6 del regolamento (UE) 2021/… ([+]) e contribuisce all'attuazione di Orizzonte Europa, in particolare riguardo del pilastro II, sezione 3.1.3., dell'allegato I della decisione (UE) …/… e del Consiglio ([12]) ([++]).

3. Gli Stati membri contribuiscono collettivamente ai lavori del Centro di competenza e della rete.

4. Il presente regolamento fa salve le competenze degli Stati membri per quanto riguardala pubblica sicurezza, la difesa, la sicurezza nazionale e le attività dello Stato nell'ambito del diritto penale.

([11]) Regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio, del 18 luglio 2018, che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione, che modifica i regolamenti (UE) n. 1296/2013, (UE) n. 1301/2013, (UE) n. 1303/2013, (UE) n. 1304/2013, (UE) n. 1309/2013, (UE) n. 1316/2013, (UE) n. 223/2014, (UE) n. 283/2014 e la decisione n. 541/2014/UE e abroga il regolamento (UE, Euratom) n. 966/2012 (GU L 193 del 30.7.2018, pag. 1).

([+]) Regolamento di cui al documento ST 6789/20.

([12]) Decisione (UE) …/… del Consiglio del … che istituisce il programma specifico per l'attuazione di Orizzonte Europa — il programma quadro per la ricerca e l'innovazione, e che abroga la decisione 2013/743/UE (GU …).

([++]) Decisione di cui al documento ST 8967/20.

Articolo 2

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) «cibersicurezza»: le attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche;

2) «rete e sistema informativo»: una rete e un sistema informativo quali definiti all'articolo 4, punto 1, della direttiva (UE) 2016/1148;

3) «prodotti, servizi e processi per la cibersicurezza»: prodotti, servizi o processi TIC commerciali e non commerciali con la finalità specifica di proteggere la rete e i sistemi informativi o garantire la riservatezza, l'integrità e l'accessibilità dei dati che sono trattati o conservati nella rete e nei sistemi informativi, nonché la cibersicurezza degli utenti di tali sistemi e di altre persone interessate dalle minacce informatiche;

4) «minaccia informatica»: qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone;

5) «azione congiunta»: un'azione prevista nel programma di lavoro annuale che riceve un sostegno finanziario a titolo di Orizzonte Europa, del Programma Europa digitale o di altri programmi dell'Unione, nonché un sostegno finanziario o in natura da parte di uno o più Stati membri, ed è attuata mediante progetti che coinvolgono beneficiari stabiliti in tali negli Stati membri e che ricevono un sostegno finanziario o in natura ai beneficiari provenienti dai medesimi Stati membri;

6) «contributo in natura»: spese ammissibili sostenute dai centri nazionali di coordinamento e da altri enti pubblici quando questi partecipano a progetti finanziati dal presente regolamento, laddove tali spese non sono finanziate mediante un contributo dell'Unione o un contributo finanziario degli Stati membri;

7) «poli europei dell'innovazione digitale»: poli europei dell'innovazione digitale ai sensi dell'articolo 2, lettera e), del regolamento (UE) 2021/… ([+]);

8) «agenda»: una strategia di cibersicurezza in materia industriale, tecnologica e della ricerca globale e sostenibile, che formula raccomandazioni strategiche per lo sviluppo e la crescita del settore europeo della cibersicurezza nell'ambito industriale, tecnologico e della ricerca, e che contiene le priorità strategiche per le attività del Centro di competenza e non è vincolante per quanto attiene alle decisioni da adottare riguardo ai programmi di lavoro annuali;

9) «assistenza tecnica»: l'assistenza del Centro di competenza offerta ai centri nazionali di coordinamento o alla comunità nello svolgimento dei loro compiti, fornendo conoscenze o agevolando l'accesso a competenze tecnologiche, industriali e di ricerca in materia di cibersicurezza, facilitando la creazione di reti, sensibilizzando e promuovendo la cooperazione, o l'assistenza del Centro di competenza in collaborazione con i centri nazionali di coordinamento offerta ai portatori di interessi riguardo alla preparazione di progetti in relazione alla missione del Centro di competenza e della rete e agli obiettivi del Centro di competenza.

Articolo 3

Missione del Centro di competenza e della rete

1. La missione del Centro di competenza e della rete è di aiutare l'Unione a:

a) potenziare la sua leadership e la sua autonomia strategica in materia di cibersicurezza mantenendo e sviluppando le capacità e i mezzi dell'Unione in materia di cibersicurezza a livello accademico, sociale, tecnologico, industriale e della ricerca, necessari per rafforzare la fiducia e la sicurezza, ivi comprese la riservatezza, l'integrità e l'accessibilità dei dati nel mercato unico digitale;

b) sostenere le capacità, i mezzi e le competenze tecnologiche dell'Unione in relazione alla resilienza e all'affidabilità dell'infrastruttura della rete e dei sistemi informativi, ivi comprese le infrastrutture critiche nonché gli hardware e i software comunemente utilizzati nell'Unione; e

c) aumentare la competitività globale dell'industria della cibersicurezza dell'Unione, per garantire standard elevati in materia di cibersicurezza in tutta l'Unione e trasformare la cibersicurezza in un vantaggio competitivo per altri settori industriali dell'Unione.

([+]) Regolamento di cui al documento ST 6789/20.

2. Il Centro di competenza e la rete svolgono i loro compiti in collaborazione con l'ENISA e la comunità, se del caso.

3. Il Centro di competenza, conformemente agli atti legislativi che istituiscono i pertinenti programmi, in particolare Orizzonte Europa e il Programma Europa digitale, utilizza le pertinenti risorse finanziarie dell'Unione in modo tale da contribuire alla missione di cui al paragrafo 1.

Articolo 4

Obiettivi del Centro di competenza

1. Il Centro di competenza ha l'obiettivo generale di promuovere la ricerca, l'innovazione e la diffusione nel settore della cibersicurezza al fine di assolvere la missione di cui all'articolo 3.

2. Il Centro di competenza ha gli obiettivi specifici seguenti:

a) rafforzare le capacità, i mezzi, le conoscenze e le infrastrutture in materia di cibersicurezza a favore dell'industria, in particolare le PMI, le comunità della ricerca, il settore pubblico e la società civile, nella maniera ritenuta appropriata;

b) promuovere la resilienza e l'adozione di migliori prassi in materia di cibersicurezza, nonché il principio della «sicurezza fin dalla progettazione» e la certificazione della sicurezza dei prodotti e dei servizi digitali, integrando gli sforzi di altri soggetti pubblici;

c) contribuire a creare un solido ecosistema europeo della cibersicurezza che riunisca tutti i pertinenti portatori di interessi.

3. Il Centro di competenza attua gli obiettivi specifici di cui al paragrafo 2 mediante:

a) la definizione di raccomandazioni strategiche per la ricerca, l'innovazione e la diffusione nel settore della cibersicurezza, in conformità del diritto dell'Unione, nonché la definizione delle priorità strategiche per le attività del Centro di competenza;

b) l'attuazione di azioni nell'ambito dei pertinenti programmi di finanziamento dell'Unione in conformemente ai pertinenti programmi di lavoro e atti legislativi dell'Unione che istituiscono tali programmi di finanziamento;

c) la promozione della cooperazione e del coordinamento tra i centri nazionali di coordinamento nonché con la comunità e al suo interno; e

d) ove pertinente e opportuno, l'acquisizione e il funzionamento di infrastrutture e servizi TIC ove necessario per svolgere i compiti di cui all'articolo 5 e conformemente ai rispettivi programmi di lavoro di cui all'articolo 5, paragrafo 3, lettera b).

Articolo 5

Compiti del Centro di competenza

1. Al fine di assolvere la missione e conseguire gli obiettivi, il Centro di competenza ha i compiti seguenti:

a) compiti strategici; e

b) compiti di esecuzione.

2. I compiti strategici di cui al paragrafo 1, lettera 1) consistono in:

a) sviluppare e monitorare l'attuazione dell'agenda;

b) attraverso l'agenda e il programma di lavoro pluriennale, evitando nel contempo duplicazioni delle attività con l'ENISA e tenendo conto della necessità di creare sinergie tra la cibersicurezza e altre parti di Orizzonte Europa e del Programma Europa digitale:

   i) definire le priorità per i lavori del Centro di competenza in relazione a:

      1) il rafforzamento della ricerca e dell'innovazione in materia di cibersicurezza, coprendo l'intero ciclo dell'innovazione, e la diffusione di tale ricerca e innovazione;

      2) lo sviluppo di capacità, abilità e infrastrutture di cibersicurezza nell'ambito industriale, tecnologico e della ricerca;

      3) il rafforzamento delle competenze e delle capacità in materia di cibersicurezza e tecnologia nei settori dell'industria, della tecnologia e della ricerca nonché a tutti i livelli di istruzione pertinenti, sostenendo l'equilibrio di genere;

      4) la diffusione di prodotti, servizi e processi per la cibersicurezza;

5) il sostegno alla diffusione sul mercato di prodotti, servizi e processi per la cibersicurezza atti a contribuire alla missione di cui all'articolo 3;

6) il sostegno all'adozione e all'integrazione di prodotti, servizi e processi all'avanguardia per la cibersicurezza da parte delle autorità pubbliche, su loro richiesta, delle industrie sul versante della domanda e di altri utenti;

ii) sostenere l'industria della cibersicurezza, in particolare le PMI, al fine di rafforzare l'eccellenza, la capacità e la competitività dell'Unione riguardo alla cibersicurezza, anche al fine di accedere a mercati potenziali e opportunità di diffusione e di attrarre investimenti; e

iii) fornire sostegno e assistenza tecnica alle start-up, alle PMI, alle microimprese, alle associazioni, ai singoli esperti e ai progetti di tecnologia civica nel settore della cibersicurezza;

c) assicurare le sinergie e la cooperazione tra altre istituzioni, organi e organismi pertinenti dell'Unione, in particolare l'ENISA, evitando nel contempo duplicazioni delle attività con tali istituzioni, organi e organismi dell'Unione;

d) coordinare i centri nazionali di coordinamento attraverso la rete e garantire uno scambio regolare di competenze;

e) fornire agli Stati membri che ne facciano richiesta consulenze qualificate in materia di cibersicurezza nell'ambito industriale, tecnologico e della ricerca, anche in merito ad appalti e diffusione di tecnologie;

f) facilitare la collaborazione e la condivisione di competenze tra tutti i pertinenti portatori di interessi, in particolare i membri della comunità;

g) partecipare a conferenze, fiere e consessi nazionali, dell'Unione e internazionali connessi alla missione, agli obiettivi e ai compiti del Centro di competenza, allo scopo di condividere opinioni e scambiare le migliori prassi pertinenti con altri partecipanti;

h) facilitare l'utilizzo dei risultati dei progetti di ricerca e innovazione nelle azioni connesse allo sviluppo di prodotti, servizi e processi per la cibersicurezza, cercando di evitare la frammentazione e la duplicazione degli sforzi e replicando le buone pratiche in materia di cibersicurezza e i prodotti, servizi e processi per la cibersicurezza, in particolare quelli sviluppati dalle PMI e quelli che utilizzano software con codice sorgente aperto (open source);

3. i compiti di esecuzione, di cui al paragrafo 1, lettera b), consistono in:

a) coordinare e amministrare i lavori della rete e della comunità al fine di assolvere la missione di cui all'articolo 3, in particolare sostenendo le start-up, le PMI, le microimprese, le associazioni e i progetti di tecnologia civica nel settore della cibersicurezza nell'Unione e facilitando il loro accesso alle competenze, ai finanziamenti, agli investimenti e ai mercati;

b) stabilire e attuare il programma di lavoro annuale, in linea con l'agenda e con il programma di lavoro pluriennale, per quanto riguarda le parti relative alla cibersicurezza:

i) del Programma Europa digitale e, in particolare, delle azioni di cui all'articolo 6 del regolamento (UE) 2021/… (+);

ii) delle azioni congiunte che ricevono il sostegno, ai sensi delle disposizioni relative alla cibersicurezza di Orizzonte Europa, in particolare riguardo al pilastro II, sezione 3.1.3, dell'allegato I della decisione(UE) 2021/… (++), e conformemente al programma di lavoro pluriennale, nonché al processo di pianificazione strategica di Orizzonte Europa; e

iii) di altri programmi, ove previsto nei pertinenti atti legislativi dell'Unione;

c) sostenere, se del caso, la realizzazione dell'obiettivo specifico 4 «Competenze digitali avanzate» di cui all'articolo 7 del regolamento (UE) 2021/… (+) in cooperazione con i poli europei dell'innovazione digitale;

d) fornire consulenze qualificate in materia di cibersicurezza nell'ambito industriale, tecnologico e della ricerca alla Commissione quando quest'ultima elabora i progetti di programmi di lavoro a norma dell'articolo 13 della decisione (UE) 2021/… (++);

(+) Regolamento di cui al documento ST 6789/20.
(++) Decisione di cui al documento ST 8967/20.

e) realizzare o consentire la diffusione di infrastrutture TIC e facilitarne l'acquisizione a beneficio della società, dell'industria e del settore pubblico su richiesta degli Stati membri, delle comunità di ricerca e degli operatori di servizi essenziali mediante, tra l'altro, contributi degli Stati membri e finanziamenti dell'Unione per azioni congiunte, i conformemente all'agenda, al programma di lavoro pluriennale e al programma di lavoro annuale;

f) sensibilizzare alla missione del Centro di competenza e della rete e agli obiettivi e ai compiti del Centro di competenza; e

g) fatta salva la natura civile dei progetti da finanziare a titolo di Orizzonte Europa e in conformità dei regolamenti (UE) 2021/… (+) e … (UE) 2021/… (++), migliorare le sinergie e il coordinamento tra gli aspetti della cibersicurezza civili e della difesa, mediante la facilitazione dello scambio di:

i) conoscenze e informazioni in merito alle tecnologie e applicazioni a duplice uso;

ii) risultati, requisiti e migliori pratiche; e

iii) informazioni sulle priorità dei pertinenti programmi dell'Unione.

4. Il Centro di competenza svolge i compiti di cui al paragrafo 1 in stretta collaborazione con la rete.

5. Conformemente all'articolo 6 del regolamento (UE) 2021/… (+) e con riserva di un accordo di contributo ai sensi dell'articolo 2, punto 18), del regolamento finanziario, il Centro di competenza può essere incaricato dell'attuazione delle parti relative alla cibersicurezza nel quadro di Orizzonte Europa non cofinanziate dagli Stati membri, in particolare riguardo al pilastro II, sezione 3.1.3, dell'allegato I della decisione (UE) 2021/… (+++).

Articolo 6

Designazione dei centri nazionali di coordinamento

1. Entro il … *[sei mesi dall'entrata in vigore del presente regolamento]*, ciascuno Stato membro designa un ente conforme ai criteri di cui al paragrafo 5 che agisce in qualità di centro nazionale di coordinamento ai fini del presente regolamento. Ciascuno Stato membro ne informa il consiglio di direzione senza ritardo. Tale ente può essere un ente già situato in tale Stato membro.

Il termine di cui al primo comma del presente paragrafo è prorogato per il periodo durante il quale la Commissione emette il parere di cui al paragrafo 2.

2. Uno Stato membro può, in qualsiasi momento, chiedere alla Commissione un parere in merito al possesso della necessaria capacità dell'ente che ha designato o intende designare quale proprio centro nazionale di coordinamento per la gestione dei fondi al fine di assolvere la missione e conseguire gli obiettivi di cui al presente regolamento. La Commissione emette il suo parere a tale Stato membro entro tre mesi dalla richiesta.

3. Sulla base della notifica da parte di uno Stato membro di un ente di cui al paragrafo 1, il consiglio di direzione provvede, entro tre mesi dalla notifica, a inserire nell'elenco tale ente in quanto centro nazionale di coordinamento. Il Centro di competenza pubblica l'elenco dei centri nazionali di coordinamento designati.

4. Gli Stati membri possono designare in qualsiasi momento un nuovo ente come centro nazionale di coordinamento ai fini del presente regolamento. I paragrafi 1, 2 e 3 si applicano alla designazione di qualsiasi nuovo ente.

5. Il centro nazionale di coordinamento designato è un ente del settore pubblico o un ente a partecipazione pubblica maggioritaria che esercita funzioni amministrative pubbliche ai sensi del diritto nazionale, anche per delega, ed è in grado di sostenere il Centro di competenza e la rete nell'assolvimento della loro missione di cui all'articolo 3 del presente regolamento. Esso dispone di competenze in materia di cibersicurezza nell'ambito della ricerca e della tecnologia o vi ha accesso. Esso è in grado di interagire e di coordinarsi efficacemente con l'industria, il settore pubblico, la comunità accademica e della ricerca e i cittadini, nonché con le autorità designate a norma della direttiva (UE) 2016/1148.

6. In qualsiasi momento, i centri nazionali di coordinamento possono chiedere di ottenere il riconoscimento della loro necessaria capacità di gestire i fondi in per assolvere la missione e conseguire gli obiettivi di cui al presente regolamento, conformemente ai regolamenti (UE) 2021/… (+) e (UE) 2021/… (++). Entro tre mesi da tale richiesta, la Commissione valuta tale capacità del centro nazionale di coordinamento in questione di gestire i fondi e adotta una decisione.

(+) Regolamento di cui al documento ST 7064/20.
(++) Regolamento di cui al documento ST 6789/20.
(+++) Decisione di cui al documento ST 8967/20.

Se uno Stato membro riceve il parere positivo della Commissione secondo la procedura di cui al paragrafo 2, tale parere è considerato una decisione che riconosce in capo al pertinente ente la sussistenza della necessaria capacità per i fini di cui al presente paragrafo.

Entro il … *[due mesi dalla data di entrata in vigore del presente regolamento]*, previa consultazione del consiglio di direzione, la Commissione formula orientamenti sulla valutazione di cui al primo comma, inclusa la precisazione delle condizioni per il riconoscimento e delle modalità di elaborazione dei pareri e delle valutazioni.

Prima di emettere il parere di cui al paragrafo 2 e la decisione di cui al primo comma del presente paragrafo, la Commissione tiene conto di ogni informazione e documentazione fornita dal centro nazionale di coordinamento richiedente.

Qualsiasi decisione di non riconoscere in capo ad un centro nazionale di coordinamento la sussistenza della necessaria capacità di gestire fondi per assolvere la missione e conseguire gli obiettivi di cui al presente regolamento deve essere debitamente motivata, indicando i requisiti che il centro nazionale di coordinamento richiedente deve ancora soddisfare che giustificano la decisione di diniego di riconoscimento. Qualsiasi centro nazionale di coordinamento la cui richiesta di riconoscimento sia stata respinta può presentare nuovamente la richiesta in qualsiasi momento corredandola di informazioni supplementari.

Gli Stati membri informano la Commissione in caso di cambiamenti relativi al centro nazionale di coordinamento, quali la composizione centro nazionale di coordinamento, la sua natura giuridica o altri aspetti pertinenti, che incidono sulla sua capacità di gestire i fondi dell'Unione per assolvere la missione e conseguire gli obiettivi di cui al presente regolamento. Una volta ricevute tali informazioni, la Commissione può rivedere di conseguenza la sua decisione di concedere o negare il riconoscimento in capo al centro nazionale di coordinamento della sussistenza della necessaria capacità di gestire fondi per assolvere la missione e conseguire gli obiettivi.

7. La rete è costituita da tutti i centri nazionali di coordinamento notificati al consiglio di direzione dagli Stati membri.

Articolo 7

Compiti dei centri nazionali di coordinamento

1. I centri nazionali di coordinamento hanno i compiti seguenti:

a) fungere da punti di contatto a livello nazionale per la comunità al fine di assistere il Centro di competenza nell'assolvimento della sua missione e nel conseguimento dei suoi obiettivi, in particolare nel coordinamento della comunità mediante il coordinamento dei membri della comunità nei loro Stati membri;

b) fornire consulenza riguardo ai compiti strategici di cui all'articolo 5, paragrafo 2, e contribuire attivamente a tali compiti, tenendo conto delle pertinenti sfide nazionali e regionali per la cibersicurezza nei diversi settori;

c) promuovere, incoraggiare e agevolare la partecipazione della società civile, dell'industria, in particolare delle start-up e delle PMI, della comunità accademica e della ricerca, nonché di altri portatori di interessi a livello nazionale ai progetti transfrontalieri e alle azioni relative alla cibersicurezza finanziati dai pertinenti programmi dell'Unione;

d) fornire assistenza tecnica ai portatori di interessi sostenendoli nella fase di presentazione delle domande per i progetti gestiti dal Centro di competenza in relazione alla sua missione e ai suoi obiettivi e nel pieno rispetto delle norme di sana gestione finanziaria, in particolare riguardo al conflitto di interessi;

e) cercare di creare sinergie con attività pertinenti a livello nazionale, regionale e locale, quali le politiche nazionali in materia di ricerca, sviluppo e innovazione nel settore della cibersicurezza, in particolare delle politiche indicate nelle strategie nazionali in materia di cibersicurezza;

f) attuare azioni specifiche per le quali il Centro di competenza ha concesso sovvenzioni, anche fornendo sostegno finanziario a terzi, conformemente all'articolo 204 del regolamento finanziario, alle condizioni specificate nelle convenzioni di sovvenzione pertinenti;

g) fatte salve le competenze degli Stati membri in materia di istruzione e tenendo conto dei pertinenti compiti dell'ENISA, avviare un dialogo con le autorità nazionali in merito a un possibile contributo alla promozione e alla diffusione di programmi didattici in materia di cibersicurezza;

h) promuovere e divulgare i risultati dell'attività della rete, della comunità e del Centro di competenza a livello nazionale, regionale o locale;

i) valutare le richieste di adesione alla comunità da parte di enti situati nello stesso Stato membro del centro nazionale di coordinamento;

j) sostenere e promuovere la partecipazione degli enti pertinenti alle attività condotte dal Centro di competenza, dalla rete e dalla comunità, e monitorare, se del caso, il livello di impegno nello sviluppo e nella diffusione della ricerca in tema di cibersicurezza, e il relativo ammontare di sostegno finanziario pubblico.

2. Ai fini del paragrafo 1, lettera f), del presente articolo il sostegno finanziario a terzi può essere fornito sotto una qualsiasi delle forme di contributo dell'Unione specificate all'articolo 125 del regolamento finanziario, anche sotto forma di somme forfettarie.

3. In base a una decisione di cui all'articolo 6, paragrafo 6, del presente regolamento, i centri nazionali di coordinamento possono ricevere una sovvenzione dall'Unione a norma dell'articolo 195, primo comma, lettera d), del regolamento finanziario in relazione all'espletamento dei compiti stabiliti dal presente articolo.

4. Se del caso, i centri nazionali di coordinamento cooperano mediante la rete.

Articolo 8

Comunità delle competenze in materia di cibersicurezza

1. La comunità contribuisce alla missione del Centro di competenza e della rete di cui all'articolo 3, consolidando, condividendo e divulgando le competenze in materia di cibersicurezza in tutta l'Unione.

2. La comunità è costituita da organizzazioni industriali, comprese le PMI, accademiche e di ricerca, da altre associazioni pertinenti della società civile, nonché, se del caso, da organizzazioni europee di normazione, enti pubblici o altri enti pertinenti che si occupano di questioni operative e tecniche in materia di cibersicurezza e, se del caso, da portatori di interessi nei settori interessati alla cibersicurezza e che sono posti di fronte a sfide in materia di cibersicurezza. La comunità riunisce i principali portatori di interessi per quanto concerne le capacità in materia di cibersicurezza nell'ambito tecnologico, industriale, accademico e della ricerca nell'Unione, coinvolgendo i centri nazionali di coordinamento, i poli europei dell'innovazione digitale, se del caso, e le istituzioni, gli organi e gli organismi competenti dell'Unione, quali l'ENISA.

3. Solo enti istituiti all'interno degli Stati membri possono essere registrati in qualità di membri della comunità. Essi dimostrano di essere in grado di contribuire alla missione e possiedono competenze in materia di cibersicurezza in merito ad almeno uno degli ambiti seguenti:

a) ambito accademico, ricerca o innovazione;

b) sviluppo industriale o di prodotti;

c) formazione e istruzione;

d) sicurezza delle informazioni o interventi in caso di incidenti;

e) etica;

f) normazione e specifiche formali e tecniche.

4. Il Centro di competenza registra, su loro richiesta, enti in quanto membri della comunità delle competenze in materia di cibersicurezza dopo una valutazione, effettuata dal centro nazionale di coordinamento dello Stato membro in tali enti sono stabiliti, al fine di confermare che tali enti soddisfano i criteri di cui al paragrafo 3 del presente articolo. Tale valutazione tiene parimenti conto, se del caso, di eventuali valutazioni nazionali effettuate per motivi di sicurezza dalle autorità nazionali competenti. Tali registrazioni non sono limitate nel tempo, ma possono essere revocate in qualsiasi momento dal Centro di competenza se il centro nazionale di coordinamento pertinente ritiene che l'ente in questione non soddisfi più i criteri di cui al paragrafo 3 del presente articolo o rientri nell'ambito di applicazione dell'articolo 136 del regolamento finanziario, oppure per giustificati motivi di sicurezza. In caso di revoca dell'adesione alla comunità per motivi di sicurezza, la decisione di revoca è proporzionata e motivata. I centri nazionali di coordinamento mirano a conseguire una rappresentanza equilibrata dei portatori di interessi nella comunità, e stimolano attivamente la partecipazione, in particolare delle PMI.

5. I centri nazionali di coordinamento sono incoraggiati a cooperare mediante la rete al fine di armonizzare le modalità di applicazione dei criteri di cui al paragrafo 3 e le procedure di valutazione e registrazione degli enti di cui al paragrafo 4.

6. Il Centro di competenza registra istituzioni, organi e organismi competenti dell'Unione quali membri della comunità dopo aver valutato se l'istituzione, l'organo o l'organismo dell'Unione soddisfa i criteri di cui al paragrafo 3 del presente articolo. Tali registrazioni non sono limitate nel tempo, ma possono essere revocate in qualsiasi momento dal Centro di competenza se quest'ultimo ritiene che l'istituzione, l'organo o l'organismo dell'Unione non soddisfi più i criteri di cui al paragrafo 3 del presente articolo o rientri nell'articolo 136 del regolamento finanziario.

7. I rappresentanti delle istituzioni, degli organi e degli organismi dell'Unione possono partecipare ai lavori della comunità.

8. Un ente registrato come membro della comunità designa i suoi rappresentanti per garantire un dialogo efficiente. Tali rappresentanti possiedono competenze in materia di cibersicurezza nell'ambito della ricerca, della tecnologia o dell'industria. I requisiti possono essere ulteriormente precisati dal consiglio di direzione, senza limitare indebitamente gli enti nella designazione dei loro rappresentanti.

9. La comunità fornisce al direttore esecutivo e al consiglio di direzione, tramite i suoi gruppi di lavoro e in particolare tramite il gruppo consultivo strategico, consulenza strategica sull'agenda e sul programma di lavoro annuale e pluriennale, conformemente al regolamento interno del consiglio di direzione.

Articolo 9

Compiti dei membri della comunità

I membri della comunità:

a) assistono il Centro di competenza nell'assolvimento della sua missione e nel conseguimento dei suoi obiettivi e, a tal fine, operano a stretto contatto con il Centro di competenza e i centri nazionali di coordinamento;

b) se del caso, partecipano ad attività formali o informali e ai gruppi di lavoro di cui all'articolo 13, paragrafo 3, lettera n), per svolgere attività specifiche previste dal programma di lavoro annuale; e

c) se del caso, assistono il Centro di competenza e i centri nazionali di coordinamento nella promozione di progetti specifici;

Articolo 10

Cooperazione del Centro di competenza con altre istituzioni, organi e organismi dell'Unione e organizzazioni internazionali

1. Al fine di garantire coerenza e complementarità, evitando duplicazioni degli sforzi, il Centro di competenza coopera con istituzioni, organi e organismi pertinenti dell'Unione, tra cui l'ENISA, il servizio europeo per l'azione esterna, la direzione generale del Centro comune di ricerca della Commissione, l'Agenzia europea esecutiva per la ricerca, l'Agenzia esecutiva per l'innovazione, l'Agenzia esecutiva del Consiglio europeo della ricerca e l'Agenzia esecutiva europea per la salute e il digitale istituite dalla decisione di esecuzione (UE) 2021/173 della Commissione ([13]), i pertinenti poli europei dell'innovazione digitale, il Centro europeo per la lotta alla criminalità informatica presso l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto istituita dal regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio ([14]), l'Agenzia europea per la difesa in relazione ai compiti di cui all'articolo 5 del presente regolamento e altri soggetti pertinenti dell'Unione. Il Centro di competenza può anche cooperare con organizzazioni internazionali, se del caso.

2. La cooperazione di cui al paragrafo 1 del presente articolo può svolgersi nel quadro di accordi di lavoro. Detti accordi vengono sottoposti all'approvazione del consiglio di direzione. La condivisione di informazioni classificate avviene nel quadro di intese amministrative concluse a norma dell'articolo 36, paragrafo 3.

CAPO II

ORGANIZZAZIONE DEL CENTRO DI COMPETENZA

Articolo 11

Membri e struttura

1. I membri del Centro di competenza sono l'Unione, rappresentata dalla Commissione, e gli Stati membri.

2. La struttura del Centro di competenza assicura il conseguimento degli obiettivi di cui all'articolo 4 e l'esecuzione dei compiti di cui all'articolo 5 e comprende:

a) un consiglio di direzione;

([13]) Decisione di esecuzione (UE) 2021/173 della Commissione, del 12 febbraio 2021, che istituisce l'Agenzia esecutiva europea per il clima, le infrastrutture e l'ambiente, l'Agenzia esecutiva europea per la salute e il digitale, l'Agenzia esecutiva per la ricerca europea, il Consiglio europeo per l'innovazione e il dirigente per le PMI Agenzia, l'Agenzia esecutiva del Consiglio europeo della ricerca e l'Agenzia esecutiva europea per l'istruzione e la cultura e che abroga le decisioni di esecuzione 2013/801/UE, 2013/771/UE, 2013/778/UE, 2013/779/UE, 2013/776/UE e 2013/770/UE (GU L 50 del 15.2.2021 pag. 9).

([14]) Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI (GU L 135 del 24.5.2016, pag. 53).

b) un direttore esecutivo;

c) un gruppo consultivo.

SEZIONE I

Consiglio di direzione

Articolo 12

Composizione del consiglio di direzione

1. Il consiglio di direzione è composto di un rappresentante per ciascuno Stato membro e di due rappresentanti della Commissione, a nome dell'Unione.

2. Ciascun membro del consiglio di direzione ha un supplente. Tale supplente rappresenta il membro in sua assenza.

3. I membri del consiglio di direzione nominati dagli Stati membri e i loro supplenti sono dipendenti del settore pubblico dei rispettivi Stati membri e sono selezionati in base alle loro conoscenze in materia di cibersicurezza nell'ambito della ricerca, della tecnologia e dell'industria, alla loro capacità di provvedere al coordinamento di azioni e posizioni con il rispettivo centro nazionale di coordinamento o alle loro pertinenti competenze gestionali, amministrative e di bilancio. La Commissione nomina i suoi membri in base alle loro conoscenze nel settore della cibersicurezza e in ambito tecnologico o alle loro pertinenti competenze gestionali, amministrative e di bilancio, e alla loro capacità di assicurare il coordinamento, le sinergie e, per quanto possibile, la realizzazione di iniziative congiunte tra diverse politiche dell'Unione settoriali e orizzontali che attengono alla cibersicurezza. La Commissione e gli Stati membri si sforzano di limitare l'avvicendamento dei loro rappresentanti nel consiglio di direzione, al fine di assicurare la continuità dei lavori di quest'ultimo. La Commissione e gli Stati membri mirano a conseguire una rappresentanza equilibrata tra uomini e donne nel consiglio di direzione.

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

5. I membri del consiglio di direzione provvedono affinché la missione, gli obiettivi, l'identità e del Centro di competenza siano salvaguardate e che le sue azioni siano coerenti con tali missione e obiettivi, in modo indipendente e trasparente.

6. Il consiglio di direzione può invitare osservatori a partecipare, ove opportuno, alle sue riunioni, fra cui rappresentanti di istituzioni, organi e organismi pertinenti dell'Unione e membri della comunità.

7. Un rappresentante di ENISA è un osservatore permanente nel consiglio di direzione. Il consiglio di direzione può invitare a partecipare alle sue riunioni un rappresentante del gruppo consultivo strategico.

8. Il direttore esecutivo partecipa alle riunioni del consiglio di direzione ma non ha diritto di voto.

Articolo 13

Compiti del consiglio di direzione

1. Il consiglio di direzione assume la responsabilità generale dell'orientamento strategico e delle operazioni del Centro di competenza, sovrintende all'attuazione delle sue attività ed è responsabile di tutti i compiti non espressamente attribuiti al direttore esecutivo.

2. Il consiglio di direzione adotta il proprio regolamento interno. Tale regolamento prevede procedure specifiche per individuare ed evitare i conflitti di interessi e garantire la riservatezza di tutte le informazioni sensibili.

3. Il consiglio di direzione adotta le decisioni strategiche necessarie, in particolare riguardo a:

a) lo sviluppo e l'adozione dell'agenda e il monitoraggio della sua attuazione;

b) rispecchiando le priorità di intervento dell'Unione e l'agenda, l'adozione del programma di lavoro pluriennale contenente priorità strategiche comuni, industriali, tecnologiche e di ricerca, basate sulle esigenze individuate dagli Stati membri in cooperazione con la comunità e su cui occorre concentrare il sostegno finanziario dell'Unione, inclusi le tecnologie e i settori chiave per lo sviluppo delle capacità proprie dell'Unione in materia di cibersicurezza;

c) l'adozione del programma di lavoro annuale per l'esecuzione dei pertinenti fondi dell'Unione, in particolare le parti relative alla cibersicurezza di Orizzonte Europa, nella misura in cui siano cofinanziate su base volontaria dagli Stati membri, e del programma Europa digitale, in conformità del programma di lavoro pluriennale del Centro di competenza e del processo di pianificazione strategica di Orizzonte Europa;

d) l'adozione dei conti e del bilancio annuali, nonché della relazione annuale di attività del Centro di competenza, sulla base di una proposta del direttore esecutivo;

e) l'adozione delle regole finanziarie specifiche del Centro di competenza, conformemente all'articolo 70 del regolamento finanziario;

f) nell'ambito del programma di lavoro annuale, la destinazione dei fondi del bilancio dell'Unione a temi delle azioni congiunte tra l'Unione e gli Stati membri;

g) nell'ambito del programma di lavoro annuale e in conformità delle decisioni di cui alla lettera f) del presente comma, e in conformità dei regolamenti (UE) 2021/… (+) e (UE) 2021/… (++), la descrizione delle azioni congiunte di cui alla lettera f) del presente comma e la definizione delle condizioni per la loro attuazione;

h) l'adozione di una procedura di nomina del direttore esecutivo e la nomina del direttore esecutivo, la revoca e proroga del mandato, la definizione di orientamenti e il controllo dell'operato del direttore esecutivo;

i) l'adozione di orientamenti per la valutazione e la registrazione degli enti in qualità di membri della comunità;

j) l'adozione degli accordi di lavoro di cui all'articolo 10, paragrafo 2;

k) la nomina del contabile;

l) l'adozione del bilancio annuale del Centro di competenza, compresa la tabella dell'organico con l'indicazione del numero di posti temporanei per gruppo di funzioni e per grado e del numero di agenti contrattuali e di esperti nazionali distaccati espressi in equivalenti a tempo pieno;

m) l'adozione di norme di trasparenza per il Centro di competenza e norme per la prevenzione e la gestione dei conflitti di interessi, anche in relazione ai membri del consiglio di direzione, conformemente all'articolo 42 del regolamento delegato (UE) 2019/715 della Commissione;

n) l'istituzione gruppi di lavoro all'interno della comunità, se del caso tenendo conto della consulenza fornita dal gruppo consultivo strategico;

o) la nomina membri del gruppo consultivo strategico;

p) l'adozione di norme sul rimborso spese per i membri del gruppo consultivo strategico;

q) l'istituzione di un meccanismo di controllo per garantire che l'esecuzione dei rispettivi fondi gestiti dal Centro di competenza sia effettuata conformemente all'agenda, alla missione, al programma di lavoro pluriennale e alle norme dei programmi da cui provengono i finanziamenti pertinenti;

r) la garanzia di un dialogo regolare e l'instaurazione di un efficace meccanismo di cooperazione con la comunità;

s) la definizione della strategia di comunicazione del Centro di competenza, in base a una raccomandazione del direttore esecutivo;

t) se del caso, l'adozione delle modalità di applicazione dello Statuto dei funzionari e del regime applicabile agli altri agenti dell'Unione europea di cui al regolamento (CEE, Euratom, CECA) n. 259/68 del Consiglio ([15]) («statuto dei funzionari» e «regime applicabile agli altri agenti») conformemente all'articolo 30, paragrafo 3, del presente regolamento;

u) se del caso, l'adozione delle regole per il distacco di esperti nazionali presso il Centro di competenza e per il ricorso a tirocinanti conformemente all'articolo 31, paragrafo 2;

v) l'adozione delle norme di sicurezza per il Centro di competenza;

w) l'adozione di una strategia antifrode e anticorruzione proporzionata ai rischi di frode e di corruzione e adotta misure globali, conformemente alla legislazione dell'Unione applicabile, per la protezione delle persone che segnalano violazioni del diritto dell'Unione, tenendo conto di un'analisi costi-benefici delle misure da attuare;

x) se necessario, l'adozione della metodologia per il calcolo del contributo finanziario volontario e in natura degli Stati membri contributori in conformità dei regolamenti (UE) 2021/… (+) e (UE) 2021/… (++) o di altra legislazione applicabile;

(+) Regolamento di cui al documento ST 7064/20.
(++) Regolamento di cui al documento ST 6789/20.
([15]) GU L 56 del 4.3.1968, pag.1.

y) nel contesto del programma di lavoro annuale e del programma di lavoro pluriennale, la garanzia della coerenza e delle sinergie con le parti del programma Europa digitale e di Orizzonte Europa che non sono gestite dal Centro di competenza, come pure con altri programmi dell'Unione;

z) l'adozione della relazione annuale sull'attuazione delle priorità e degli obiettivi strategici del Centro di competenza fornendo, se necessario, una raccomandazione per una migliore realizzazione di tali priorità e obiettivi.

Nella misura in cui il programma di lavoro annuale contiene azioni comuni, contiene informazioni sui contributi volontari degli Stati membri alle azioni comuni. Se del caso, le proposte, in particolare la proposta di programma di lavoro annuale, valutano la necessità di applicare norme di sicurezza di cui all'articolo 33 del presente regolamento, compresa la procedura di autovalutazione della sicurezza ai sensi dell'articolo 20 del regolamento (UE) 2021/… (+)

4. Per quanto riguarda le decisioni di cui al paragrafo 3, lettere a), b) e c), il direttore esecutivo e il consiglio di direzione tengono conto di ogni pertinente consulenza strategica e contributo forniti dall'ENISA conformemente al regolamento interno stabilito dal consiglio di direzione.

5. Il consiglio di direzione è responsabile di provvedere affinché alle raccomandazioni di cui alla relazione sull'attuazione e la valutazione di cui all'articolo 38, paragrafi 2 e 4, sia dato adeguato seguito.

Articolo 14

Presidente e riunioni del consiglio di direzione

1. Il consiglio di direzione elegge un presidente e un vicepresidente tra i suoi membri per un periodo di tre anni. Il mandato del presidente e del vicepresidente può essere prorogato una sola volta con decisione del consiglio di direzione. Tuttavia, qualora il presidente o il vicepresidente cessino di far parte del consiglio di direzione in un qualsiasi momento in corso di mandato, questo giunge automaticamente a termine alla stessa data. Il vicepresidente sostituisce d'ufficio il presidente nel caso in cui quest'ultimo non sia in grado di svolgere i propri compiti. Il presidente partecipa al voto.

2. Il consiglio di direzione tiene riunioni ordinarie almeno tre volte all'anno. Può convocare riunioni straordinarie su richiesta della Commissione, su richiesta di un terzo di tutti i suoi membri oppure su richiesta del presidente o del direttore esecutivo nell'esercizio delle sue funzioni.

3. Il direttore esecutivo partecipa alle deliberazioni, salvo diversa decisione del consiglio di direzione, ma non ha diritto di voto.

4. Il consiglio di direzione può invitare, sulla base di una valutazione caso per caso, altre persone ad assistere alle proprie riunioni in veste di osservatori.

5. Il presidente può invitare rappresentanti della comunità a partecipare senza diritto di voto alle riunioni del consiglio di direzione.

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

7. Il Centro di competenza provvede alle funzioni di segretariato del consiglio di direzione.

Articolo 15

Regole di voto del consiglio di direzione

1. Il consiglio di direzione adotta un approccio consensuale nelle sue discussioni. Si procede a una votazione se i membri del consiglio di direzione non raggiugono il consenso.

2. Se il consiglio di direzione non raggiunge il consenso su di una questione, delibera a maggioranza di almeno il 75 % dei voti di tutti i suoi membri; a tal fine i rappresentanti della Commissione sono considerati un solo membro. Un membro assente del consiglio di direzione può delegare il suo diritto di voto al suo supplente o, in assenza di quest'ultimo, a un altro membro. Nessun membro del consiglio di direzione può rappresentare più di un altro membro.

3. Le decisioni del consiglio di direzione relative alle azioni congiunte e alla loro gestione, di cui all'articolo 13, paragrafo 3, lettere f) e g), sono adottate come segue:

a) le decisioni di cui all'articolo 13, paragrafo 3, lettera f), volte a destinare i fondi del bilancio dell'Unione ad azioni congiunte e le decisioni volte a includere tali azioni congiunte nel programma di lavoro annuale, sono adottate conformemente alle norme di cui al paragrafo 2 del presente articolo;

(+) Regolamento di cui al documento ST 7064/20.

b) le decisioni, di cui all'articolo 13, paragrafo 3, lettera g), relative alla descrizione delle azioni congiunte e che stabiliscono condizioni per la loro attuazione sono adottate dagli Stati membri partecipanti e dalla Commissione, e i diritti di voto dei membri sono proporzionali al rispettivo contributo alla specifica azione congiunta, calcolato conformemente alla metodologia adottata ai sensi dell'articolo 13, paragrafo 3, lettera x).

4. Per le decisioni adottate a norma dell'articolo 13, paragrafo 3, lettere b), c), d), e), f), k), l), p), q), t), u), w), x) e y), la Commissione detiene il 26 % del totale dei voti in seno al comitato di direzione.

5. Per decisioni diverse da quelle indicate al paragrafo 3, lettera b), e al paragrafo 4, ciascuno Stato membro e l'Unione dispongono di un voto. Il voto dell'Unione è espresso congiuntamente dai due rappresentanti della Commissione.

6. Il presidente partecipa al voto.

SEZIONE II

Direttore esecutivo

Articolo 16

Nomina, revoca e proroga del mandato del direttore esecutivo

1. Il direttore esecutivo è una persona in possesso di un'esperienza specifica e che gode di una solida reputazione nei settori in cui opera il Centro di competenza.

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

3. Il consiglio di direzione nomina il direttore esecutivo scegliendolo da una rosa di candidati proposta dalla Commissione, in esito a una procedura di selezione aperta, trasparente e non discriminatoria.

4. Ai fini della conclusione del contratto del direttore esecutivo, il Centro di competenza è rappresentato dal presidente del consiglio di direzione.

5. La durata del mandato del direttore esecutivo è di quattro anni. Prima della fine di tale periodo, la Commissione esegue una valutazione che tiene conto della prestazione del direttore esecutivo e dei compiti e delle sfide futuri del Centro di competenza.

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

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

8. Il direttore esecutivo è rimosso dall'incarico solo su decisione del consiglio di direzione, che agisce su proposta della Commissione o di almeno il 50 % degli Stati membri.

Articolo 17

Compiti del direttore esecutivo

1. Il direttore esecutivo è incaricato delle operazioni e della gestione quotidiana del Centro di competenza, di cui è il rappresentante legale. Il direttore esecutivo è responsabile dinanzi al consiglio di direzione e svolge i propri compiti in assoluta indipendenza nell'ambito delle proprie competenze. Il direttore esecutivo è assistito dal personale del Centro di competenza.

2. Il direttore esecutivo svolge, tra gli altri, i compiti seguenti, in modo indipendente:

a) attua le decisioni adottate dal consiglio di direzione;

b) assiste il consiglio di direzione nel suo lavoro, provvede al segretariato per le sue riunioni e fornisce tutte le informazioni necessarie per l'esercizio delle sue funzioni;

c) dopo essersi consultato con il consiglio di direzione e con la Commissione, tenendo conto del contributo dei centri nazionali di coordinamento e della comunità, prepara l'agenda e, conformemente ad essa, il progetto di programma di lavoro pluriennale e il progetto di programma di lavoro annuale del Centro di competenza e li presenta per adozione al consiglio di direzione, specificando l'oggetto degli inviti a presentare proposte, degli inviti a manifestare interesse e delle gare d'appalto necessari per attuare il programma di lavoro annuale e le corrispondenti previsioni di spesa proposte dagli Stati membri e dalla Commissione;

d) prepara il progetto di bilancio annuale, compresa la corrispondente tabella dell'organico di cui all'articolo 13, paragrafo 3, lettera l), con l'indicazione del numero di posti temporanei per gruppo di funzioni e per grado, nonché del numero di agenti contrattuali e di esperti nazionali distaccati espressi in equivalenti a tempo pieno, e lo presenta per adozione al consiglio di direzione;

e) attua il programma di lavoro annuale e il programma di lavoro pluriennale e riferisce al consiglio di direzione in merito;

f) prepara il progetto di relazione annuale di attività del Centro di competenza, comprensivo delle informazioni sulle spese relative e sull'attuazione dell'agenda e del programma di lavoro pluriennale; se necessario, tale relazione è corredata di proposte per l'ulteriore miglioramento della realizzazione o per la riformulazione delle priorità e degli obiettivi strategici;

g) garantisce l'attuazione di procedure efficaci di monitoraggio e valutazione delle prestazioni del Centro di competenza;

h) predispone un piano d'azione per dare seguito alle conclusioni della relazione sull'attuazione e della valutazione di cui all'articolo 38, paragrafi 2 e 4, e, ogni due anni, presenta al Parlamento europeo e alla Commissione relazioni sui progressi compiuti;

i) prepara e conclude accordi con i centri nazionali di coordinamento;

j) è incaricato delle questioni amministrative, finanziarie e del personale, compresa l'esecuzione del bilancio del Centro di competenza, tenendo in debito conto i pareri ricevuti dalla pertinente funzione di audit interno, conformemente alle decisioni di cui all'articolo 13, paragrafo 3, lettere e), l), t), u), v) e w);

k) approva e gestisce la pubblicazione degli inviti a presentare proposte, conformemente al programma di lavoro annuale, e gestisce le risultanti convenzioni e le decisioni di sovvenzione;

l) approva l'elenco delle azioni selezionate per il finanziamento sulla base di una graduatoria stilata da un gruppo di esperti indipendenti;

m) approva e gestisce la pubblicazione dei bandi di gare d'appalto, conformemente al programma di lavoro annuale e gestisce i contratti risultanti;

n) approva le offerte selezionate ai fini del finanziamento;

o) sottopone il progetto di conti e di bilancio annuali alla pertinente funzione di audit interno e, successivamente, al consiglio di direzione;

p) assicura lo svolgimento delle attività di valutazione e gestione dei rischi;

q) firma le singole convenzioni e decisioni di sovvenzione e i singoli contratti di sovvenzione;

r) firma i contratti di appalto;

s) predispone un piano d'azione per dare seguito alle conclusioni delle relazioni di audit interni ed esterni e alle indagini dell'Ufficio europeo per la lotta antifrode (OLAF), istituito dalla decisione 1999/352/CE, CECA, Euratom della Commissione ([16]) e riferisce sui progressi compiuti due volte l'anno alla Commissione e periodicamente al consiglio di direzione;

t) predispone il progetto di regole finanziarie applicabili al Centro di competenza;

u) istituisce un sistema di controllo interno efficace ed efficiente e ne assicura il funzionamento; riferisce al consiglio di direzione ogni modifica sostanziale dello stesso;

v) assicura un'efficace comunicazione con le istituzioni dell'Unione e riferisce, qualora invitato, al Parlamento europeo e al Consiglio;

w) adotta ogni altro provvedimento necessario per valutare l'assolvimento della propria missione e il conseguimento dei propri obiettivi;

x) svolge qualsiasi altro compito affidatogli o delegatogli dal consiglio di direzione.

([16]) Decisione 1999/352/CE, CECA, Euratom della Commissione, del 28 aprile 1999, che istituisce l'Ufficio europeo per la lotta antifrode (OLAF) (GU L 136 del 31.5.1999, pag. 20).

SEZIONE III

Gruppo consultivo strategico

Articolo 18

Composizione del gruppo consultivo strategico

1. Il gruppo consultivo strategico è composto di un massimo di 20 membri. Su proposta del direttore esecutivo, il consiglio di direzione nomina i membri tra i rappresentanti dei membri della comunità, diversi dai rappresentanti delle istituzioni, degli organi e degli organismi dell'Unione. Sono ammissibili soltanto i rappresentanti di membri non controllati da un paese terzo o da un soggetto stabilito in un paese terzo. La nomina avviene in conformità di una procedura aperta, trasparente e non discriminatoria. Il consiglio di direzione mira, nella composizione del gruppo consultivo strategico, a conseguire una rappresentanza equilibrata della comunità tra enti scientifici, industriali e della società civile, le industrie sul versante della domanda e dell'offerta, le grandi imprese e le PMI, anche in termini sia di provenienza geografica e genere. Mira altresì a conseguire un equilibrio intrasettoriale, tenuto conto della coesione dell'Unione e di tutti gli Stati membri in materia di cibersicurezza nell'ambito della ricerca, dell'industria e della tecnologia. Il gruppo consultivo strategico mira è composto in modo tale da consentire un dialogo globale, costante e permanente tra la comunità e il Centro di competenza.

2. I membri del gruppo consultivo strategico possiedono competenze nella ricerca in materia di cibersicurezza, nello sviluppo industriale, nell'offerta, nella realizzazione o nell'impiego di servizi o prodotti professionali. I requisiti inerenti a tali competenze sono ulteriormente precisati dal consiglio di direzione.

3. Le procedure relative alla nomina dei membri del gruppo consultivo strategico e al suo funzionamento sono specificate nel regolamento interno del consiglio di direzione e sono rese pubbliche.

4. La durata del mandato dei membri del gruppo consultivo strategico è di due anni. Il mandato è rinnovabile una volta.

5. Il gruppo consultivo strategico può invitare rappresentanti della Commissione e di altre istituzioni, organi e organismi dell'Unione, in particolare dell'ENISA, a partecipare ai propri lavori e a fornirvi supporto. Il gruppo consultivo strategico può invitare altri rappresentanti della comunità in qualità di osservatori, consulenti o esperti, ove opportuno, con discrezionalità caso per caso, al fine di tenere conto della dinamica degli sviluppi nel settore della cibersicurezza. I membri del consiglio di direzione possono partecipare alle riunioni del gruppo consultivo strategico in qualità di osservatori.

Articolo 19

Funzionamento del gruppo consultivo strategico

1. Il gruppo consultivo strategico si riunisce almeno tre volte l'anno.

2. Il gruppo consultivo strategico fornisce consulenza al consiglio di direzione in merito all'istituzione di gruppi di lavoro all'interno della comunità ai sensi dell'articolo 13, paragrafo 3, lettera n), su questioni specifiche inerenti all'attività del Centro di competenza ogniqualvolta tali questioni si riferiscano direttamente ai compiti e gli ambiti di competenza di cui all'articolo 20. Ove necessario, tali gruppi di lavoro sono soggetti al con coordinamento generale di uno o più membri del gruppo consultivo strategico.

3. Il gruppo consultivo strategico elegge il proprio presidente a maggioranza semplice dei suoi membri.

4. Le funzioni di segretariato del gruppo consultivo strategico sono svolte dal direttore esecutivo e dal personale del Centro di competenza, usando risorse esistenti, tenendo in debita considerazione il carico di lavoro complessivo del Centro di competenza. Le risorse destinate al sostegno del gruppo consultivo strategico sono riportate nel progetto di bilancio annuale.

5. Il gruppo consultivo strategico adotta il proprio regolamento interno a maggioranza semplice dei suoi membri.

Articolo 20

Compiti del gruppo consultivo strategico

Il gruppo consultivo strategico fornisce regolarmente consulenza al Centro di competenza relativamente allo svolgimento delle sue attività, si occupa della comunicazione con la comunità e altri portatori di interessi pertinenti. Il gruppo consultivo strategico inoltre:

a) tenuto conto dei contributi della comunità e dei gruppi di lavoro di cui all'articolo 13, paragrafo 3, lettera i), ove opportuno, fornisce al direttore esecutivo e al consiglio di direzione consulenza strategica e il proprio contributo, con aggiornamenti costanti, in merito all'agenda, ai programmi di lavoro annuale e pluriennale, entro i termini fissati dal consiglio di direzione;

b) fornisce consulenza al consiglio di direzione in merito all'istituzione di gruppi di lavoro all'interno della comunità ai sensi dell'articolo 13, paragrafo 3, lettera n), su questioni specifiche inerenti all'attività del Centro di competenza;

c) previa approvazione del consiglio di direzione, dispone e organizza consultazioni pubbliche aperte a tutti i portatori di interessi pubblici e privati del settore della cibersicurezza, al fine di raccogliere indicazioni per la consulenza strategica di cui alla lettera a).

CAPO III

DISPOSIZIONI FINANZIARIE

Articolo 21

Contributi finanziari dell'Unione e degli Stati membri

1. Il Centro di competenza è finanziato dall'Unione mentre le azioni congiunte sono finanziate dall'Unione e da contributi volontari degli Stati membri.

2. Le spese amministrative e di funzionamento delle azioni congiunte sono coperte dall'Unione e dagli Stati membri che contribuiscono a dette azioni, in conformità dei regolamenti (UE) 2021/… ([+]) e (UE) 2021/… ([++]).

3. Il contributo dell'Unione al Centro di competenza a copertura delle spese amministrative e di funzionamento comprende:

a) fino a 1 649 566 000 EUR provenienti dal Programma Europa digitale, di cui fino a 32 000 000 EUR per le spese amministrative;

b) un importo proveniente da Orizzonte Europa, anche a copertura delle spese amministrative, per le azioni congiunte, pari all'importo del contributo degli Stati membri a norma del paragrafo 7 del presente articolo, ma non superiore all'importo determinato nel quadro del processo di pianificazione strategica di Orizzonte Europa da svolgersi in conformità dell'articolo 6, paragrafo 6, del regolamento (UE) 2021/… ([+]), del programma di lavoro pluriennale o del programma di lavoro annuale.

c) un importo proveniente dagli altri pertinenti programmi dell'Unione, nella misura necessaria all'esecuzione dei compiti o al raggiungimento degli obiettivi del Centro di competenza, fatte salve le decisioni adottate conformemente ai regolamenti che istituiscono tali programmi.

4. Il contributo massimo dell'Unione è prelevato dagli stanziamenti del bilancio generale dell'Unione assegnati al Programma Europa digitale, al programma specifico di attuazione di Orizzonte Europa, stabilito dalla decisione (UE) 2021/… ([+++]) e ad altri programmi e progetti che rientrano nell'ambito di attività del Centro di competenza o della rete.

5. Il Centro di competenza attua azioni relative alla cibersicurezza del Programma Europa digitale e di Orizzonte Europa a norma dell'articolo 62, paragrafo 1, primo comma, lettera c), punto iv), del regolamento finanziario.

6. I contributi provenienti da programmi dell'Unione diversi da quelli di cui ai paragrafi 3 e 4, che rientrano nel cofinanziamento dell'Unione a favore di un programma attuato da uno degli Stati membri, non sono presi in considerazione nel calcolo del contributo finanziario massimo dell'Unione di cui a tali paragrafi.

7. Gli Stati membri partecipano volontariamente alle azioni congiunte con contributi finanziari e/o in natura su base volontaria. Se uno Stato membro partecipa a un'azione congiunta, il suo contributo finanziario copre le spese amministrative in proporzione al suo contributo all'azione congiunta. Le spese amministrative delle azioni congiunte sono coperte da contributi di natura finanziaria. Le spese di funzionamento delle azioni congiunte possono essere coperte da contributi finanziari o in natura, come previsto da Orizzonte Europa e dal Programma Europa digitale. I contributi di ciascuno Stato membro possono assumere la forma del sostegno che tale Stato membro ha fornito, nell'ambito di un'azione congiunta, a beneficiari dell'azione congiunta stabiliti in tale Stato membro. I contributi in natura degli Stati membri consistono nelle spese ammissibili sostenute dai centri nazionali di coordinamento e da altri enti pubblici quando questi partecipano a progetti finanziati a titolo del presente regolamento, al netto dell'eventuale contributo dell'Unione a copertura di tali spese. Nel caso di progetti finanziati mediante Orizzonte Europa, le spese ammissibili sono calcolate a norma dell'articolo 32 del regolamento (EU) 2021/… ([+]). Nel caso di progetti finanziati mediante il Programma Europa digitale, le spese ammissibili sono calcolate conformemente al regolamento finanziario.

([+]) Regolamento di cui al documento ST 7064/20.
([++]) Regolamento di cui al documento ST 6789/20.
([+++]) Decisione di cui al documento ST 8967/20.

L'importo previsto dei contributi volontari totali degli Stati membri a favore delle azioni congiunte nell'ambito di Orizzonte Europa, compresi i contributi finanziari a copertura delle spese amministrative, è determinato affinché se ne tenga conto nel quadro del processo di pianificazione strategica del programma Orizzonte Europa da svolgersi a norma dell'articolo 6, paragrafo 6, del regolamento (UE) 2021/… (*), con il contributo del consiglio di direzione. Per le azioni nel quadro del Programma Europa digitale, nonostante l'articolo 15 del regolamento (UE) 2021/… (**), gli Stati membri possono contribuire alle spese del Centro di competenza cofinanziate dal Programma Europa digitale in misura inferiore agli importi specificati al paragrafo 3, lettera a), del presente articolo.

8. Il cofinanziamento nazionale da parte degli Stati membri di azioni sostenute da programmi dell'Unione diversi da Orizzonte Europa e dal Programma Europa digitale è considerato un contributo nazionale degli Stati membri nella misura in cui tali contributi sono parte di azioni congiunte e sono inclusi nel programma di lavoro del Centro di competenza.

9. Ai fini della valutazione dei contributi di cui al paragrafo 3 del presente articolo e all'articolo 22, paragrafo 2, lettera b), le spese sono determinate secondo le prassi contabili abitualmente seguite dallo Stato membro interessato, le norme contabili applicabili dallo Stato membro interessato, le norme contabili internazionali e i principi internazionali di informativa finanziaria applicabili. Le spese sono certificate da un revisore esterno indipendente nominato dallo Stato membro interessato. Il metodo di valutazione può essere verificato dal Centro di competenza in caso di dubbi sulla certificazione.

10. Se uno degli Stati membri non adempie ai suoi impegni per quanto riguarda il contributo finanziario o in natura riguardante azioni congiunte, il direttore esecutivo lo notifica per iscritto allo Stato membro in questione e fissa un termine ragionevole entro il quale ovviare all'inadempienza. Se lo Stato membro inadempiente non pone rimedio alla situazione entro il termine stabilito, il direttore esecutivo convoca una riunione del consiglio di direzione per decidere se revocargli il diritto di voto o applicare altre misure fino a quando detto Stato membro non avrà adempiuto ai suoi obblighi. I diritti di voto dello Stato membro inadempiente riguardanti azioni congiunte sono sospesi finché non verrà posto rimedio all'inadempimento degli impegni.

11. La Commissione può annullare, ridurre proporzionalmente o sospendere il contributo finanziario dell'Unione alle azioni congiunte qualora lo Stato membro contributore non fornisca i contributi di cui al paragrafo 3, lettera b), li fornisca solo parzialmente o in ritardo. L'annullamento, la riduzione o la sospensione del contributo finanziario dell'Unione da parte della Commissione è proporzionato, in termini di importo e di tempi, all'inadempienza dello Stato membro nel fornire contributi, alla fornitura parziale o al ritardo della fornitura dei medesimi.

12. Gli Stati membri contributori riferiscono al consiglio di direzione, entro il 31 gennaio di ogni anno, in merito al valore dei contributi di cui al paragrafo 7 per azioni congiunte con l'Unione forniti nel corso dell'esercizio finanziario precedente.

Articolo 22

Spese e risorse del Centro di competenza

1. Le spese amministrative del Centro di competenza sono coperte in linea di principio da contributi finanziari su base annua forniti dall'Unione. Gli Stati membri contributori forniscono contributi finanziari supplementari in proporzione ai loro contributi volontari alle azioni congiunte. Qualora una parte del contributo destinato a coprire le spese amministrative non sia utilizzata, può essere resa disponibile per coprire le spese di funzionamento del Centro di competenza.

2. Le spese di funzionamento del Centro di competenza sono coperte mediante:

a) il contributo finanziario dell'Unione;

b) i contributi volontari, finanziari o in natura, degli Stati membri contributori nel caso di azioni congiunte.

3. Le risorse del Centro di competenza iscritte a bilancio si compongono dei contributi seguenti:

a) contributi finanziari dell'Unione alle spese amministrative e di funzionamento;

b) contributi finanziari volontari degli Stati membri contributori alle spese amministrative nel caso di azioni congiunte;

c) contributi finanziari volontari degli Stati membri contributori alle spese di funzionamento nel caso di azioni congiunte;

(*) Regolamento di cui al documento ST 7064/20.
(**) Regolamento di cui al documento ST 6789/20.

d) eventuali entrate generate dal Centro di competenza;

e) eventuali altri contributi finanziari, risorse o entrate.

4. Gli interessi maturati dai contributi versati al Centro di competenza dagli Stati membri contributori sono considerati una sua entrata.

5. Tutte le risorse del Centro di competenza e le sue attività sono utilizzate per conseguimento dei suoi obiettivi.

6. Il Centro di competenza è proprietario di tutti gli attivi che genera o che gli sono trasferiti ai fini della realizzazione dei suoi obiettivi. Fatte salve le norme applicabili del pertinente programma di finanziamento, la proprietà degli attivi generati o acquisiti in azioni congiunte è decisa in conformità dell'articolo 15, paragrafo 3, lettera b).

7. Le eventuali eccedenze rispetto alle spese rimangono di proprietà del Centro di competenza e non sono ridistribuite ai suoi membri contributori, salvo in caso di liquidazione del Centro di competenza.

8 Il Centro di competenza coopera strettamente con altre istituzioni, organi e organismi dell'Unione, tenendo debitamente conto dei rispettivi mandati ed evitando duplicazioni di meccanismi di cooperazione esistenti, per trarre beneficio delle sinergie e, ove del caso, ridurre le spese amministrative.

Articolo 23

Impegni finanziari

Gli impegni finanziari del Centro di competenza non superano l'importo delle risorse finanziarie disponibili o iscritte a bilancio dai suoi membri.

Articolo 24

Esercizio finanziario

L'esercizio finanziario ha inizio il 1º gennaio e si chiude il 31 dicembre.

Articolo 25

Formazione del bilancio

1. Ogni anno il direttore esecutivo redige un progetto di stato di previsione delle entrate e delle spese del Centro di competenza per l'esercizio finanziario successivo e lo trasmette al consiglio di direzione, corredato di un progetto di tabella dell'organico di cui all'articolo 13, paragrafo 3, lettera l). Le entrate e le spese risultano in pareggio. Le spese del Centro di competenza comprendono le spese per il personale, amministrative, per le infrastrutture e di funzionamento. Le spese amministrative sono ridotte al minimo, anche mediante riassegnazione di personale o di posti.

2. Ogni anno il consiglio di direzione 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 del Centro di competenza per l'esercizio finanziario successivo.

3. Entro il 31 gennaio di ogni anno il consiglio di direzione invia alla Commissione lo stato di previsione di cui al paragrafo 2 del presente articolo, che forma parte integrante del progetto di documento unico di programmazione di cui all'articolo 32, paragrafo 1, del regolamento delegato (UE) 2019/715 della Commissione.

4. Sulla base dello stato di previsione, di cui al paragrafo 2 del presente articolo, la Commissione iscrive le stime che ritiene necessarie per quanto concerne la tabella dell'organico, di cui all'articolo 13, paragrafo 3, lettera l), del presente regolamento, 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 agli articoli 313 e 314 del trattato sul funzionamento dell'Unione europea (TFUE).

5. Il Parlamento europeo e il Consiglio autorizzano gli stanziamenti a titolo del contributo destinato al Centro di competenza.

6. Il Parlamento europeo e il Consiglio adottano la tabella dell'organico di cui all'articolo 13, paragrafo 3, lettera l).

7. Insieme al programma di lavoro annuale e al programma di lavoro pluriennale, il consiglio di direzione adotta il bilancio del Centro di competenza. Esso diventa definitivo dopo l'adozione definitiva del bilancio generale dell'Unione. Se del caso, il consiglio di direzione modifica il bilancio e il programma di lavoro annuale del Centro di competenza per conformarli al bilancio generale dell'Unione.

Articolo 26

Presentazione dei conti del Centro di competenza e discarico

La presentazione dei conti provvisori e definitivi del Centro di competenza e il discarico sono conformi alle regole e al calendario del regolamento finanziario e delle regole finanziarie del Centro di competenza.

Articolo 27

Rendicontazione operativa e finanziaria

1. Il direttore esecutivo riferisce annualmente al consiglio di direzione in merito all'esecuzione dei suoi compiti conformemente alle regole finanziarie del Centro di competenza.

2. Entro due mesi dalla fine di ciascun esercizio finanziario, il direttore esecutivo sottopone all'approvazione del consiglio di direzione una relazione annuale di attività sui progressi compiuti dal Centro di competenza nell'anno civile precedente, in particolare in riferimento al programma di lavoro annuale relativo a quell'anno e al conseguimento delle sue priorità e dei suoi obiettivi strategici. Tale relazione include informazioni sugli aspetti seguenti:

a) le azioni operative svolte e le spese corrispondenti;

b) le azioni presentate, suddivise per tipologia di partecipanti, comprese le PMI, e per Stato membro;

c) le azioni selezionate per il finanziamento, suddivise per tipologia di partecipanti, comprese le PMI, e per Stato membro, con l'indicazione del contributo erogato dal Centro di competenza ai singoli partecipanti e alle singole azioni;

d) l'assolvimento della missione e il conseguimento degli obiettivi di cui al presente regolamento, nonché le proposte di ulteriori iniziative necessarie per assolvere tale missione e conseguire tali obiettivi;

e) la coerenza dei compiti di esecuzione con l'agenda e al programma di lavoro pluriennale.

3. Una volta approvata dal consiglio di direzione, la relazione annuale di attività è resa pubblica.

Articolo 28

Regole finanziarie

Il Centro di competenza adotta le proprie regole finanziarie specifiche a norma dell'articolo 70 del regolamento finanziario.

Articolo 29

Tutela degli interessi finanziari dell'Unione

1. Il Centro di competenza adotta provvedimenti opportuni volti a garantire che, nella realizzazione delle azioni finanziate ai sensi del presente regolamento, gli interessi finanziari dell'Unione siano tutelati mediante l'applicazione di misure preventive contro la frode, la corruzione e ogni altra attività illecita, mediante controlli regolari ed efficaci e, ove fossero rilevate irregolarità, mediante il recupero delle somme indebitamente versate e, se del caso, sanzioni amministrative effettive, proporzionate e dissuasive.

2. Il Centro di competenza accorda al personale della Commissione e alle altre persone da essa autorizzate, nonché alla Corte dei conti, l'accesso ai siti e locali del Centro di competenza, nonché a tutte le informazioni, anche in formato elettronico, necessarie per effettuare i controlli.

3. L'OLAF può effettuare indagini, inclusi controlli e verifiche sul posto, conformemente alle disposizioni e alle procedure di cui al regolamento (Euratom, CE) n. 2185/96 del Consiglio ([17]) e al regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio ([18]), per accertare eventuali frodi, casi di corruzione o altre attività illecite lesive degli interessi finanziari dell'Unione in relazione a convenzioni di sovvenzione o a contratti finanziati, direttamente o indirettamente, conformemente al presente regolamento.

([17]) 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).

([18]) 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).

4. Fatti salvi i paragrafi 1, 2 e 3, i contratti e le convenzioni di sovvenzione derivanti dall'attuazione del presente regolamento contengono disposizioni che autorizzano esplicitamente la Commissione, il Centro di competenza, la Corte dei conti e l'OLAF a procedere a tali controlli e indagini secondo le loro rispettive competenze. Qualora l'attuazione di un'azione sia esternalizzata o sottodelegata, in tutto o in parte, o richieda l'aggiudicazione di un appalto o la concessione di un sostegno finanziario a terzi, il contratto o la convenzione di sovvenzione includono l'obbligo per il contraente o il beneficiario di imporre a eventuali terze parti interessate l'accettazione esplicita di questi poteri della Commissione, del Centro di competenza, della Corte dei conti e dell'OLAF.

CAPO IV

PERSONALE DEL CENTRO DI COMPETENZA

Articolo 30

Personale

1. Al personale del Centro di competenza si applicano lo statuto dei funzionari e il regime applicabile agli altri agenti e le norme adottate di comune accordo dalle istituzioni dell'Unione per l'applicazione dello statuto dei funzionari e del regime applicabile agli altri agenti.

2. Il consiglio di direzione esercita, nei confronti del personale del Centro di competenza, i poteri conferiti dallo statuto dei funzionari all'autorità che ha il potere di nomina e i poteri conferiti dal regime applicabile agli altri agenti all'autorità abilitata a stipulare contratti («poteri dell'autorità che ha il potere di nomina»).

3. Il consiglio di direzione adotta, a norma 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 pertinenti poteri dell'autorità che ha il potere di nomina e definisce le condizioni di sospensione di tale delega. Il direttore esecutivo è autorizzato a sottodelegare tali poteri.

4. Se circostanze eccezionali lo richiedono, il consiglio di direzione può, mediante una decisione, sospendere temporaneamente i poteri dell'autorità che ha il potere di nomina delegati al direttore esecutivo, nonché qualsiasi potere sottodelegato da quest'ultimo. In tal caso il consiglio di direzione esercita i poteri dell'autorità che ha il potere di nomina o li delega a uno dei suoi membri o a un membro del personale del Centro di competenza che non sia il direttore esecutivo.

5. Il consiglio di direzione adotta modalità per garantire l'attuazione dello statuto dei funzionari e del regime applicabile agli altri agenti conformemente all'articolo 110 dello statuto dei funzionari.

6. Il numero degli effettivi è stabilito nella tabella dell'organico di cui all'articolo 13, paragrafo 3, lettera l), che indica il numero di posti temporanei per gruppo di funzioni e per grado e il numero di agenti contrattuali espresso in equivalenti a tempo pieno, in linea con il bilancio annuale del Centro di competenza.

7. Il fabbisogno di risorse umane del Centro di competenza è coperto in primis mediante riassegnazione di personale o di posti delle istituzioni, degli organi e degli organismi dell'Unione europea e mediante l'assunzione di risorse umane aggiuntive. Il personale del Centro di competenza può essere costituito da agenti temporanei e contrattuali.

8. Tutte le spese relative al personale sono a carico del Centro di competenza.

Articolo 31

Esperti nazionali distaccati e altro personale

1. Il Centro di competenza può avvalersi di esperti nazionali distaccati o di altro personale non alle sue dipendenze.

2. D'intesa con la Commissione, il consiglio di direzione adotta una decisione che stabilisce le disposizioni applicabili al distacco di esperti nazionali presso il Centro di competenza.

Articolo 32

Privilegi e immunità

Al Centro di competenza e al suo personale si applica il protocollo n. 7 sui privilegi e sulle immunità dell'Unione europea, allegato al TFUE.

CAPO V

DISPOSIZIONI COMUNI

Articolo 33

Norme di sicurezza

1. Alla partecipazione a tutte le azioni finanziate dal Centro di competenza si applicano le disposizioni dell'articolo 12 del regolamento (UE) 2021/… (+).

2. Le norme di sicurezza specifiche seguenti si applicano ad azioni finanziate da Orizzonte Europa:

a) ai fini dell'articolo 38, paragrafo 1, del regolamento (UE) 2021/… (++), qualora il programma di lavoro annuale lo preveda, è possibile limitare la concessione di licenze non esclusive a terzi stabiliti o considerati stabiliti in uno Stato membro e controllati da tale Stato membro o cittadini di tale Stato membro;

b) ai fini dell'articolo 40, paragrafo 4, primo comma, lettera b), del regolamento (UE) 2021/… (++), il trasferimento o la concessione di una licenza a favore di un soggetto giuridico stabilito in un paese associato o nell'Unione, ma controllato da paesi terzi, possono costituire un motivo di opposizione al trasferimento di proprietà dei risultati o alla concessione di licenze esclusive sui risultati;

c) ai fini dell'articolo 41, paragrafo 7, primo comma, lettera a), del regolamento(UE) 2021/… (++), qualora il programma di lavoro annuale lo preveda, è possibile limitare la concessione di diritti di accesso, come definiti all'articolo 2, punto 9), di tale regolamento, a un solo soggetto giuridico stabilito o considerato stabilito in uno Stato membro e controllato da tale Stato membro o da cittadini di tale Stato membro.

Articolo 34

Trasparenza

1. Il Centro di competenza svolge le proprie attività con un livello elevato di trasparenza.

2. Il Centro di competenza provvede affinché il pubblico e le parti interessate dispongano tempestivamente di informazioni adeguate, obiettive, affidabili e facilmente accessibili, in particolare sui risultati del suo lavoro. Inoltre, rende pubbliche le dichiarazioni di interessi rese a norma dell'articolo 43. Il medesimo requisito si applica ai centri nazionali di coordinamento, alla comunità e al gruppo consultivo strategico, conformemente al diritto pertinente.

3. Il consiglio di direzione, su proposta del direttore esecutivo, può autorizzare le parti interessate a presenziare in qualità di osservatori allo svolgimento di alcune attività del Centro di competenza.

4. Il Centro di competenza stabilisce nel regolamento interno del consiglio di direzione e del gruppo consultivo strategico le disposizioni pratiche per l'attuazione delle regole di trasparenza di cui ai paragrafi 1 e 2 del presente articolo. Ai fini delle azioni finanziate da Orizzonte Europa, tali regolamento interno e disposizioni tengono conto del regolamento (UE) 2021/… (++).

Articolo 35

Equilibrio di genere

Nell'attuazione del presente regolamento, all'atto della nomina di candidati o della proposta di rappresentanti, la Commissione europea, gli Stati membri e tutti gli altri portatori di interessi del settore istituzionale e privato scelgono rappresentanti tra diversi candidati, ove possibile, al fine di garantire l'equilibrio di genere.

Articolo 36

Norme di sicurezza sulla protezione delle informazioni classificate e delle informazioni sensibili non classificate

1. Previa approvazione della Commissione, il consiglio di direzione adotta le norme di sicurezza del Centro di competenza. Tali norme di sicurezza applicano i principi e le regole stabilite nelle decisioni (UE, Euratom) 2015/443 ([19]) e (UE, Euratom) 2015/444 ([20]) della Commissione.

(+) Regolamento di cui al documento ST 6789/20.
(++) Regolamento di cui al documento ST 7064/20
([19]) Decisione (UE, Euratom) 2015/443 della Commissione, del 13 marzo 2015, sulla sicurezza nella Commissione (GU L 72 del 17.3.2015, pag. 41).
([20]) 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).

2. I membri del consiglio di direzione, il direttore esecutivo, gli esperti esterni che partecipano ai gruppi di lavoro ad hoc e il personale del Centro di competenza rispettano gli obblighi di riservatezza di cui all'articolo 339TFUE, anche dopo la cessazione dalle proprie funzioni.

3. Il Centro di competenza può adottare le misure necessarie per semplificare lo scambio di informazioni utili allo svolgimento dei suoi compiti con la Commissione e gli Stati membri e, ove opportuno, con le istituzioni, organi e organismi dell'Unione pertinenti. Tutte le intese amministrative concluse a tal fine in merito alla condivisione delle informazioni classificate (ICUE) o, in assenza di intese, qualsiasi comunicazione eccezionale ad hoc di ICUE deve essere approvata dalla Commissione in via preliminare.

Articolo 37

Accesso ai documenti

1. Ai documenti detenuti dal Centro di competenza si applicano le disposizioni del regolamento (CE) n. 1049/2001.

2. Il consiglio di direzione adotta entro il … *[sei mesi dalla data di entrata in vigore del presente regolamento]* disposizioni per l'attuazione del regolamento (CE) n. 1049/2001.

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

Articolo 38

Monitoraggio, valutazione e riesame

1. Il Centro di competenza provvede affinché le sue attività, comprese quelle gestite attraverso i centri nazionali di coordinamento e la rete, siano oggetto di un monitoraggio continuo e sistematico e di periodiche valutazioni. Il Centro di competenza provvede affinché i dati per il monitoraggio dell'attuazione e dei risultati dei programmi di finanziamento dell'Unione di cui all'articolo 4, paragrafo 3, lettera b), siano raccolti in maniera efficiente, efficace e tempestiva, e impone ai destinatari dei fondi dell'Unione e degli Stati membri obblighi di relazione proporzionati. Le conclusioni di tale valutazione sono rese pubbliche.

2. La Commissione, tenendo conto del contributo preliminare del consiglio di direzione, dei centri nazionali di coordinamento e della comunità, elabora una relazione sull'attuazione relativa al Centro di competenza non appena siano disponibili informazioni sufficienti sull'attuazione del presente regolamento e comunque non oltre trenta mesi dalla data di cui all'articolo 46, paragrafo 4, del presente regolamento. La Commissione trasmette tale relazione sulla valutazione al Parlamento europeo e al Consiglio entro il 30 giugno 2024. Il Centro di competenza e gli Stati membri forniscono alla Commissione le informazioni necessarie per redigere tale relazione.

3. La relazione sull'attuazione di cui al paragrafo 2 include una valutazione:

a) della capacità lavorativa del Centro di competenza per quanto riguarda i suoi obiettivi, missione e compiti, nonché la cooperazione e il coordinamento con altri portatori di interessi, in particolare i centri nazionali di coordinamento, la comunità e l'ENISA;

b) dei risultati conseguiti dal Centro di competenza in relazione alla sua missione, ai suoi obiettivi, al suo mandato e ai suoi compiti, in particolare all'efficienza del Centro di competenza nel coordinare i fondi dell'Unione e mettere in comune le competenze;

c) della coerenza dei compiti di esecuzione conformemente all'agenda e al programma di lavoro pluriennale;

d) del coordinamento e della cooperazione del Centro di competenza con i comitati di programma di Orizzonte Europa e del Programma Europa digitale, in particolare al fine di aumentare la coerenza e le sinergie con il programma di lavoro annuale, il programma di lavoro pluriennale, l'agenda, Orizzonte Europa e il programma Europa digitale;

e) delle azioni congiunte.

4. Dopo la presentazione della relazione sull'attuazione di cui al paragrafo 2 del presente articolo, la Commissione procede a una valutazione finale del Centro di competenza tenendo conto del contributo preliminare del consiglio di direzione, dei centri nazionali di coordinamento e della comunità. Tale valutazione fa riferimento alle valutazioni di cui al paragrafo 3 del presente articolo, oppure se del caso le aggiorna, ed è effettuata prima del termine del periodo specificato all'articolo 47, paragrafo 1, al fine di determinare in tempo utile se sia appropriato prorogare la durata del mandato del Centro di competenza oltre tale periodo. Tale valutazione esamina gli aspetti giuridici e amministrativi relativi al mandato del Centro di competenza e il potenziale per creare sinergie e evitare la frammentazione con altre istituzioni, organi e organismi dell'Unione.

Se ritiene che sia giustificato mantenere il Centro di competenza, tenuto conto della sua missione, dei suoi obiettivi, del suo mandato e dei suoi compiti, la Commissione può presentare una proposta legislativa per prorogare la durata del mandato del Centro di competenza quale indicata all'articolo 47.

5. Sulla base delle conclusioni della relazione sull'attuazione di cui al paragrafo 2, la Commissione può adottare provvedimenti appropriati.

6. Il monitoraggio, la valutazione, la soppressione graduale e il rinnovo del contributo di Orizzonte Europa sono svolti conformemente agli articoli 10, 50 e 52 del regolamento (UE) 2021/… (+) e delle disposizioni di attuazione concordate.

7. Il monitoraggio, la rendicontazione e la valutazione in merito al contributo del Programma Europa digitale sono svolti conformemente agli articoli 24 e 25 del regolamento (UE) 2021/… (++).

8. In caso di liquidazione del Centro di competenza, la Commissione esegue una valutazione finale del Centro di competenza entro sei mesi dalla sua liquidazione, ma comunque non oltre due anni dall'avvio della procedura di liquidazione di cui all'articolo 47 del presente regolamento. I risultati della valutazione finale sono presentati al Parlamento europeo e al Consiglio.

Articolo 39

Personalità giuridica del Centro di competenza

1. Il Centro di competenza ha personalità giuridica.

2. In ogni Stato membro, il Centro di competenza gode della più ampia capacità giuridica riconosciuta alle persone giuridiche dalla legislazione di tale Stato. In particolare, può acquisire o alienare beni mobili e immobili e stare in giudizio.

Articolo 40

Responsabilità del Centro di competenza

1. La responsabilità contrattuale del Centro di competenza è regolata dalla legge applicabile all'accordo, alla decisione o al contratto in causa.

2. In caso di responsabilità extracontrattuale, il Centro di competenza risarcisce i danni causati dal personale nell'esercizio delle sue funzioni, secondo i principi generali comuni agli ordinamenti degli Stati membri.

3. Tutti i pagamenti effettuati dal Centro di competenza connessi alla responsabilità di cui ai paragrafi 1 e 2, nonché i costi e le spese sostenuti in relazione ad essa, sono considerati spese del Centro di competenza e sono coperti dalle sue risorse.

4. Il Centro di competenza è il solo responsabile del rispetto dei propri obblighi.

Articolo 41

Competenza della Corte di giustizia dell'Unione europea e diritto applicabile

1. La Corte di giustizia dell'Unione europea è competente a pronunciarsi:

a) mediante una pronuncia in base alle clausole compromissorie contenute nelle decisioni adottate dal Centro di competenza o negli accordi o nei contratti stipulati da quest'ultimo;

b) sulle controversie relative al risarcimento dei danni causati dal personale del Centro di competenza nell'esercizio delle sue funzioni;

c) sulle controversie tra il Centro di competenza e il suo personale, nei limiti e alle condizioni fissati dallo statuto dei funzionari.

2. Per tutte le questioni non contemplate dal presente regolamento o da altri atti giuridici dell'Unione, si applica il diritto dello Stato membro in cui ha sede il Centro di competenza.

Articolo 42

Responsabilità dell'Unione e degli Stati membri e assicurazioni

1. La responsabilità finanziaria dell'Unione e degli Stati membri per i debiti contratti dal Centro di competenza è limitata al rispettivo contributo già fornito per le spese amministrative.

(+) Regolamento di cui al documento ST 7064/20.
(++) Regolamento di cui al documento ST 6789/20.

2. Il Centro di competenza sottoscrive le idonee assicurazioni e le mantiene in vigore.

Articolo 43

Conflitti di interessi

Il consiglio di direzione adotta norme per la prevenzione, l'individuazione e la risoluzione dei conflitti di interessi che riguardino i suoi membri, i suoi organi e il suo personale, compreso il direttore esecutivo. Tali norme contengono disposizioni volte a evitare situazioni di conflitto di interessi per i rappresentanti dei membri che fanno parte del consiglio di direzione e del gruppo consultivo strategico ai sensi del regolamento finanziario, incluse disposizioni su eventuali dichiarazioni di interessi. In materia di conflitto di interessi i centri nazionali di coordinamento sono soggetti al diritto nazionale.

Articolo 44

Protezione dei dati personali

1. Il trattamento dei dati personali da parte del Centro di competenza è soggetto al regolamento (UE) 2018/1725.

2. Il consiglio di direzione adotta le misure di attuazione di cui all'articolo 45, paragrafo 3, del regolamento (UE) 2018/1725. Il consiglio di direzione può adottare misure aggiuntive necessarie per l'applicazione di tale regolamento da parte del Centro di competenza.

Articolo 45

Sostegno da parte dello Stato membro ospitante

Tra il Centro di competenza e lo Stato membro ospitante in cui esso ha sede può essere concluso un accordo amministrativo concernente i privilegi e le immunità e altre agevolazioni che tale Stato membro è tenuto a concedere al Centro di competenza.

CAPO VI

DISPOSIZIONI FINALI

Articolo 46

Misure iniziali

1. La Commissione è responsabile dell'istituzione e del funzionamento iniziale del Centro di competenza fino a quando questo non avrà la capacità operativa di dare esecuzione al proprio bilancio. La Commissione adotta, conformemente al diritto dell'Unione, tutti i provvedimenti necessari con il coinvolgimento degli organi competenti del Centro di competenza.

2. Ai fini del paragrafo 1 del presente articolo, la Commissione può designare un direttore esecutivo ad interim fino a quando il direttore esecutivo non assume le sue funzioni dopo essere stato nominato dal consiglio di direzione a norma dell'articolo 16. Tale direttore esecutivo ad interim esercita le funzioni del direttore esecutivo e può essere assistito da un numero limitato di membri del personale della Commissione. La Commissione può distaccare ad interim un numero limitato di membri del personale del Centro di competenza.

3. Il direttore esecutivo ad interim può autorizzare tutti i pagamenti coperti dagli stanziamenti previsti nel bilancio annuale del Centro di competenza, previa approvazione da parte del consiglio di direzione, e può stipulare convenzioni e contratti, anche relativi al personale, e adottare decisioni, in seguito all'adozione della tabella dell'organico di cui all'articolo 13, paragrafo 3, lettera l).

4. Il direttore esecutivo ad interim, di comune accordo con il direttore esecutivo e fatta salva l'approvazione del consiglio di direzione, stabilisce la data alla quale il Centro di competenza avrà la capacità di dare esecuzione al proprio bilancio. A partire da tale data, la Commissione si astiene dall'assumere impegni e dall'eseguire pagamenti per le attività del Centro di competenza.

Articolo 47

Durata

1. Il Centro di competenza è istituito per il periodo compreso fra il … *[la data di entrata in vigore del presente regolamento]* e il 31 dicembre 2029.

2. Al termine del periodo di cui al paragrafo 1 del presente articolo, a meno che il mandato del Centro di competenza sia prorogato ai sensi dell'articolo 38, paragrafo 4, sarà avviata automaticamente la procedura di liquidazione al termine del periodo di cui al paragrafo 1 del presente articolo.

3. Ai fini della procedura di liquidazione del Centro di competenza, il consiglio di direzione nomina uno o più liquidatori, i quali si attengono alle decisioni del consiglio di direzione.

4. Durante la procedura di liquidazione del Centro di competenza, le attività sono utilizzate per coprire le passività e le spese relative alla liquidazione. Eventuali eccedenze sono distribuite fra l'Unione e gli Stati membri contributori, proporzionalmente al loro contributo finanziario al Centro di competenza. Qualsiasi eccedenza a favore dell'Unione è restituita al bilancio dell'Unione.

Articolo 48

Entrata in vigore

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

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

Fatto a Bruxelles, il …

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

Motivazione del Consiglio: Posizione (UE) n. 18/2021 del Consiglio in prima lettura in vista dell'adozione del regolamento del Parlamento europeo e del Consiglio che istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento

(2021/C 191/02)

I. INTRODUZIONE

1. Il 12 settembre 2018, nel contesto della propria strategia per il mercato unico digitale, la Commissione ha adottato e trasmesso al Consiglio e al Parlamento europeo la proposta ([1]) di regolamento del Parlamento europeo e del Consiglio che istituisce il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento, avente come base giuridica l'articolo 173, paragrafo 3, e l'articolo 188 TFUE.

2. L'obiettivo della proposta è aiutare l'UE a mantenere e sviluppare le capacità tecnologiche e industriali in materia di cibersicurezza necessarie a tutelare il suo mercato unico digitale. La proposta prevede la creazione di strutture a tre livelli istituzionali: una rete di centri nazionali di coordinamento (livello nazionale), una comunità delle competenze in materia di cibersicurezza (livello dei portatori di interessi) e un Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca sulla cibersicurezza (livello dell'UE). Il Centro di competenza gestirà il sostegno finanziario legato alla cibersicurezza a carico del bilancio dell'UE e agevolerà gli investimenti congiunti dell'UE, degli Stati membri e dell'industria per rafforzare la cibersicurezza dell'UE.

3. La Commissione ha presentato la proposta al gruppo orizzontale «Questioni riguardanti il ciberspazio» (di seguito «il gruppo») il 17 settembre 2018; a ciò ha fatto seguito un esame della valutazione d'impatto in sede di gruppo il 28 settembre 2018. La discussione della proposta stessa in sede di gruppo è iniziata il 28 settembre 2018 sotto la presidenza austriaca ed è proseguita sotto le presidenze rumena, finlandese, croata e tedesca.

4. Il Comitato economico e sociale europeo (CESE) ha adottato il suo parere ([2]) sulla proposta il 23 gennaio 2019. Il CESE ha accolto con favore l'iniziativa della Commissione, considerandola funzionale allo sviluppo di una strategia industriale per la cibersicurezza e un'iniziativa strategica per raggiungere una solida ed ampia autonomia digitale.

5. In seno al Parlamento europeo il fascicolo è stato assegnato alla commissione per l'industria, la ricerca e l'energia (ITRE) e Julia REDA (ITRE, Verts/ALE) è stata nominata relatrice. La relazione è stata adottata il 19 febbraio 2019 dalla commissione ITRE e approvata dal Parlamento durante la tornata di marzo I 2019. Il 17 aprile 2019, con 489 voti favorevoli, 73 contrari e 56 astensioni, il Parlamento europeo ha adottato la sua posizione in prima lettura ([3]), con 112 emendamenti alla proposta della Commissione. A seguito delle elezioni europee Rasmus ANDRESEN (ITRE, Verts/ALE) è stato nominato nuovo relatore.

6. Il 13 marzo 2019 il Coreper ha dato mandato ([4]) per avviare i negoziati con il Parlamento europeo. Da allora si sono tenuti cinque triloghi: il 13 e il 20 marzo 2019 durante la presidenza rumena, il 25 giugno 2020 durante la presidenza croata e il 29 ottobre e l'11 dicembre 2020 durante la presidenza tedesca.

7. Il primo trilogo, che si è tenuto il 13 marzo 2019 a Strasburgo, non ha portato a discussioni sostanziali. Entrambe le parti hanno presentato le loro posizioni e le principali modifiche formulate nelle rispettive proposte, oltre a concordare le fasi successive e il calendario. I colegislatori hanno confermato il loro forte impegno a raggiungere un accordo il prima possibile.

8. Nel corso del secondo trilogo, tenutosi il 20 marzo 2019 a Bruxelles, sono state discusse le questioni che nella prima riunione tecnica erano state individuate come politiche, ossia principalmente la missione e i compiti del Centro di competenza, il finanziamento e il consiglio di direzione. La presidenza rumena ha basato il suo approccio sul mandato ricevuto per il primo trilogo. Il secondo trilogo ha rivelato un atteggiamento positivo da entrambe le parti, in quanto è stata dimostrata flessibilità su varie questioni e sono stati forniti orientamenti a livello tecnico al fine di compiere ulteriori progressi sul testo di compromesso.

9. Il 3 giugno 2020 il Coreper ha approvato un mandato riveduto per i negoziati con il Parlamento europeo ([5]). Un terzo trilogo si è tenuto il 25 giugno 2020, al termine della presidenza croata, al fine di informare il Parlamento europeo in merito alle principali modifiche del nuovo mandato del Consiglio, con particolare attenzione a quanto segue: 1) la missione, gli obiettivi e i compiti del Centro di competenza, 2) la sua struttura, 3) le disposizioni finanziarie e 4) la comunità delle competenze in materia di cibersicurezza.

([1]) Doc. 12104/18.
([2]) Doc. 5898/19 (GU C 159 del 10.5.2019, pag. 63).
([3]) GU C 158 del 30.4.2021, pag. 850.
([4]) Doc. 7583/19.
([5]) Doc. 8315/20.

10. Una questione relativa alla posizione del Consiglio sui diritti di voto del consiglio di direzione del Centro, che era rimasta in sospeso, è stata risolta in sede di Consiglio durante la presidenza tedesca. Il 22 luglio 2020 il Coreper ha adottato un mandato riveduto che chiarisce la portata del diritto di veto della Commissione.

11. Un'altra questione in sospeso sulla sede del Centro di competenza è stata risolta a margine del Coreper del 28 ottobre 2020 dai rappresentanti dei governi degli Stati membri, che hanno concordato una procedura di selezione per tale sede ([6]). La decisione sulla sede è stata presa dai rappresentanti dei governi degli Stati membri a margine del Coreper del 9 dicembre 2020. Bucarest (Romania) è stata scelta come sede.

12. Il quarto trilogo, tenutosi il 29 ottobre 2020, ha conferito un ampio mandato a livello tecnico per trovare compromessi sulle restanti questioni in sospeso. Nel corso di varie riunioni tecniche sono stati trovati compromessi sulla maggior parte delle questioni.

13. Nel quinto e ultimo trilogo, tenutosi l'11 dicembre 2020, il Consiglio e il Parlamento europeo hanno raggiunto un accordo provvisorio in linea con il mandato che è stato rinnovato dal Coreper il 9 dicembre 2020. Il 18 dicembre 2020 il Coreper ha approvato il testo di compromesso finale concordato in sede di trilogo.

II. OBIETTIVO

14. La proposta in oggetto prevede la creazione di un Centro di competenza, che costituirebbe il principale strumento dell'UE per concentrare gli investimenti nello sviluppo industriale, nella tecnologia e nella ricerca sulla cibersicurezza e fornirebbe inoltre il sostegno finanziario legato alla cibersicurezza e concesso dai programmi Europa digitale e Orizzonte Europa. Come sopra indicato, la proposta prevede anche la creazione di una rete dei centri nazionali di coordinamento e di una comunità delle competenze in materia di cibersicurezza.

15. Il Centro di competenza sarebbe dotato di un consiglio di direzione, composto da rappresentanti degli Stati membri e della Commissione, che definisce l'orientamento generale delle operazioni del Centro e garantisce che quest'ultimo svolga i propri compiti conformemente al regolamento. L'obiettivo del Centro sarebbe quello di garantire un maggiore coordinamento tra la ricerca e l'innovazione, nonché la diffusione di strategie a livello nazionale e dell'UE, e di consentire agli Stati membri di prendere decisioni in merito ai loro contributi finanziari alle azioni congiunte.

16. Il Centro di competenza avrebbe la capacità di:

    i) attuare azioni di ricerca e innovazione (sostenute da Orizzonte Europa) nonché azioni di sviluppo delle capacità (sostenute da Europa digitale), conformemente alla suddetta governance (ossia la Commissione e gli Stati membri);

    ii) sostenere, insieme agli Stati membri, lo sviluppo e l'acquisizione di attrezzature, infrastrutture di dati e strumenti avanzati per la cibersicurezza in Europa e garantire un'ampia diffusione delle più recenti soluzioni di cibersicurezza in tutta l'economia; a tal fine, il Centro di competenza sarebbe anche in grado di facilitare l'acquisizione condivisa di capacità per conto degli Stati membri.

III. ANALISI DELLA POSIZIONE DEL CONSIGLIO IN PRIMA LETTURA

A. CONTESTO PROCEDURALE

17. Il Parlamento europeo e il Consiglio hanno condotto negoziati al fine di concludere un accordo nella fase della posizione del Consiglio in prima lettura («accordo rapido in seconda lettura»). Il testo della posizione del Consiglio in prima lettura rispecchia il pacchetto di compromesso concordato tra i due colegislatori, con il sostegno della Commissione.

B. SINTESI DELLE PRINCIPALI QUESTIONI

18. Rispetto alla proposta iniziale della Commissione, le principali modifiche concordate da entrambi i colegislatori sono le seguenti:

    1) è stata introdotta una formulazione di compromesso in varie disposizioni per allineare il testo alle disposizioni del regolamento Europa digitale e del regolamento Orizzonte Europa, dal momento che il Centro di competenza gestirà il sostegno finanziario legato alla cibersicurezza e concesso dai programmi Orizzonte Europa e Europa digitale;

    2) il riferimento alla sede del Centro di competenza nella parte dispositiva del regolamento (articolo 1) è stato soppresso. È stato invece aggiunto un nuovo considerando (20);

([6]) Doc. 13405/20.

3) è stata aggiunta una serie di concetti, con le opportune definizioni, quali «minaccia informatica», «azione congiunta», «contributo in natura» e «poli europei dell'innovazione digitale»;

4) è stata aggiunta l'«agenda», segnatamente una strategia di cibersicurezza in materia industriale, tecnologica e della ricerca globale e sostenibile, che formula raccomandazioni strategiche per lo sviluppo e la crescita del settore europeo della cibersicurezza nell'ambito industriale, tecnologico e della ricerca, e che contiene le priorità strategiche per le attività del Centro di competenza;

5) i compiti del Centro di competenza, originariamente definiti in un unico articolo insieme agli obiettivi, sono ora delineati in un articolo specifico e viene operata una distinzione tra i compiti strategici e i compiti di esecuzione del Centro;

6) il ruolo dell'ENISA è stato rafforzato. L'ENISA sarà un osservatore permanente nel consiglio di direzione del Centro di competenza e potrà fornire consulenza e contributi per l'elaborazione dell'agenda e dei programmi di lavoro annuale e pluriennale;

7) sono state introdotte nuove disposizioni relative ai centri nazionali di coordinamento, in particolare per quanto riguarda la designazione dei centri e la valutazione della Commissione;

8) i compiti del consiglio di direzione sono stati ulteriormente precisati, in particolare per quanto riguarda l'adozione dell'agenda e dei programmi di lavoro annuale e pluriennale;

9) le regole di voto del consiglio di direzione del Centro di competenza sono state modificate ed è stato stabilito il principio «un membro, un voto», anziché la disposizione originaria della proposta della Commissione, secondo la quale l'UE dovrebbe detenere il 50 % dei diritti di voto. Tuttavia, per talune decisioni connesse all'esecuzione del bilancio dell'Unione, nonché per quanto riguarda il programma di lavoro annuale, il programma di lavoro pluriennale e la metodologia per il calcolo dei contributi degli Stati membri, la Commissione deterrà il 26 % dei diritti di voto; il consiglio di direzione delibera a maggioranza di almeno il 75 % di tutti i suoi membri;

10) il consiglio consultivo industriale e scientifico è stato trasformato nel gruppo consultivo strategico, che fornirà consulenza sulla base di un dialogo costante tra il Centro di competenza e la comunità delle competenze in materia di cibersicurezza;

11) la comunità delle competenze in materia di cibersicurezza sarà costituita da organizzazioni/organi collettivi e non comprenderà singoli individui; a titolo di compromesso, il Centro di competenza e i suoi organi potranno ricorrere alle competenze di singoli individui e persone fisiche in qualità di esperti ad hoc;

12) sono stati aggiunti nuovi articoli sull'equilibrio di genere (articolo 35) e sulla personalità giuridica del Centro di competenza (articolo 39).

IV. **CONCLUSIONE**

19. La posizione del Consiglio in prima lettura rispecchia il pacchetto di compromesso concordato tra il Consiglio e il Parlamento europeo, con il sostegno della Commissione.

20. Il Consiglio ritiene che la sua posizione in prima lettura rappresenti un pacchetto equilibrato e che, una volta adottato, il nuovo regolamento svolgerà un ruolo chiave nell'ulteriore sviluppo delle capacità tecnologiche, industriali e di ricerca dell'UE in materia di cibersicurezza.

ISSN 1977-0944 (edizione elettronica)
ISSN 1725-2466 (edizione cartacea)

Ufficio delle pubblicazioni dell'Unione europea
L-2985 Lussemburgo
LUSSEMBURGO

IT