DIRETTIVE

DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 14 dicembre 2022

relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

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

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere della Banca centrale europea ([1]),

visto il parere del Comitato economico e sociale europeo ([2]),

previa consultazione del Comitato delle regioni,

deliberando secondo la procedura legislativa ordinaria ([3]),

considerando quanto segue:

(1) La direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio ([4]) mirava a sviluppare le capacità di cibersicurezza in tutta l'Unione, a mitigare le minacce ai sistemi informatici e di rete utilizzati per fornire servizi essenziali in settori chiave e a garantire la continuità di tali servizi in caso di incidenti, contribuendo in tal modo alla sicurezza dell'Unione e al funzionamento efficace della sua economia e della sua società.

(2) Dall'entrata in vigore della direttiva (UE) 2016/1148 sono stati compiuti progressi significativi nell'aumentare il livello dell'Unione in materia di ciberresilienza. La revisione di tale direttiva ha mostrato quanto quest'ultima sia servita da catalizzatore per l'approccio istituzionale e normativo alla cibersicurezza nell'Unione, aprendo la strada a un significativo cambiamento della mentalità. Tale direttiva ha garantito il completamento dei quadri nazionali sulla sicurezza dei sistemi informatici e di rete definendo le strategie nazionali sulla sicurezza dei sistemi informatici e di rete e stabilendo capacità nazionali e attuando misure normative riguardanti le infrastrutture e gli attori essenziali individuati da ciascuno Stato membro. La direttiva (UE) 2016/1148 ha inoltre contribuito alla cooperazione a livello dell'Unione mediante l'istituzione del gruppo di cooperazione e della rete di gruppi nazionali di intervento per la sicurezza informatica in caso di incidente. Nonostante tali risultati, la revisione della direttiva (UE) 2016/1148 ha rivelato carenze intrinseche che le impediscono di affrontare efficacemente le sfide attuali ed emergenti in materia di cibersicurezza.

(3) I sistemi informatici e di rete occupano ormai una posizione centrale nella vita di tutti i giorni, con la rapida trasformazione digitale e l'interconnessione della società, anche negli scambi transfrontalieri. Ciò ha portato a un'espansione del panorama delle minacce informatiche, con nuove sfide che richiedono risposte adeguate, coordinate e innovative in tutti gli Stati membri. Il numero, la portata, il livello di sofisticazione, la frequenza e l'impatto degli incidenti stanno aumentando e rappresentano una grave minaccia per il funzionamento dei sistemi informatici e di rete. Tali incidenti possono quindi impedire l'esercizio delle attività economiche nel mercato

([1]) GU C 233 del 16.6.2022, pag. 22.
([2]) GU C 286 del 16.7.2021, pag. 170.
([3]) Posizione del Parlamento europeo del 10 novembre 2022 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 28 novembre 2022.
([4]) Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante 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).

interno, provocare perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia e alla società dell'Unione. Pertanto la preparazione e l'efficacia della cibersicurezza sono oggi più che mai essenziali per il corretto funzionamento del mercato interno. Inoltre, la cibersicurezza è un fattore abilitante fondamentale per molti settori critici, affinché questi possano attuare con successo la trasformazione digitale e cogliere appieno i vantaggi economici, sociali e sostenibili della digitalizzazione.

(4) La base giuridica della direttiva (UE) 2016/1148 era l'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE), il cui obiettivo è l'instaurazione e il funzionamento del mercato interno mediante il rafforzamento delle misure relative al ravvicinamento delle normative nazionali. Gli obblighi di cibersicurezza imposti ai soggetti che forniscono servizi o svolgono attività economicamente rilevanti variano notevolmente da uno Stato membro all'altro in termini di tipo di obbligo, livello di dettaglio e metodo di vigilanza. Tali disparità comportano costi aggiuntivi e creano difficoltà per le entità che offrono beni o servizi transfrontalieri. Gli obblighi imposti da uno Stato membro che sono diversi o addirittura in conflitto con quelli imposti da un altro Stato membro possono incidere in modo sostanziale su tali attività transfrontaliere. Inoltre, è probabile che una progettazione o attuazione inadeguata degli obblighi in materia di cibersicurezza in uno Stato membro abbia ripercussioni sul livello di cibersicurezza di altri Stati membri, in particolare in considerazione dell'intensità degli scambi transfrontalieri. Il riesame della direttiva (UE) 2016/1148 ha evidenziato notevoli divergenze nella sua attuazione da parte degli Stati membri, anche per quanto riguarda il suo ambito di applicazione, la cui delimitazione è stata lasciata in larga misura alla discrezione degli Stati membri. La direttiva (UE) 2016/1148 ha inoltre conferito agli Stati membri un ampio potere discrezionale per quanto riguarda l'attuazione degli obblighi in materia di sicurezza e segnalazione degli incidenti ivi stabiliti. Tali obblighi sono stati pertanto attuati in modi significativamente diversi a livello nazionale. Analoghe divergenze sussistono nell'attuazione delle disposizioni della direttiva (UE) 2016/1148 in materia di vigilanza e esecuzione.

(5) Tutte tali divergenze comportano una frammentazione del mercato interno e possono avere un effetto pregiudizievole sul suo funzionamento, con ripercussioni in particolare sulla fornitura transfrontaliera di servizi e sul livello di ciberresilienza dovute all'applicazione di misure diverse. Dette divergenze possono portare infine a una maggiore vulnerabilità di taluni Stati membri di fronte alle minacce informatiche, con potenziali ricadute sull'intera Unione. La presente direttiva mira a eliminare tali ampie divergenze tra gli Stati membri, in particolare stabilendo norme minime riguardanti il funzionamento di un quadro normativo coordinato, istituendo meccanismi per una cooperazione efficace tra le autorità responsabili in ciascuno Stato membro, aggiornando l'elenco dei settori e delle attività soggetti agli obblighi in materia di cibersicurezza e prevedendo mezzi di ricorso e misure di esecuzione effettivi che siano funzionali all'efficace applicazione di tali obblighi. La direttiva (UE) 2016/1148 dovrebbe pertanto essere abrogata e sostituita dalla presente direttiva.

(6) Con l'abrogazione della direttiva (UE) 2016/1148, l'ambito di applicazione per settore dovrebbe essere esteso a una parte più ampia dell'economia per fornire una copertura completa dei settori e dei servizi di vitale importanza per le principali attività sociali ed economiche nel mercato interno. In particolare, la presente direttiva mira a superare le carenze della differenziazione tra gli operatori di servizi essenziali e i fornitori di servizi digitali, che si è rivelata obsoleta, in quanto non riflette l'effettiva importanza dei settori o dei servizi per le attività sociali ed economiche nel mercato interno.

(7) Ai sensi della direttiva (UE) 2016/1148, gli Stati membri erano responsabili di identificare i soggetti che soddisfacevano i criteri per essere considerati operatori di servizi essenziali. Al fine di eliminare le ampie divergenze tra gli Stati membri a tale riguardo e garantire la certezza del diritto per quanto riguarda le misure di gestione dei rischi di cibersicurezza e gli obblighi di segnalazione per tutti i soggetti pertinenti, è opportuno stabilire un criterio uniforme che determini quali soggetti rientrano nell'ambito di applicazione della presente direttiva. Tale criterio dovrebbe consistere nell'applicazione di una regola della soglia di dimensione, in base alla quale si considerano medie imprese ai sensi dell'articolo 2, paragrafo 1, dell'allegato alla raccomandazione 2003/361/CE della Commissione ([5]), o superano i massimali per le medie imprese di cui al paragrafo 1 di tale articolo, e che operano

([5]) Raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

nei settori e forniscono le tipologie di servizi o svolgono le attività contemplati dalla presente direttiva. Gli Stati membri dovrebbero inoltre prevedere che determinate piccole imprese e microimprese, quali definite all'articolo 2, paragrafi 2 e 3, di tale allegato, che soddisfano criteri specifici che indicano un ruolo chiave per la società, l'economia o per particolari settori o tipi di servizi rientrino nell'ambito di applicazione della presente direttiva.

(8) L'esclusione degli enti della pubblica amministrazione dall'ambito di applicazione della presente direttiva dovrebbe applicarsi ai soggetti che operano principalmente nei settori della sicurezza nazionale, della sicurezza pubblica, della difesa o svolgono attività di contrasto, compresi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati. Tuttavia, gli enti della pubblica amministrazione le cui attività sono solo marginalmente connesse a tali settori non dovrebbero essere esclusi dall'ambito di applicazione della presente direttiva. Ai fini della presente direttiva, non si considera che i soggetti con competenze normative operino nel settore dell'attività di contrasto e pertanto essi non sono esclusi su tale base dall'ambito di applicazione della presente direttiva. Gli enti della pubblica amministrazione istituiti congiuntamente con un paese terzo in conformità di un accordo internazionale sono esclusi dall'ambito di applicazione della presente direttiva. La presente direttiva non si applica alle missioni diplomatiche e consolari degli Stati membri nei paesi terzi né ai loro sistemi informatici e di rete, nella misura in cui tali sistemi siano situati nei locali della missione o utilizzati per utenti in un paese terzo.

(9) Gli Stati membri dovrebbero essere in grado di adottare le misure necessarie a garantire la tutela degli interessi essenziali della sicurezza nazionale, a salvaguardare l'ordine pubblico e la pubblica sicurezza e a consentire la prevenzione, l'indagine, l'accertamento e il perseguimento dei reati. A tal fine, gli Stati membri dovrebbero poter esentare soggetti specifici che svolgono attività nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o dell'applicazione della legge, compresi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati da determinati obblighi previsti dalla presente direttiva per quanto riguarda tali attività. Qualora un soggetto fornisca servizi esclusivamente a un ente della pubblica amministrazione escluso dall'ambito di applicazione della presente direttiva, gli Stati membri dovrebbero poter esentare tale soggetto da determinati obblighi stabiliti dalla presente direttiva per quanto riguarda tali servizi. Inoltre, nessuno Stato membro dovrebbe essere tenuto a fornire informazioni la cui divulgazione sia contraria agli interessi essenziali della propria pubblica sicurezza. Dovrebbero essere prese in considerazione in tale contesto le norme dell'Unione o nazionali per la protezione delle informazioni classificate, gli accordi di non divulgazione o gli accordi di non divulgazione informali, quale il protocollo TLP. Il protocollo TLP deve essere inteso come uno strumento per fornire informazioni su eventuali limitazioni per quanto riguarda l'ulteriore diffusione delle informazioni. È utilizzato in quasi tutti i team di risposta agli incidenti di sicurezza informatica (CSIRT) e in alcuni centri di analisi e condivisione delle informazioni.

(10) Sebbene la presente direttiva si applichi ai soggetti che svolgono attività di produzione di energia elettrica da centrali nucleari, alcune di tali attività possono essere collegate alla sicurezza nazionale. In tal caso, uno Stato membro dovrebbe poter esercitare la propria responsabilità per la salvaguardia della propria sicurezza nazionale in relazione a tali attività, comprese le attività all'interno della catena del valore nucleare, conformemente ai trattati.

(11) Alcuni soggetti svolgono attività nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o dell'applicazione della legge, compresi la prevenzione, l'indagine, l'accertamento e il perseguimento dei reati, fornendo nel contempo anche servizi fiduciari. I prestatori di servizi fiduciari che rientrano nell'ambito di applicazione del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio ([6]) dovrebbero rientrare nell'ambito di applicazione della presente direttiva al fine di garantire un livello di requisiti di sicurezza e supervisione analogo a quello precedentemente stabilito in tale regolamento nei confronti dei prestatori di servizi fiduciari. In linea con l'esclusione di alcuni servizi specifici dal regolamento (UE) n. 910/2014, la presente direttiva non dovrebbe applicarsi alla prestazione di servizi fiduciari che sono utilizzati esclusivamente nell'ambito di sistemi chiusi contemplati dal diritto nazionale o da accordi conclusi tra un insieme definito di partecipanti.

([6]) Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73).

(12) I fornitori di servizi postali come definiti dalla direttiva 97/67/CE del Parlamento europeo e del Consiglio ([7]), inclusi i fornitori di servizi di corriere, dovrebbero essere soggetti alla presente direttiva se provvedono ad almeno una delle fasi della catena di consegna postale, in particolare la raccolta, lo smistamento, il trasporto o la distribuzione di invii postali, compresi i servizi di ritiro, tenendo conto nel contempo del grado di relativa dipendenza dai sistemi informatici e di rete. I servizi di trasporto che non sono forniti nell'ambito di una di tali fasi dovrebbero essere esclusi dall'ambito di applicazione dei servizi postali.

(13) Data l'intensificazione e la crescente sofisticazione delle minacce informatiche, gli Stati membri dovrebbero adoperarsi per garantire che i soggetti esclusi dall'ambito di applicazione della presente direttiva raggiungano un livello elevato di cibersicurezza e sostengano l'attuazione di misure equivalenti di gestione dei rischi di cibersicurezza, che riflettano la natura sensibile di tali soggetti.

(14) A qualsiasi trattamento di dati personali ai sensi della presente direttiva si applica il diritto dell'Unione in materia di protezione dei dati personali e della vita privata. La presente direttiva non pregiudica in particolare il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([8]) e la direttiva 2002/58/CE del Parlamento europeo e del Consiglio ([9]). La presente direttiva non dovrebbe pertanto pregiudicare, tra l'altro, i compiti e i poteri delle autorità competenti di monitorare il rispetto del diritto dell'Unione in vigore in materia di protezione dei dati personali e della vita privata.

(15) I soggetti che rientrano nell'ambito di applicazione della presente direttiva ai fini del rispetto delle misure di gestione dei rischi di cibersicurezza e degli obblighi di segnalazione dovrebbero essere classificati in due categorie, essenziali e importanti, in funzione della loro importanza per il settore o il tipo di servizi che forniscono, nonché delle loro dimensioni. A tale riguardo, si dovrebbe tenere debitamente conto, se del caso, di tutte le valutazioni settoriali dei rischi o di tutti gli orientamenti pertinenti elaborati dalle autorità competenti. I regimi di esecuzione e di vigilanza per tali due categorie di soggetti dovrebbero essere differenziati per garantire un giusto equilibrio tra i requisiti e gli obblighi basati sui rischi, da un lato, e gli oneri amministrativi derivanti dalla vigilanza della conformità, dall'altro.

(16) Al fine di evitare che soggetti che hanno imprese partner o che sono imprese collegate siano considerati soggetti essenziali o importanti qualora ciò sarebbe sproporzionato, gli Stati membri possono tenere conto del grado di indipendenza di cui gode un soggetto in relazione alle sue imprese partner e collegate nell'applicazione dell'articolo 6, paragrafo 2, dell'allegato alla raccomandazione 2003/361/CE. In particolare, gli Stati membri possono tenere conto del fatto che un soggetto è indipendente dalle sue imprese partner o collegate in termini di sistemi informatici e di rete che utilizza nella fornitura dei suoi servizi e in termini di servizi che fornisce. Su tale base, se del caso, gli Stati membri possono ritenere che tale soggetto non sia considerato una media impresa ai sensi dell'articolo 2 dell'allegato della raccomandazione 2003/361/CE, o non superi i massimali per le medie imprese di cui al paragrafo 1 di tale articolo se, tenuto conto del grado di indipendenza di tale soggetto, si ritenga che esso non sia consideri una media impresa o superi tali massimali nel caso in cui siano stati presi in considerazione solo i suoi dati. Ciò lascia impregiudicati gli obblighi di cui alla presente direttiva per le imprese associate e collegate che rientrano nel campo di applicazione della presente direttiva.

(17) Gli Stati membri dovrebbero poter decidere che i soggetti definiti, prima dell'entrata in vigore della presente direttiva, come operatori di servizi essenziali ai sensi della direttiva (UE) 2016/1148 debbano essere considerati soggetti essenziali.

([7]) Direttiva 97/67/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, concernente regole comuni per lo sviluppo del mercato interno dei servizi postali comunitari e il miglioramento della qualità del servizio (GU L 15 del 21.1.1998, pag. 14).

([8]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

([9]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

(18) Al fine di garantire una panoramica chiara dei soggetti che rientrano nell'ambito di applicazione della presente direttiva, gli Stati membri dovrebbero definire un elenco dei soggetti essenziali ed importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio. A tal fine, gli Stati membri dovrebbero imporre ai soggetti di trasmettere alle autorità competenti almeno le seguenti informazioni, vale a dire il nome, l'indirizzo e i recapiti aggiornati, compresi gli indirizzi di posta elettronica, le serie IP e i numeri di telefono del soggetto, se del caso, il settore e il sottosettore pertinente di cui agli allegati e, ove applicabile, un elenco degli Stati membri in cui prestano servizi che rientrano nell'ambito di applicazione della presente direttiva. A tal fine, la Commissione, assistita dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA), dovrebbe fornire senza indebito ritardo orientamenti e modelli relativi all'obbligo di fornire informazioni. Per facilitare la compilazione e l'aggiornamento dell'elenco dei soggetti essenziali e importanti, nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio, gli Stati membri dovrebbero poter istituire meccanismi nazionali che consentano ai soggetti di registrarsi. Qualora esistano registri a livello nazionale, gli Stati membri possono decidere in merito ai meccanismi appropriati che consentono di identificare i soggetti che rientrano nell'ambito di applicazione della presente direttiva.

(19) Gli Stati membri dovrebbero essere tenuti a comunicare alla Commissione almeno il numero di soggetti essenziali e importanti per ciascun settore e sottosettore di cui agli allegati, nonché le informazioni pertinenti sul numero di soggetti identificati e sulla disposizione, tra quelle previste dalla presente direttiva, sulla base della quale sono stati identificati, e la tipologia dei servizi che forniscono. Gli Stati membri sono incoraggiati a scambiare con la Commissione informazioni sui soggetti essenziali e importanti e, in caso di incidente di cibersicurezza su vasta scala, informazioni pertinenti quali il nome del soggetto interessato.

(20) La Commissione, in collaborazione con il gruppo di cooperazione e previa consultazione dei pertinenti portatori di interessi, dovrebbe fornire orientamenti relativi all'attuazione dei criteri applicabili alle microimprese e alle piccole imprese per valutare se rientrino nell'ambito di applicazione della presente direttiva. La Commissione dovrebbe inoltre garantire che vengano forniti orientamenti adeguati alle microimprese e alle piccole imprese rientranti nell'ambito di applicazione della presente direttiva. La Commissione, con il sostegno degli Stati membri, dovrebbe fornire alle microimprese e alle piccole imprese informazioni al riguardo.

(21) La Commissione potrebbe fornire orientamenti volti ad assistere gli Stati membri nell'attuazione delle disposizioni della presente direttiva sull'ambito di applicazione e nella valutazione della proporzionalità delle misure da adottare ai sensi della presente direttiva, segnatamente per quanto riguarda i soggetti con modelli di business o contesti operativi complessi, in base ai quali un soggetto può soddisfare contemporaneamente i criteri assegnati ai soggetti essenziali e importanti o può svolgere simultaneamente attività che rientrano in parte nell'ambito di applicazione della presente direttiva e in parte ne sono escluse.

(22) La presente direttiva stabilisce lo scenario di riferimento per le misure di gestione dei rischi di cibersicurezza e gli obblighi di segnalazione in tutti i settori che rientrano nel suo ambito di applicazione. Al fine di evitare la frammentazione delle disposizioni in materia di cibersicurezza contenute negli atti giuridici dell'Unione, allorché ulteriori atti giuridici settoriali dell'Unione relativi alle misure di gestione dei rischi di cibersicurezza e agli obblighi di segnalazione siano ritenuti necessari per garantire un elevato livello di cibersicurezza in tutta l'Unione, la Commissione dovrebbe valutare se tali ulteriori disposizioni possano essere stabilite in un atto di esecuzione ai sensi della presente direttiva. Qualora tali atti di esecuzione non siano adeguati a detto scopo, gli atti giuridici settoriali dell'Unione potrebbero contribuire a garantire un livello elevato di cibersicurezza in tutta l'Unione, tenendo pienamente conto delle specificità e delle complessità dei settori interessati. A tal fine, la presente direttiva non preclude l'adozione di ulteriori atti giuridici settoriali dell'Unione riguardanti le misure di gestione dei rischi di cibersicurezza e gli obblighi di segnalazione che tengano debitamente conto della necessità di un quadro di sicurezza informatica globale e coerente. La presente direttiva lascia impregiudicate le competenze di esecuzione esistenti conferite alla Commissione in una serie di settori, tra cui i trasporti e l'energia.

(23) Qualora un atto giuridico settoriale dell'Unione faccia obbligo ai soggetti essenziali o importanti di adottare misure di gestione dei rischi di cibersicurezza o di notificare incidenti significativi, e nella misura in cui gli effetti di tali obblighi siano almeno equivalenti a quelli degli obblighi di cui alla presente direttiva, tali disposizioni, comprese

quelle relative alla vigilanza e all'esecuzione, si applicano a detti soggetti. Qualora un atto giuridico settoriale dell'Unione non contempli tutti i soggetti di un settore specifico che rientra nell'ambito di applicazione della presente direttiva, le pertinenti disposizioni della presente direttiva dovrebbero continuare ad applicarsi ai soggetti non contemplati da tale atto.

(24) Qualora le disposizioni di un atto giuridico settoriale dell'Unione impongano ai soggetti essenziali o importanti di rispettare gli obblighi di effetto almeno equivalente agli obblighi di segnalazione di cui alla presente direttiva, è opportuno garantire la coerenza e l'efficacia del trattamento delle notifiche degli incidenti. A tal fine, le disposizioni in materia di notifica degli incidenti dell'atto giuridico settoriale dell'Unione dovrebbero fornire ai CSIRT, alle autorità competenti o ai punti di contatto unici di cui alla presente direttiva un accesso immediato alle notifiche degli incidenti di cibersicurezza (punti di contatto unici) presentate in conformità dell'atto giuridico settoriale dell'Unione. In particolare, tale accesso immediato può essere garantito se le notifiche degli incidenti sono trasmesse senza indebito ritardo al CSIRT, all'autorità competente o al punto di contatto unico ai sensi della presente direttiva. Se del caso, gli Stati membri dovrebbero istituire un meccanismo di segnalazione automatica e diretta, che garantisca la condivisione sistematica e immediata delle informazioni con i CSIRT, le autorità competenti o il punto di contatto unico per quanto riguarda la gestione di tali notifiche di incidenti. Al fine di semplificare la comunicazione e di attuare il meccanismo di segnalazione automatica e diretta, gli Stati membri potrebbero, conformemente all'atto giuridico settoriale dell'Unione, utilizzare un punto di accesso unico.

(25) Gli atti giuridici settoriali dell'Unione che prevedono misure di gestione dei rischi di cibersicurezza o obblighi di segnalazione di effetto almeno equivalente a quelli stabiliti nella presente direttiva potrebbero prevedere che le autorità competenti ai sensi di tali atti esercitino i loro poteri di vigilanza ed esecuzione in relazione a tali misure o obblighi con l'assistenza delle autorità competenti ai sensi della presente direttiva. Le autorità competenti interessate potrebbero stabilire modalità di cooperazione a tale scopo. Tali modalità di cooperazione potrebbero precisare, tra l'altro, le procedure relative al coordinamento delle attività di vigilanza, tra cui le procedure di indagine e di ispezione in loco conformemente al diritto nazionale e un meccanismo per lo scambio di informazioni pertinenti in materia di vigilanza ed esecuzione tra autorità competenti, compreso l'accesso alle informazioni relative alla cibersicurezza richieste dalle autorità competenti ai sensi della presente direttiva.

(26) Qualora atti giuridici settoriali dell'Unione impongano o forniscano incentivi a soggetti affinché notifichino minacce informatiche significative, gli Stati membri dovrebbero altresì incoraggiare la condivisione di minacce informatiche significative con i CSIRT, le autorità competenti o i punti di contatto unici ai sensi della presente direttiva, al fine di garantire un maggiore livello di consapevolezza di tali organismi in merito al panorama delle minacce informatiche e consentire loro di rispondere in modo efficace e tempestivo qualora tali minacce si concretizzino.

(27) I futuri atti giuridici settoriali dell'Unione dovrebbero tenere debitamente conto delle definizioni e del quadro di vigilanza e applicazione previsto dalla presente direttiva.

(28) Il regolamento UE 2022/2554 del Parlamento europeo e del Consiglio ([10]) dovrebbe essere considerato un atto giuridico settoriale dell'Unione in relazione alla presente direttiva per quanto riguarda i soggetti del settore finanziario. Invece delle disposizioni stabilite nella presente direttiva dovrebbero applicarsi quelle del regolamento (UE) 2022/2554 relative alle misure di gestione del rischio relativo alle tecnologie dell'informazione e della comunicazione (TIC), alla gestione degli incidenti relativi alle TIC e, in particolare, alla segnalazione degli incidenti gravi relativi alle TIC, nonché alle prove di resilienza operativa digitale, agli accordi di condivisione delle informazioni e ai rischi di terze parti relativi alle TIC. Gli Stati membri non dovrebbero pertanto applicare le disposizioni della presente direttiva riguardanti gli obblighi di gestione e segnalazione dei rischi di cibersicurezza e la vigilanza e l'esecuzione ai soggetti finanziari contemplati dal regolamento (UE) 2022/2554 Al tempo stesso è importante mantenere una solida relazione e lo scambio di informazioni con il settore finanziario a norma della presente direttiva. A tal fine, il regolamento (UE) 2022/2554 consente alle autorità europee di vigilanza (AEV) e alle autorità competenti a norma di tale regolamento di partecipare alle attività del gruppo di cooperazione, di scambiare informazioni e cooperare con i punti di contatto unici, nonché con i CSIRT e le autorità competenti ai sensi della presente direttiva. Le autorità competenti a norma del regolamento (UE) 2022/2554 dovrebbero inoltre trasmettere

([10]) Regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (Cfr. pag. 1 della presente Gazzetta ufficiale).

i dettagli degli incidenti più gravi connessi alle TIC e, se del caso, delle minacce informatiche significative ai CSIRT, alle autorità competenti o ai punti di contatto unici nazionali a norma della presente direttiva. Ciò è possibile fornendo accesso immediato alle notifiche di incidenti e la loro trasmissione diretta o attraverso un unico punto di accesso. Gli Stati membri dovrebbero inoltre continuare a includere il settore finanziario nelle loro strategie di cibersicurezza e i CSIRT nazionali possono contemplare il settore finanziario nelle loro attività.

(29) Al fine di evitare lacune o duplicazioni per quanto riguarda gli obblighi di cibersicurezza imposti ai soggetti del settore dell'aviazione, le autorità nazionali designate a norma dei regolamenti (CE) n. 300/2008 ([11]) e (UE) 2018/1139 ([12]) del Parlamento europeo e del Consiglio e le autorità competenti a norma della presente direttiva dovrebbero cooperare in relazione all'attuazione delle misure di gestione dei rischi di cibersicurezza e alla vigilanza della conformità con tali misure a livello nazionale. La conformità di un soggetto con i requisiti di sicurezza di cui ai regolamenti (CE) n. 300/2008 e (UE) 2018/1139 e ai pertinenti atti delegati e di esecuzione adottati a norma di tali regolamenti potrebbe essere considerata dalle autorità competenti ai sensi della presente direttiva una conformità ai corrispondenti requisiti di cui alla presente direttiva.

(30) In considerazione delle interconnessioni tra la cibersicurezza e la sicurezza fisica dei soggetti, dovrebbe essere garantito un approccio coerente tra la direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio ([13]) e la presente direttiva. A tal fine, i soggetti identificati come soggetti critici a norma della direttiva (UE) 2022/2557 dovrebbero essere considerati soggetti essenziali a norma della presente direttiva. Inoltre, ciascuno Stato membro dovrebbe provvedere affinché la propria strategia nazionale in materia di cibersicurezza preveda un quadro strategico per il rafforzamento del coordinamento all'interno di detto Stato membro tra le proprie autorità competenti a norma della presente direttiva e quelle previste dalla direttiva (UE) 2022/2557 nel contesto della condivisione delle informazioni sui rischi, sulle minacce informatiche e sugli incidenti nonché sui rischi, sulle minacce e sugli incidenti non informatici e dello svolgimento di compiti di vigilanza. Le autorità competenti a norma della presente direttiva e della direttiva (UE) 2022/2557 dovrebbero cooperare e scambiarsi informazioni senza indebito ritardo, in particolare per quanto riguarda l'individuazione dei soggetti critici, delle minacce informatiche, dei rischi e degli incidenti nonché per quanto riguarda i rischi, le minacce e gli incidenti non informatici che interessano i soggetti critici, tra cui le misure di cibersicurezza e fisiche adottate dai soggetti critici nonché i risultati delle attività di vigilanza svolte riguardo a tali soggetti.

Inoltre, al fine di razionalizzare le attività di vigilanza tra le autorità competenti a norma della presente direttiva e della direttiva (UE) 2022/2557 e di ridurre al minimo gli oneri amministrativi per i soggetti interessati, tali autorità competenti dovrebbero adoperarsi per armonizzare i modelli di notifica degli incidenti e le procedure di vigilanza. Se del caso, le autorità competenti a norma della direttiva (UE) 2022/2557 dovrebbero poter chiedere alle autorità competenti ai sensi della presente direttiva di esercitare i propri poteri di vigilanza e di esecuzione in relazione a un soggetto che è individuato come soggetto critico ai sensi della direttiva (UE) 2022/2557 A tal fine, le autorità competenti a norma della presente direttiva e della direttiva (UE) 2022/2557 dovrebbero cooperare e scambiarsi informazioni, ove possibile in tempo reale.

(31) I soggetti appartenenti al settore delle infrastrutture digitali sono essenzialmente basati su sistemi informatici e di rete e pertanto gli obblighi loro imposti a norma della presente direttiva dovrebbero riguardare in modo globale la sicurezza fisica di tali sistemi nell'ambito delle loro misure di gestione dei rischi di cibersicurezza e obblighi di segnalazione. Poiché tali materie sono disciplinate dalla presente direttiva, gli obblighi di cui ai capi III, IV e VI della direttiva (UE) 2022/2557 non si applicano a detti soggetti.

([11]) Regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, che istituisce norme comuni per la sicurezza dell'aviazione civile e che abroga il regolamento (CE) n. 2320/2002 (GU L 97 del 9.4.2008, pag. 72).

([12]) Regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio, del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che modifica i regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il regolamento (CEE) n. 3922/91 del Consiglio (GU L 212 del 22.8.2018, pag. 1).

([13]) Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio del 14 dicembre 2022 sulla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE (cfr. pag. 164 della presente Gazzetta ufficiale).

(32) Sostenere e preservare un sistema dei nomi di dominio affidabile, resiliente e sicuro sono fattori chiave per mantenere l'integrità di internet e sono essenziali per il suo funzionamento costante e stabile, da cui dipendono l'economia e la società digitali. La presente direttiva dovrebbe applicarsi ai server dei nomi di dominio di primo livello (*top level domain* — TLD) e ai fornitori di servizi DNS che si intendono come soggetti che forniscono servizi di risoluzione dei nomi di dominio ricorsivi accessibili al pubblico per gli utenti finali di internet o ai servizi di risoluzione autorevoli dei nomi di dominio. La presente direttiva non dovrebbe applicarsi ai server dei nomi radice (*root name server*).

(33) I servizi di cloud computing dovrebbero comprendere servizi digitali che consentono l'amministrazione su richiesta di un pool scalabile ed elastico di risorse di calcolo condivisibili e l'ampio accesso remoto a quest'ultimo, anche quando tali risorse sono distribuite in varie ubicazioni. Le risorse di calcolo comprendono risorse come reti, server o altre infrastrutture, sistemi operativi, software, archiviazione, applicazioni e servizi. I modelli di servizio del cloud computing comprendono, tra gli altri, il servizio a livello di infrastruttura (IaaS), il servizio a livello di piattaforma (PaaS), il servizio a livello di software (SaaS) e il servizio a livello di rete (NaaS). I modelli di distribuzione del cloud computing dovrebbero comprendere il cloud privato, di comunità, pubblico e ibrido. I servizi di cloud computing e di distribuzione hanno lo stesso significato dei termini di servizio e dei modelli di distribuzione di cui alla norma ISO/IEC 17788:2014. La capacità dell'utente di cloud computing di provvedere unilateralmente all'autofornitura di capacità di calcolo, come il tempo di utilizzo di un server o lo spazio di archiviazione in rete, senza alcuna interazione umana da parte del fornitore di servizi di cloud computing potrebbe essere descritta come «amministrazione su richiesta».

L'espressione «ampio accesso remoto» (*broad network access*) è utilizzata per descrivere il fatto che le capacità cloud sono fornite sulla rete e accessibili attraverso meccanismi che promuovono l'uso di piattaforme client eterogenee leggere o pesanti (compresi telefoni cellulari, tablet, computer portatili e workstation). Il termine «scalabile» si riferisce alle risorse informatiche che sono assegnate in modo flessibile dal fornitore di servizi nel cloud, indipendentemente dall'ubicazione geografica delle risorse, per gestire le fluttuazioni della domanda. L'espressione «pool elastico» è usata per descrivere le risorse di calcolo fornite e rilasciate in base alla domanda, al fine di aumentare e diminuire rapidamente le risorse disponibili in base al carico di lavoro. Il termine «condivisibile» è usato per descrivere le risorse di calcolo che sono fornite a una molteplicità di utenti che condividono un accesso comune al servizio, mentre l'elaborazione è effettuata separatamente per ciascun utente anche se il servizio è fornito a partire dalla stessa apparecchiatura elettronica. Il termine «distribuito» è usato per descrivere le risorse di calcolo che si trovano su diversi computer o dispositivi collegati in rete e che comunicano e si coordinano tra di loro mediante il passaggio di messaggi.

(34) Dato l'emergere di tecnologie innovative e di nuovi modelli di business, si prevede che compariranno sul mercato interno nuovi modelli di servizio e di distribuzione del cloud computing in risposta all'evoluzione delle esigenze dei clienti. In tale contesto, i servizi di cloud computing possono essere forniti in una forma altamente distribuita, anche più vicina al luogo in cui i dati vengono generati o raccolti, passando così dal modello tradizionale a un modello altamente distribuito (*edge computing*).

(35) È possibile che i servizi offerti dai fornitori di servizi di data center non siano sempre forniti sotto forma di servizi di cloud computing. È pertanto possibile che i data center non facciano sempre parte dell'infrastruttura di cloud computing. Al fine di gestire tutti i rischi posti alla sicurezza dei sistemi informatici e di rete, la presente direttiva dovrebbe pertanto applicarsi ai fornitori di servizi di data center che non sono servizi di cloud computing. Ai fini della presente direttiva, il termine «servizio di data center» dovrebbe applicarsi alla fornitura di un servizio che comprende strutture, o gruppi di strutture, dedicate a ospitare, interconnettere e far funzionare in modo centralizzato apparecchiature informatiche e di rete che forniscono servizi di conservazione, elaborazione e trasporto di dati insieme a tutti gli impianti e le infrastrutture per la distribuzione dell'energia e il controllo ambientale. Il termine «servizio di data center» non si dovrebbe applicare ai data center interni e aziendali posseduti e gestiti per fini propri dal soggetto interessato.

(36) Le attività di ricerca svolgono un ruolo fondamentale nello sviluppo di nuovi prodotti e processi. Molte di tali attività sono svolte da soggetti che condividono, diffondono o sfruttano i risultati della loro ricerca per scopi commerciali. Tali soggetti possono pertanto essere attori importanti nelle catene del valore, il che rende la sicurezza dei loro sistemi informatici e di rete parte integrante della cibersicurezza globale del mercato interno. Gli organismi di ricerca dovrebbero essere intesi come soggetti che concentrano la parte essenziale delle loro attività sullo

svolgimento di ricerca applicata o sviluppo sperimentale, ai sensi del Manuale di Frascati 2015 dell'Organizzazione per la cooperazione e lo sviluppo economici: «Linee guida per la raccolta e la trasmissione di dati sulla ricerca e lo sviluppo sperimentale», al fine di sfruttarne i risultati a fini commerciali quali la produzione o lo sviluppo di un prodotto o di un processo, la prestazione di un servizio, o la loro commercializzazione.

(37) Le crescenti interdipendenze sono il risultato di una rete di fornitura di servizi sempre più transfrontaliera e interdipendente che utilizza infrastrutture chiave in tutta l'Unione in settori quali quelli dell'energia, dei trasporti, delle infrastrutture digitali, delle acque potabili e reflue, della sanità, di determinati aspetti della pubblica amministrazione, nonché dello spazio, per quanto riguarda la fornitura di determinati servizi che dipendono da infrastrutture di terra possedute, gestite e utilizzate dagli Stati membri o da soggetti privati, ad esclusione, pertanto, delle infrastrutture possedute, gestite o utilizzate dall'Unione o per suo conto nell'ambito del suo programma spaziale. Tali interdipendenze implicano che qualsiasi perturbazione, anche se inizialmente limitata a un soggetto o a un settore, possa avere effetti a cascata più ampi, con potenziali ripercussioni negative di ampia portata e di lunga durata sulla fornitura di servizi in tutto il mercato interno. Gli attacchi informatici intensificatisi durante la pandemia di COVID-19 hanno mostrato la vulnerabilità di società sempre più interdipendenti di fronte a rischi di bassa probabilità.

(38) In considerazione delle differenze esistenti tra le strutture di governance nazionali e al fine di salvaguardare gli accordi settoriali già esistenti o gli organismi di vigilanza e di regolamentazione dell'Unione, è opportuno che gli Stati membri abbiano la facoltà di designare o istituire una o più autorità nazionali competenti responsabili per la cibersicurezza e per i compiti di supervisione ai sensi della presente direttiva.

(39) Al fine di agevolare la cooperazione e la comunicazione transfrontaliere tra autorità e permettere che la presente direttiva sia attuata efficacemente, è necessario che ogni Stato membro designi un punto di contatto unico nazionale incaricato di coordinare le questioni relative alla sicurezza dei sistemi informatici e di rete e la cooperazione transfrontaliera a livello dell'Unione.

(40) I punti di contatto unici dovrebbero garantire un'efficace cooperazione transfrontaliera con le autorità competenti di altri Stati membri e, se del caso, con la Commissione e l'ENISA. I punti di contatto unici dovrebbero pertanto essere incaricati di trasmettere le notifiche di incidenti significativi con impatto transfrontaliero ai punti di contatto unici degli altri Stati membri interessati, su richiesta del CSIRT o dell'autorità competente. A livello nazionale, i punti di contatto unici dovrebbero consentire un'agevole cooperazione intersettoriale con le altre autorità competenti. I punti di contatto unici potrebbero anche ricevere dalle autorità competenti, a norma del regolamento (UE) 2022/2554, le pertinenti informazioni sugli incidenti riguardanti i soggetti del settore finanziario, che essi dovrebbero poter trasmettere, a seconda dei casi, ai CSIRT o alle autorità competenti a norma della presente direttiva.

(41) Gli Stati membri dovrebbero essere adeguatamente dotati delle capacità tecniche e organizzative necessarie a prevenire e rilevare gli incidenti e i rischi, nonché a rispondervi e a mitigare il loro impatto. Gli Stati membri dovrebbero pertanto designare uno o più CSIRT ai sensi della presente direttiva e garantire che essi dispongano di risorse e capacità tecniche adeguate. I CSIRT dovrebbero rispondere ai requisiti stabiliti nella presente direttiva al fine di garantire l'esistenza di capacità efficaci e compatibili per far fronte ai rischi e agli incidenti e garantire un'efficiente collaborazione a livello di Unione. Gli Stati membri dovrebbero poter designare come CSIRT le squadre di pronto intervento informatico (CERT) esistenti. Al fine di rafforzare il rapporto di fiducia tra i soggetti e i CSIRT, nei casi in cui un CSIRT faccia parte di un'autorità competente, gli Stati membri dovrebbero poter prendere in considerazione la separazione funzionale tra i compiti operativi svolti dai CSIRT, in particolare per quanto riguarda la condivisione delle informazioni e l'assistenza fornita ai soggetti, e le attività di vigilanza delle autorità competenti.

(42) I CSIRT sono incaricati della gestione degli incidenti. Ciò comprende il trattamento di grandi volumi di dati talvolta sensibili. Gli Stati membri dovrebbero garantire che i CSIRT dispongano di un'infrastruttura per la condivisione e il trattamento delle informazioni, nonché di personale ben attrezzato, che garantisca la riservatezza e l'affidabilità delle loro operazioni. I CSIRT potrebbero anche adottare codici di condotta a tale riguardo.

(43) Per quanto riguarda i dati personali, i CSIRT dovrebbero poter fornire, in conformità del regolamento (UE) 2016/679, su richiesta di un soggetto essenziale o importante, una scansione proattiva dei sistemi informatici e di rete utilizzati per la fornitura dei servizi del soggetto. Se del caso, gli Stati membri dovrebbero mirare a garantire un pari livello di capacità tecniche per tutti i CSIRT settoriali. Gli Stati membri dovrebbero poter chiedere l'assistenza dell'ENISA nello sviluppo di CSIRT nazionali.

(44) I CSIRT dovrebbero avere la capacità, su richiesta di un soggetto essenziale o importante, di monitorare le risorse di quest'ultimo connesse a internet, sia in loco che a distanza, per identificare, comprendere e gestire i rischi organizzativi generali del soggetto con riguardo alle compromissioni della catena di approvvigionamento individuate di recente o le vulnerabilità critiche. Il soggetto dovrebbe essere incoraggiato a comunicare al CSIRT se gestisce un'interfaccia gestionale privilegiata, poiché ciò potrebbe incidere sulla velocità delle azioni di mitigazione.

(45) Data l'importanza della cooperazione internazionale in materia di cibersicurezza, i CSIRT dovrebbero poter partecipare a reti di cooperazione internazionale, oltre alla rete di CSIRT istituita dalla presente direttiva. Pertanto, ai fini dello svolgimento dei loro compiti, i CSIRT e le autorità competenti dovrebbero poter scambiare informazioni, compresi i dati personali, con team nazionali di risposta agli incidenti per la sicurezza informatica o autorità competenti di paesi terzi, purché siano soddisfatte le condizioni previste dal diritto dell'Unione in materia di protezione dei dati per i trasferimenti di dati personali verso paesi terzi, tra cui quelle a norma dell'articolo 49 del regolamento (UE) 2016/679.

(46) È essenziale garantire risorse adeguate per il conseguimento degli obiettivi della presente direttiva e consentire alle autorità competenti e ai CSIRT di lo svolgimento dei compiti ivi stabiliti. Gli Stati membri possono introdurre a livello nazionale un meccanismo di finanziamento per coprire le spese necessarie in relazione allo svolgimento dei compiti degli enti pubblici responsabili della cibersicurezza nello Stato membro ai sensi della presente direttiva. Tale meccanismo dovrebbe essere conforme al diritto dell'Unione, essere proporzionato e non discriminatorio e dovrebbe tenere conto dei diversi approcci nella fornitura di servizi sicuri.

(47) La rete di CSIRT dovrebbe continuare a contribuire al rafforzamento della fiducia e a promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri. Al fine di rafforzare la cooperazione operativa a livello di Unione, la rete di CSIRT dovrebbe prendere in considerazione la possibilità di invitare a partecipare ai suoi lavori organismi e agenzie dell'Unione coinvolti nella politica in materia di cibersicurezza, quali Europol.

(48) Al fine di conseguire e mantenere un livello elevato di cibersicurezza, le strategie nazionali per la cibersicurezza richieste dalla presente direttiva dovrebbero comprendere quadri coerenti che forniscano obiettivi e priorità strategici nel settore della cibersicurezza e la governance per conseguirli. Tali strategie possono essere rappresentate da uno o più strumenti legislativi o non legislativi.

(49) Le politiche di igiene informatica (*cyber hygiene*) pongono le fondamenta per la protezione delle infrastrutture delle reti e dei sistemi di informazione, dell'hardware, del software e della sicurezza delle applicazioni online, nonché dei dati aziendali o degli utenti finali su cui si basano i soggetti. Le politiche di igiene informatica, che comprendono uno scenario di riferimento comune delle prassi, tra cui gli aggiornamenti del software e dell'hardware, i cambi di password, la gestione delle nuove installazioni, la limitazione degli account di accesso a livello di amministratore e il backup dei dati, consentono un quadro proattivo di preparazione e sicurezza e protezione generale in caso di incidenti o minacce informatiche. L'ENISA dovrebbe monitorare e analizzare le politiche di igiene informatica degli Stati membri.

(50) La consapevolezza in materia di cibersicurezza e l'igiene informatica sono essenziali per migliorare il livello di cibersicurezza all'interno dell'Unione, in particolare alla luce del crescente numero di dispositivi connessi sempre più utilizzati negli attacchi informatici. È opportuno adoperarsi per migliorare la consapevolezza generale dei rischi connessi a tali dispositivi; al contempo, valutazioni a livello di Unione potrebbero contribuire a garantire una comprensione comune di tali rischi nel mercato interno.

(51) Gli Stati membri dovrebbero incoraggiare l'uso di ogni tecnologia innovativa, compresa l'intelligenza artificiale, il cui utilizzo potrebbe migliorare l'individuazione e la prevenzione degli attacchi informatici, consentendo di destinare in modo più efficace risorse per affrontare gli attacchi informatici. Gli Stati membri dovrebbero pertanto incoraggiare, nelle loro strategie nazionali per la cibersicurezza, le attività di ricerca e sviluppo volte a facilitare l'uso di tali tecnologie, in particolare quelle relative agli strumenti automatizzati o semiautomatizzati nella cibersicurezza, e, se del caso, la condivisione dei dati necessari per formare gli utenti di tali tecnologie e migliorarle. L'utilizzo di tutte le tecnologie innovative, compresa l'intelligenza artificiale, dovrebbe rispettare il diritto dell'Unione in materia di protezione dei dati, compresi i principi di protezione dei dati con riguardo all'accuratezza, alla minimizzazione dei dati, all'equità e alla trasparenza, nonché alla sicurezza dei dati, come la più recente crittografia. I requisiti di protezione dei dati fin dalla progettazione e predefiniti di cui al regolamento (UE) 2016/679 dovrebbero essere pienamente rispettati.

(52) Gli strumenti e le applicazioni di cibersicurezza open source possono contribuire a un livello più elevato di apertura e avere un impatto positivo sull'efficienza dell'innovazione industriale. Gli standard aperti facilitano l'interoperabilità tra gli strumenti di sicurezza, a vantaggio della sicurezza dei portatori di interessi industriali. Gli strumenti e le applicazioni open source in materia di cibersicurezza possono mobilitare la più ampia comunità di sviluppatori, consentendo la diversificazione dei fornitori. Una fonte aperta può portare a un processo di verifica più trasparente degli strumenti connessi alla cibersicurezza e a un processo di individuazione delle vulnerabilità guidato dalla comunità. Gli Stati membri dovrebbero pertanto poter promuovere l'utilizzo di software open source e standard aperti, perseguendo politiche relative all'uso di dati aperti e open source come parte della sicurezza attraverso la trasparenza. Le politiche che promuovono l'introduzione e l'uso sostenibile di strumenti di sicurezza informatica open source rivestono particolare importanza per le piccole e medie imprese che devono sostenere notevoli costi per l'attuazione, e che potrebbero essere minimizzati riducendo la necessità di applicazioni o strumenti specifici.

(53) I servizi pubblici sono sempre più collegati alle reti digitali nelle città per migliorare le reti di trasporto urbano, l'approvvigionamento idrico e gli impianti di smaltimento dei rifiuti, nonché aumentare l'efficienza dell'illuminazione e del riscaldamento degli edifici. Tali servizi pubblici digitali sono vulnerabili agli attacchi informatici e corrono il rischio, in caso di successo di un attacco informatico, di danneggiare i cittadini su larga scala a causa della loro interconnessione. Gli Stati membri dovrebbero elaborare una politica che affronti lo sviluppo di tali città connesse o intelligenti, così come i loro potenziali effetti sulla società, nell'ambito della loro strategia nazionale per la cibersicurezza.

(54) Negli ultimi anni l'Unione ha dovuto far fronte a un aumento esponenziale di attacchi ransomware, in cui i malware criptano dati e sistemi e chiedono il pagamento di un riscatto per il rilascio. La frequenza e la gravità crescenti degli attacchi ransomware possono essere determinate da diversi fattori, come i diversi modelli di attacco, i modelli criminali commerciali che considerano il «ransomware come un servizio» e le criptovalute, le richieste di riscatto e l'aumento degli attacchi contro la catena di approvvigionamento. Gli Stati membri dovrebbero sviluppare politiche, come parte delle loro strategie nazionali per la cibersicurezza, che affrontino l'aumento degli attacchi ransomware.

(55) I partenariati pubblico-privato (PPP) nell'ambito della cibersicurezza possono fornire il quadro appropriato per lo scambio di conoscenze, la condivisione delle migliori pratiche e la creazione di un livello comune di comprensione tra i portatori di interessi. Gli Stati membri dovrebbero promuovere politiche che sostengano l'istituzione di PPP specifici della cibersicurezza. Tali politiche dovrebbero chiarire, tra l'altro, l'ambito di applicazione e i portatori di interessi coinvolti, il modello di governance, le opzioni di finanziamento disponibili e l'interazione tra i portatori di interessi partecipanti con riguardo ai PPP. I PPP possono sfruttare le competenze dei soggetti del settore privato per assistere le autorità competenti nello sviluppo di servizi e processi all'avanguardia, compresi, lo scambio di informazioni, i preallarmi, le esercitazioni su minacce e incidenti informatici, la gestione delle crisi e la pianificazione della resilienza.

(56) Gli Stati membri dovrebbero, nelle loro strategie nazionali per la cibersicurezza, rispondere alle esigenze specifiche in materia di cibersicurezza delle piccole e medie imprese. Le piccole e medie imprese rappresentano nell'Unione, un'ampia percentuale del mercato industriale e commerciale e spesso faticano ad adattarsi alle nuove pratiche commerciali in un mondo sempre più connesso e all'ambiente digitale, con dipendenti che lavorano da casa e imprese che sono gestite in misura crescente online. Alcune piccole e medie imprese si confrontano con sfide specifiche in materia di cibersicurezza, come la scarsa consapevolezza informatica, la mancanza di sicurezza informatica a distanza, l'elevato costo delle soluzioni di cibersicurezza e l'aumento del livello di minaccia, dovuto ad esempio ai ransomware, aspetti in relazione ai quali dovrebbero ricevere linee guida e assistenza. Le piccole e medie imprese stanno diventando sempre di più il bersaglio di attacchi nella catena di approvvigionamento a causa delle loro misure meno rigorose di gestione del rischio di cibersicurezza e di gestione degli attacchi, nonché della limitata disponibilità di risorse destinate alla sicurezza. Tali attacchi della catena di approvvigionamento non solo hanno un

impatto sulle piccole e medie imprese e sulle loro operazioni isolatamente, ma possono anche avere un effetto a cascata su attacchi più gravi nei confronti di soggetti di cui sono fornitori. Gli Stati membri dovrebbero, attraverso le loro strategie nazionali in materia di cibersicurezza, aiutare le piccole e medie imprese fronteggiare le sfide a cui sono sottoposte nelle loro catene di approvvigionamento. Gli Stati membri dovrebbero disporre di un punto di contatto per le piccole e medie imprese a livello nazionale o regionale, che fornisca linee guida e assistenza alle piccole e medie imprese, o le diriga verso gli organismi appropriati per l'orientamento e l'assistenza in materia di cibersicurezza. Gli Stati membri sono altresì incoraggiati a offrire servizi come la configurazione e la registrazione di siti internet, che abilitino le microimprese e le piccole imprese che non dispongono di tali capacità.

(57) Gli Stati membri dovrebbero adottare politiche volte a promuovere la protezione informatica attiva nell'ambito delle loro strategie nazionali per la cibersicurezza, come parte di una strategia difensiva più ampia. Anziché reagire, la protezione informatica attiva consiste nel prevenire, individuare, monitorare, analizzare e attenuare in maniera attiva le violazioni della sicurezza della rete, in combinazione con il ricorso a capacità predisposte all'interno e all'esterno della rete vittima. Ciò potrebbe includere l'offerta da parte degli Stati membri di servizi o strumenti gratuiti a determinati soggetti, tra cui controlli self-service, strumenti di rilevamento e servizi di rimozione. La capacità di condividere e comprendere in modo rapido e automatico informazioni e analisi riguardanti le minacce, segnalazioni di attività informatiche e azioni di risposta è fondamentale per consentire un'unità di sforzi al fine di prevenire, individuare, affrontare e bloccare con successo gli attacchi informatici nei confronti dei sistemi informatici e di rete. La protezione informatica attiva si basa su una strategia difensiva, che esclude misure offensive.

(58) Poiché lo sfruttamento delle vulnerabilità nei sistemi informatici e di rete può causare perturbazioni e danni significativi, la rapida individuazione e correzione di tali vulnerabilità è un fattore importante per la riduzione dei rischi. I soggetti che sviluppano o amministrano tali sistemi informatici e di rete dovrebbero pertanto stabilire procedure adeguate per gestire le vulnerabilità nel momento in cui vengono scoperte. Poiché le vulnerabilità sono spesso rilevate e divulgate da terzi, il fabbricante o fornitore di prodotti TIC o servizi TIC dovrebbe anche mettere in atto le procedure necessarie per ricevere informazioni sulla vulnerabilità da terzi. A tale riguardo, le norme internazionali ISO/IEC 30111 e ISO/IEC 29147 forniscono orientamenti sulla gestione delle vulnerabilità e sulla divulgazione delle vulnerabilità. Al fine di facilitare il contesto della divulgazione volontaria delle vulnerabilità, è particolarmente importante rafforzare il coordinamento tra persone fisiche e giuridiche segnalanti e i fabbricanti o fornitori di prodotti o servizi TIC. La divulgazione coordinata delle vulnerabilità consiste in un processo strutturato attraverso il quale le vulnerabilità sono segnalate al fabbricante o al fornitore dei prodotti TIC o dei servizi TIC potenzialmente vulnerabili, in modo tale da consentire loro di diagnosticarle ed eliminarle prima che informazioni dettagliate in merito siano divulgate a terzi o al pubblico. La divulgazione coordinata delle vulnerabilità dovrebbe comprendere anche il coordinamento tra la persona fisica o giuridica segnalante e il fabbricante o il fornitore di prodotti TIC o servizi TIC potenzialmente vulnerabili, per quanto riguarda i tempi per la risoluzione e la pubblicazione delle vulnerabilità.

(59) La Commissione, l'ENISA e gli Stati membri dovrebbero continuare a promuovere gli allineamenti agli standard internazionali e alle migliori prassi industriali esistenti nel settore della gestione dei rischi, ad esempio nei settori delle valutazioni della sicurezza della catena di approvvigionamento, della condivisione delle informazioni e della divulgazione delle vulnerabilità.

(60) Gli Stati membri, in cooperazione con l'ENISA, dovrebbero adottare misure volte a facilitare la divulgazione coordinata delle vulnerabilità stabilendo una politica nazionale pertinente. Nell'ambito di tale politica nazionale, gli Stati membri dovrebbero mirare ad affrontare, nella misura del possibile, le sfide incontrate dagli esperti che fanno ricerca sulle vulnerabilità, compresa la loro potenziale esposizione alla responsabilità penale, conformemente al diritto nazionale. Dato che in alcuni Stati membri le persone fisiche e giuridiche che fanno ricerca sulle vulnerabilità potrebbero essere esposte alla responsabilità penale e civile, gli Stati membri sono incoraggiati ad adottare linee guida per quanto riguarda la non perseguibilità dei ricercatori in materia di sicurezza delle informazioni e l'esenzione dalla responsabilità civile per le loro attività.

(61) Gli Stati membri dovrebbero designare un CSIRT come coordinatore, che funga da intermediario di fiducia tra le persone fisiche o giuridiche segnalanti e i fabbricanti o fornitori di prodotti TIC o servizi TIC suscettibili di essere interessati dalle vulnerabilità, ove necessario. I compiti del CSIRT designato come coordinatore dovrebbero comprendere in particolare l'individuazione e il contatto dei soggetti interessati, l'assistenza alle persone fisiche o giuridiche che segnalano una vulnerabilità, la negoziazione dei tempi di divulgazione e la gestione delle vulnerabilità

che interessano più soggetti (divulgazione multilaterale coordinata di vulnerabilità). Qualora la vulnerabilità segnalata possa avere un impatto significativo su soggetti in più di uno Stato membro, i CSIRT designati come coordinatori dovrebbero cooperare nell'ambito della rete CSIRT, se del caso.

(62) L'accesso a informazioni corrette e tempestive sulle vulnerabilità che interessano i prodotti TIC e i servizi TIC contribuisce a una migliore gestione dei rischi di cibersicurezza. Le fonti di informazioni pubblicamente disponibili sulle vulnerabilità sono uno strumento importante per i soggetti e gli utenti dei loro servizi, ma anche per le autorità competenti e i CSIRT. Per tale motivo l'ENISA dovrebbe istituire una banca dati europea delle vulnerabilità in cui i soggetti, indipendentemente dal fatto che rientrino o meno nell'ambito di applicazione della presente direttiva, e i loro fornitori di sistemi informatici e di rete, così come le autorità competenti e i CSIRT, possano, su base volontaria, divulgare le vulnerabilità e fornire informazioni su di esse che consentano agli utenti di adottare adeguate misure di attenuazione. Lo scopo di tale banca dati è far fronte alle sfide uniche poste dai rischi per i soggetti unionali. Inoltre, l'ENISA dovrebbe istituire una procedura adeguata relativamente al processo di pubblicazione, al fine di dare ai soggetti il tempo di adottare misure di attenuazione per quanto riguarda le loro vulnerabilità e utilizzare le più avanzate misure di gestione dei rischi sulla cibersicurezza, nonché le serie di dati leggibili meccanicamente e le corrispondenti interfacce. Per incoraggiare una cultura della divulgazione delle vulnerabilità, la divulgazione non dovrebbe andare a scapito della persona fisica o giuridica segnalante.

(63) Sebbene simili registri o banche dati delle vulnerabilità esistano già, questi sono ospitati e mantenuti da soggetti non stabiliti nell'Unione. Una banca dati europea delle vulnerabilità mantenuta dall'ENISA garantirebbe una maggiore trasparenza, per quanto riguarda la procedura di pubblicazione prima della divulgazione al pubblico della vulnerabilità, e resilienza in caso di perturbazioni o interruzioni nella fornitura di servizi analoghi. Per evitare la duplicazione degli sforzi e perseguire, nella misura del possibile, la complementarità, l'ENISA dovrebbe valutare la possibilità di concludere accordi di cooperazione strutturata con registri simili o banche dati di competenza di giurisdizioni di paesi terzi. In particolare, l'ENISA dovrebbe valutare la possibilità di una stretta cooperazione con gli operatori del sistema delle vulnerabilità e delle esposizioni comuni (CVE).

(64) Il gruppo di cooperazione dovrebbe sostenere e agevolare la cooperazione strategica e lo scambio di informazioni, come anche rafforzare la fiducia tra gli Stati membri. Il gruppo di cooperazione dovrebbe stabilire un programma di lavoro ogni due anni. Il programma di lavoro dovrebbe comprendere le azioni che il gruppo di cooperazione deve intraprendere per attuare i suoi obiettivi e compiti. Il calendario per la definizione del primo programma di lavoro adottato a norma della presente direttiva dovrebbe essere allineato a quello dell'ultimo programma di lavoro definito a norma della direttiva (UE) 2016/1148, al fine di evitare eventuali perturbazioni nel lavoro del gruppo di cooperazione.

(65) Nello sviluppo delle linee guida, il gruppo di cooperazione dovrebbe coerentemente mappare le soluzioni e le esperienze nazionali, valutare l'impatto dei risultati del gruppo di cooperazione per quanto riguarda gli approcci nazionali, discutere le sfide in materia di attuazione e formulare raccomandazioni specifiche, in particolare per quanto riguarda l'agevolazione di un allineamento nel recepimento della presente direttiva tra gli Stati membri, da realizzare attraverso una migliore attuazione delle norme esistenti. Il gruppo di cooperazione potrebbe anche mappare le soluzioni nazionali al fine di promuovere la compatibilità delle soluzioni di cibersicurezza applicate a ciascun settore specifico in tutta l'Unione. Ciò è particolarmente pertinente per i settori che hanno natura internazionale e transfrontaliera.

(66) Il gruppo di cooperazione dovrebbe rimanere un forum flessibile ed essere in grado di reagire alle nuove e mutevoli priorità strategiche e alle sfide, tenendo conto nel contempo della disponibilità di risorse. Esso potrebbe organizzare riunioni congiunte periodiche con i pertinenti portatori di interessi del settore privato di tutta l'Unione per discutere le attività svolte dal gruppo di cooperazione e raccogliere dati e contributi sulle sfide strategiche emergenti. Inoltre, il gruppo di cooperazione dovrebbe effettuare una valutazione periodica dello stato di avanzamento delle minacce o degli incidenti informatici, come il ransomware. Al fine di rafforzare la cooperazione a livello di Unione, il gruppo di cooperazione dovrebbe prendere in considerazione la possibilità di invitare a partecipare ai suoi lavori le

pertinenti istituzioni, organismi e agenzie dell'Unione coinvolti nella politica in materia di cibersicurezza, quali il Parlamento europeo, Europol, il Comitato europeo per la protezione dei dati, l'Agenzia dell'Unione europea per la sicurezza aerea, istituita con il regolamento (UE) 2018/1139 e l'Agenzia dell'Unione europea per il programma spaziale, istituita con il regolamento (UE) 2021/696 del Parlamento europeo e del Consiglio ([14]).

(67) Le autorità competenti e i CSIRT dovrebbero poter partecipare a programmi di scambio per funzionari di altri Stati membri, nell'ambito di un quadro specifico e, se del caso, previo il nulla osta di sicurezza necessario per i funzionari che partecipano a tali programmi di scambio, al fine di migliorare la cooperazione e rafforzare la fiducia tra gli Stati membri. Le autorità competenti dovrebbero adottare le misure necessarie per consentire a funzionari di altri Stati membri di svolgere un ruolo efficace nelle attività dell'autorità competente ospitante o del CSIRT ospitante.

(68) Gli Stati membri dovrebbero contribuire all'istituzione del quadro di risposta alle crisi di cibersicurezza dell'UE, di cui alla raccomandazione (UE) 2017/1584 della Commissione ([15]), attraverso le reti di cooperazione esistenti, in particolare la rete europea di collegamento per le crisi informatiche (EU-CyCLONe), la rete di CSIRT e il gruppo di cooperazione. EU-CyCLONe e la rete di CSIRT dovrebbero cooperare sulla base di disposizioni procedurali che specifichino i dettagli di tale cooperazione ed evitare duplicazioni dei compiti. Il regolamento interno di EU-CyCLONe dovrebbe specificare ulteriormente i meccanismi di funzionamento della rete, compresi i ruoli, i mezzi di cooperazione, le interazioni con altri attori pertinenti e i modelli per la condivisione delle informazioni, nonché i mezzi di comunicazione. Per la gestione delle crisi a livello dell'Unione, le parti pertinenti dovrebbero affidarsi ai dispositivi integrati dell'UE per la risposta politica alle crisi nel quadro della decisione di esecuzione (UE) 2018/1993 del Consiglio ([16]) (dispositivi IPCR). A tal fine la Commissione dovrebbe far ricorso al processo di coordinamento intersettoriale delle crisi ad alto livello del sistema ARGUS. Se la crisi implica un'importante dimensione esterna o una forte correlazione con la politica di sicurezza e di difesa comune dovrebbe essere attivato il meccanismo di risposta alle crisi del servizio europeo per l'azione esterna.

(69) Conformemente all'allegato della raccomandazione (UE) 2017/1584, per incidente di cibersicurezza su vasta scala si intende un incidente di cibersicurezza che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi, o che ha un impatto significativo su almeno due Stati membri. A seconda della loro causa e del loro impatto, gli incidenti di cibersicurezza su vasta scala possono aggravarsi e trasformarsi in vere e proprie crisi che non consentono il corretto funzionamento del mercato interno, o che comportano gravi rischi di pubblica sicurezza in diversi Stati membri o nell'intera Unione. Data l'ampia portata e, nella maggior parte dei casi, la natura transfrontaliera di tali incidenti, gli Stati membri e le istituzioni, gli organismi e le agenzie pertinenti dell'Unione dovrebbero cooperare a livello tecnico, operativo e politico per coordinare adeguatamente la risposta in tutta l'Unione.

(70) Gli incidenti e le crisi di cibersicurezza su vasta scala a livello dell'Unione richiedono un'azione coordinata per garantire una risposta rapida ed efficace, a causa dell'elevato grado di interdipendenza tra settori e Stati membri. La disponibilità di sistemi informatici e di rete ciberresilienti e la disponibilità, la riservatezza e l'integrità dei dati sono essenziali per la sicurezza dell'Unione e per la protezione dei suoi cittadini, delle sue imprese e delle sue istituzioni da incidenti e minacce informatiche, nonché per rafforzare la fiducia delle persone e delle organizzazioni nella capacità dell'Unione di promuovere e proteggere un ciberspazio globale, aperto, libero, stabile e sicuro basato sui diritti umani, le libertà fondamentali, la democrazia e lo Stato di diritto.

([14]) Regolamento (UE) 2021/696 del Parlamento europeo e del Consiglio, del 28 aprile 2021, che istituisce il programma spaziale dell'Unione e l'Agenzia dell'Unione europea per il programma spaziale e che abroga i regolamenti (UE) n. 912/2010, (UE) n. 1285/2013 e (UE) n. 377/2014 e la decisione n. 541/2014/UE (GU L 170 del 12.5.2021, pag. 69).

([15]) Raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala (GU L 239 del 19.9.2017, pag. 36).

([16]) Decisione di esecuzione (UE) 2018/1993 del Consiglio, dell'11 dicembre 2018, relativa ai dispositivi integrati dell'UE per la risposta politica alle crisi (GU L 320 del 17.12.2018, pag. 28).

(71) EU-CyCLONe dovrebbe fungere da intermediario tra il livello tecnico e politico durante gli incidenti e le crisi di cibersicurezza su vasta scala e dovrebbe rafforzare la cooperazione a livello operativo e sostenere il processo decisionale a livello politico. In cooperazione con la Commissione, tenuto conto della competenza di quest'ultima nel settore della gestione delle crisi, EU-CyCLONe dovrebbe basarsi sui risultati della rete di CSIRT e utilizzare le proprie capacità per elaborare analisi d'impatto di incidenti e crisi di cibersicurezza su vasta scala.

(72) Gli attacchi informatici sono di natura transfrontaliera e un incidente significativo può perturbare e danneggiare le infrastrutture informatiche critiche da cui dipende il corretto funzionamento del mercato interno. La raccomandazione (UE) 2017/1584 tratta il ruolo di tutti i soggetti interessati. Inoltre, la Commissione è responsabile, nel quadro del meccanismo unionale di protezione civile istituito dalla decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio ([17]), delle azioni di preparazione generali, che comprendono la gestione del Centro di coordinamento della risposta alle emergenze e del sistema comune di comunicazione e di informazione in caso di emergenza, il mantenimento e l'ulteriore sviluppo della consapevolezza situazionale e delle capacità di analisi, nonché la predisposizione e la gestione della capacità di mobilitare e inviare squadre di esperti in caso di richiesta di assistenza da parte di uno Stato membro o di un paese terzo. La Commissione è inoltre responsabile di fornire relazioni analitiche per i dispositivi IPCR nel quadro della decisione di esecuzione (UE) 2018/1993, anche in relazione alla consapevolezza situazionale e alla preparazione in materia di cibersicurezza, come anche per la consapevolezza situazionale e la risposta alle crisi nei settori dell'agricoltura, delle condizioni meteorologiche avverse, della mappatura e delle previsioni dei conflitti, dei sistemi di allarme rapido in caso di catastrofi naturali, delle emergenze sanitarie, della sorveglianza delle malattie infettive, della salute delle piante, degli incidenti chimici, della sicurezza di alimenti e mangimi, della salute degli animali, della migrazione, delle dogane, delle emergenze radiologiche e nucleari, e dell'energia.

(73) Ove opportuno, l'Unione può concludere accordi internazionali, in conformità all'articolo 218 TFUE, con paesi terzi o organizzazioni internazionali, che consentano e organizzino la loro partecipazione ad attività particolari del gruppo di cooperazione, della rete di CSIRT e di EU-CyCLONe. Tali accordi dovrebbero garantire gli interessi dell'Unione e un'adeguata protezione dei dati. Ciò non dovrebbe escludere il diritto degli Stati membri di cooperare con paesi terzi sulla gestione delle vulnerabilità e la gestione dei rischi di cibersicurezza, agevolando la segnalazione e la condivisione delle informazioni generali in conformità al diritto dell'Unione.

(74) Al fine di facilitare l'effettiva attuazione della presente direttiva per quanto riguarda, tra l'altro, la gestione delle vulnerabilità, le misure di gestione dei rischi di cibersicurezza, gli obblighi di segnalazione e gli accordi di condivisione delle informazioni relative alla cibersicurezza, gli Stati membri possono cooperare con i paesi terzi e intraprendere attività ritenute appropriate a tal fine, tra cui scambi di informazioni relative a minacce informatiche, incidenti, vulnerabilità, strumenti e metodi, tattiche, tecniche e procedure, preparazione ed esercitazioni in materia di gestione delle crisi informatiche, formazioni, instaurazione di un clima di fiducia e accordi strutturati di condivisione delle informazioni.

(75) Dovrebbero essere introdotte revisioni tra pari per contribuire a trarre insegnamenti dalle esperienze condivise, rafforzare la fiducia reciproca e conseguire un livello comune elevato di cibersicurezza. Le revisioni tra pari possono portare a idee e raccomandazioni preziose che rafforzano le capacità globali in materia di cibersicurezza, creando un altro percorso funzionale per la condivisione delle migliori pratiche tra gli Stati membri e contribuendo a migliorare i livelli di maturità degli Stati membri in materia di cibersicurezza. Inoltre, le revisioni tra pari dovrebbero tenere conto dei risultati di meccanismi analoghi, come il sistema di revisione tra pari della rete di CSIRT e dovrebbero apportare un valore aggiunto ed evitare duplicazioni. L'attuazione delle revisioni tra pari dovrebbe lasciare impregiudicato il diritto dell'Unione o nazionale in materia di protezione delle informazioni riservate o classificate.

(76) Il gruppo di cooperazione dovrebbe stabilire una metodologia di autovalutazione per gli Stati membri, al fine di coprire fattori quali il livello di attuazione delle misure di gestione dei rischi di cibersicurezza e degli obblighi di segnalazione, il livello di capacità e l'efficacia dell'esercizio dei compiti delle autorità competenti, le capacità operative dei CSIRT, il livello di attuazione dell'assistenza reciproca, il livello di attuazione degli accordi di condivisione delle informazioni in materia di cibersicurezza o questioni specifiche di natura transfrontaliera o intersettoriale. Gli Stati membri dovrebbero essere incoraggiati ad effettuare autovalutazioni su base regolare e a presentare e discutere i risultati della loro autovalutazione nell'ambito del gruppo di cooperazione.

([17]) Decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio, del 17 dicembre 2013, su un meccanismo unionale di protezione civile (GU L 347 del 20.12.2013, pag. 924).

(77) La responsabilità di garantire la sicurezza dei sistemi informatici e di rete incombe in larga misura a soggetti essenziali e importanti. È opportuno promuovere e sviluppare una cultura della gestione dei rischi, che comprenda valutazioni dei rischi e l'attuazione di misure di gestione dei rischi di cibersicurezza adeguate ai rischi esistenti.

(78) Le misure di gestione dei rischi dovrebbero tenere conto del grado di dipendenza del soggetto essenziale o importante dai sistemi informatici e di rete e comprendere misure per individuare eventuali rischi di incidenti, per prevenire e rilevare incidenti, nonché per rispondervi, riprendersi da essi e attenuarne l'impatto. La sicurezza dei sistemi informatici e di rete dovrebbe comprendere la sicurezza dei dati conservati, trasmessi e elaborati. Le misure di gestione dei rischi di cibersicurezza dovrebbero prevedere un'analisi sistemica, tenendo conto del fattore umano, onde avere un quadro completo della sicurezza del sistema informatico e di rete.

(79) Poiché le minacce alla sicurezza dei sistemi informatici e di rete possono avere origini diverse, le misure di gestione dei rischi di cibersicurezza dovrebbero essere basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da eventi quali furti, incendi, inondazioni, problemi di telecomunicazione o interruzioni di corrente, o da qualsiasi accesso fisico non autorizzato nonché dai danni alle informazioni detenute dai soggetti essenziali o importanti e agli impianti di trattamento delle informazioni di questi ultimi e dalle interferenze con tali informazioni o impianti che possano compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi. Le misure di gestione dei rischi di cibersicurezza dovrebbero pertanto affrontare anche la sicurezza fisica e dell'ambiente dei sistemi informatici e di rete includendo misure volte a proteggere detti sistemi da guasti del sistema, errori umani, azioni malevole o fenomeni naturali, in linea con le norme europee e internazionali, come quelle di cui alla serie ISO/IEC 27000. A tale riguardo, i soggetti essenziali e importanti dovrebbero altresì, nell'ambito delle loro misure di gestione dei rischi di cibersicurezza, affrontare la questione della sicurezza delle risorse umane e disporre di strategie adeguate di controllo dell'accesso. Tali misure dovrebbero essere coerenti con la direttiva (UE) 2022/2557.

(80) Al fine di dimostrare la conformità alle misure di gestione dei rischi di cibersicurezza e in mancanza di adeguati sistemi europei di certificazione della cibersicurezza adottati a norma del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio ([18]), gli Stati membri, in consultazione del gruppo di cooperazione e del gruppo europeo per la certificazione della cibersicurezza, dovrebbero promuovere l'uso delle pertinenti norme europee e internazionali da parte dei soggetti essenziali e importanti o possono imporre a questi ultimi di utilizzare prodotti TIC, servizi TIC e processi TIC certificati.

(81) Per evitare di imporre un onere finanziario e amministrativo sproporzionato ai soggetti essenziali e importanti, le misure di gestione dei rischi di cibersicurezza dovrebbero essere proporzionate ai rischi posti al sistema informatico e di rete interessato, tenendo conto dello stato dell'arte di tali misure e, se del caso, di pertinenti norme europee e internazionali, come anche dei relativi costi di attuazione.

(82) Le misure di gestione dei rischi di cibersicurezza dovrebbero essere proporzionate al grado di esposizione del soggetto essenziali o importanti ai rischi e all'impatto sociale ed economico che un incidente avrebbe. Nel definire misure di gestione dei rischi di cibersicurezza adattate ai soggetti essenziali e importanti, è opportuno tenere debitamente conto dell'esposizione al rischio divergente dei soggetti essenziali e importanti, quali la criticità del soggetto, i rischi, compresi i rischi sociali, cui è esposto, le dimensioni del soggetto e la probabilità del verificarsi di incidenti e la loro gravità, compreso il loro impatto sociale ed economico.

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

(83) I soggetti essenziali e importanti dovrebbero garantire la sicurezza dei sistemi informatici e di rete che utilizzano nelle loro attività. Si tratta in particolare di sistemi informatici e di rete privati gestiti dal personale informatico interno dei soggetti essenziali e importanti oppure la cui sicurezza sia stata esternalizzata. Le misure di gestione e gli obblighi di segnalazione dei rischi di cibersicurezza stabiliti nella presente direttiva dovrebbero applicarsi ai pertinenti soggetti essenziali e importanti indipendentemente dal fatto che tali soggetti effettuino internamente la manutenzione dei loro sistemi informatici e di rete o che la esternalizzino.

(84) Tenuto conto della loro natura transfrontaliera, i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network, e i fornitori di servizi di sicurezza gestiti e i prestatori di servizi fiduciari dovrebbero essere soggetti a un elevato livello di armonizzazione a livello dell'Unione. L'attuazione delle misure di gestione del rischio di cibersicurezza con riguardo a tali soggetti dovrebbe pertanto essere agevolata da un atto di esecuzione.

(85) Affrontare i rischi derivanti dalla catena di approvvigionamento di un soggetto e dalla sua relazione con i fornitori, ad esempio i fornitori di servizi di conservazione ed elaborazione dei dati o di servizi di sicurezza gestiti e gli editori di software, è particolarmente importante data la prevalenza di incidenti in cui i soggetti sono stati vittime di attacchi informatici e in cui i responsabili di atti malevoli sono stati in grado di compromettere la sicurezza dei sistemi informatici e di rete di un soggetto sfruttando le vulnerabilità che interessano prodotti e servizi di terzi. I soggetti essenziali e importanti dovrebbero pertanto valutare e tenere in considerazione la qualità e la resilienza complessive dei prodotti e dei servizi, delle misure di gestione dei rischi di cibersicurezza in essi integrate e delle pratiche di cibersicurezza dei loro fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. In particolare, i soggetti essenziali e importanti dovrebbero essere incoraggiati a integrare misure di gestione dei rischi di cibersicurezza negli accordi contrattuali con i loro fornitori e fornitori di servizi diretti. Tali soggetti potrebbero prendere in considerazione i rischi derivanti da altri livelli di fornitori e fornitori di servizi.

(86) Tra i fornitori di servizi, i fornitori di servizi di sicurezza gestiti in settori quali la risposta agli incidenti, i test di penetrazione, gli audit di sicurezza e la consulenza svolgono un ruolo particolarmente importante nell'assistere i soggetti nei loro sforzi per la prevenzione e il rilevamento degli incidenti, la risposta agli stessi o la ripresa da essi. I fornitori di servizi di sicurezza gestiti sono stati tuttavia essi stessi bersaglio di attacchi informatici e, a causa della loro stretta integrazione nelle attività dei soggetti, presentano un particolare rischio. I soggetti essenziali e importanti dovrebbero pertanto esercitare una maggiore diligenza nella selezione di un fornitore di servizi di sicurezza gestiti.

(87) Nell'ambito dei loro compiti di vigilanza, le autorità competenti possono inoltre beneficiare di servizi di cibersicurezza quali gli audit sulla sicurezza, i test di penetrazione o la risposta agli incidenti.

(88) I soggetti essenziali e importanti dovrebbero inoltre affrontare i rischi derivanti dalle loro interazioni e relazioni con altri portatori di interessi nell'ambito di un ecosistema più ampio, anche per quanto riguarda la lotta contro lo spionaggio industriale e la tutela dei segreti commerciali. In particolare, tali soggetti dovrebbero adottare misure adeguate per garantire che la loro cooperazione con gli istituti accademici e di ricerca avvenga in linea con le loro politiche in materia di cibersicurezza e segua le buone pratiche per quanto riguarda l'accesso sicuro e la diffusione delle informazioni in generale e la tutela della proprietà intellettuale in particolare. Analogamente, data l'importanza e il valore dei dati per le attività dei soggetti essenziali e importanti, tali soggetti dovrebbero adottare tutte le opportune misure di gestione dei rischi di cibersicurezza quando si affidano ai servizi di trasformazione e analisi dei dati forniti da terzi.

(89) I soggetti essenziali e importanti dovrebbero adottare un'ampia gamma di pratiche di igiene informatica di base quali principi zero trust, aggiornamenti del software, configurazione dei dispositivi, segmentazione della rete, gestione dell'identità e dell'accesso o sensibilizzazione degli utenti, organizzare per il loro personale una formazione e sensibilizzarlo alle minacce informatiche, al phishing o alle tecniche di ingegneria sociale. Inoltre, tali soggetti dovrebbero valutare le loro capacità di cibersicurezza e, se del caso, perseguire l'integrazione di tecnologie per il rafforzamento della cibersicurezza quali l'intelligenza artificiale o i sistemi di apprendimento automatico, per migliorare le loro capacità e la sicurezza dei sistemi informatici e di rete.

(90) Per affrontare ulteriormente i principali rischi relativi alla catena di approvvigionamento e aiutare i soggetti essenziali e importanti che operano nei settori disciplinati dalla presente direttiva a gestire adeguatamente i rischi connessi alla catena di approvvigionamento e ai fornitori, il gruppo di cooperazione, in cooperazione con la Commissione e l'ENISA e, se del caso, previa consultazione dei pertinenti portatori di interessi compresi quelli del settore, dovrebbe effettuare valutazioni coordinate dei rischi per la sicurezza di catene di approvvigionamento critiche, come è avvenuto per le reti 5G in seguito alla raccomandazione (UE) 2019/534 della Commissione ([19]), al fine di individuare, per settore, i servizi TIC, i sistemi TIC o i prodotti TIC critici e le minacce e le vulnerabilità pertinenti. Dette valutazioni coordinate dei rischi per la sicurezza dovrebbero individuare le misure, i piani di attenuazione e le migliori pratiche per contrastare le dipendenze critiche, i potenziali singoli punti di vulnerabilità, le minacce, le vulnerabilità e gli altri rischi associati alla catena di approvvigionamento, ed esplorare modalità per incoraggiare ulteriormente una loro più ampia adozione da parte dei soggetti essenziali e importanti. I potenziali fattori di rischio non tecnici, come l'indebita influenza di un paese terzo sui fornitori e i fornitori di servizi, in particolare nel caso di modelli alternativi di governance, includono vulnerabilità nascoste o backdoor e potenziali turbative sistemiche dell'approvvigionamento, segnatamente in caso di lock-in tecnologico o di dipendenza dal fornitore.

(91) Le valutazioni coordinate dei rischi per la sicurezza di catene di approvvigionamento critiche, alla luce delle caratteristiche del settore interessato, dovrebbero tenere conto dei fattori tecnici e, se opportuno, non tecnici, compresi quelli definiti nella raccomandazione (UE) 2019/534, nella valutazione dei rischi coordinata dell'UE della cibersicurezza delle reti 5G e nel pacchetto di strumenti dell'UE sulla cibersicurezza del 5G concordato dal gruppo di cooperazione. Per individuare le catene di approvvigionamento che dovrebbero essere soggette a una valutazione coordinata dei rischi per la sicurezza, dovrebbero essere presi in considerazione i seguenti criteri: i) la misura in cui i soggetti essenziali e importanti ricorrono e si affidano a specifici servizi TIC, sistemi TIC o prodotti TIC critici; ii) la pertinenza di specifici servizi TIC, sistemi TIC o prodotti TIC critici per lo svolgimento di funzioni critiche o sensibili, compreso il trattamento dei dati personali; iii) la disponibilità di servizi TIC, sistemi TIC o prodotti TIC alternativi; iv) la resilienza dell'intera catena di approvvigionamento di servizi TIC, sistemi TIC o prodotti TIC, durante tutto il loro ciclo di vita, contro eventi perturbatori e v) per i servizi TIC, sistemi TIC o prodotti TIC emergenti, la loro potenziale importanza futura per le attività dei soggetti. Inoltre, si dovrebbe porre un accento particolare sui servizi TIC, i sistemi TIC o i prodotti TIC che sono soggetti a requisiti specifici derivanti da paesi terzi.

(92) Al fine di semplificare gli obblighi imposti ai fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico e ai prestatori di servizi fiduciari relativi alla sicurezza dei loro sistemi informatici e di rete, nonché di consentire a tali soggetti e alle autorità competenti ai sensi, rispettivamente, della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio ([20]) e del regolamento (UE) n. 910/2014 di beneficiare del quadro giuridico istituito dalla presente direttiva, comprese la designazione di un CSIRT responsabile della gestione degli incidenti, la partecipazione delle autorità competenti interessate alle attività del gruppo di cooperazione e della rete di CSIRT, tali soggetti dovrebbero rientrare nell'ambito di applicazione della presente direttiva. Le corrispondenti disposizioni stabilite nel regolamento (UE) n. 910/2014 e nella direttiva (UE) 2018/1972 relative all'imposizione di obblighi di sicurezza e notifica a queste tipologie di soggetti dovrebbero pertanto essere soppresse. Le norme relative agli obblighi di segnalazione stabilite nella presente direttiva dovrebbero lasciare impregiudicati il regolamento (UE) 2016/679 e la direttiva 2002/58/CE.

(93) Gli obblighi in materia di cibersicurezza stabiliti nella presente direttiva dovrebbero essere considerati complementari ai requisiti imposti ai prestatori di servizi fiduciari ai sensi del regolamento (UE) n. 910/2014. È opportuno chiedere ai prestatori di servizi fiduciari di adottare tutte le misure adeguate e proporzionate per gestire i rischi posti ai loro servizi, anche in relazione ai clienti e ai terzi che vi fanno affidamento, nonché di segnalare gli incidenti a norma della presente direttiva. Tali obblighi in materia di cibersicurezza e segnalazione dovrebbero riguardare anche la protezione fisica dei servizi forniti. I requisiti per i prestatori di servizi fiduciari qualificati stabiliti all'articolo 24 del regolamento (UE) n. 910/2014 continuano ad applicarsi.

([19]) Raccomandazione (UE) 2019/534 della Commissione, del 26 marzo 2019, Cibersicurezza delle reti 5G (GU L 88 del 29.3.2019, pag. 42).

([20]) Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche (GU L 321 del 17.12.2018, pag. 36).

(94) Gli Stati membri possono conferire il ruolo di autorità competenti per i servizi fiduciari agli organismi di vigilanza a norma del regolamento (UE) n. 910/2014 al fine di garantire la prosecuzione delle pratiche attuali e di sfruttare le conoscenze e l'esperienza acquisite con l'applicazione di detto regolamento. In tal caso, le autorità competenti a norma della presente direttiva dovrebbero cooperare strettamente e in modo tempestivo con tali organismi di vigilanza scambiando le informazioni pertinenti al fine di assicurare l'efficace vigilanza dei prestatori di servizi fiduciari nonché l'effettivo rispetto, da parte di questi ultimi, delle prescrizioni stabilite nella presente direttiva e nel regolamento (UE) n. 910/2014. Se del caso, il CSIRT o l'autorità competente a norma della presente direttiva dovrebbero informare immediatamente l'organismo di vigilanza a norma del regolamento (UE) n. 910/2014 di qualunque minaccia informatica o incidente significativi notificati aventi un impatto sui servizi fiduciari nonché di qualunque violazione, da parte di un prestatore di servizi fiduciari, della presente direttiva. Ai fini della segnalazione, gli Stati membri possono, se del caso, utilizzare il punto di ingresso unico stabilito per effettuare segnalazioni comuni e automatiche di incidenti destinate sia all'organismo di vigilanza a norma del regolamento (UE) n. 910/2014 sia al CSIRT o all'autorità competente a norma della presente direttiva.

(95) Se opportuno e per evitare inutili perturbazioni, gli orientamenti nazionali esistenti adottati per il recepimento delle norme relative alle misure di sicurezza di cui agli articoli 40 e 41 della direttiva (UE) 2018/1972 dovrebbero essere presi in considerazione nel recepimento della presente direttiva, basandosi quindi sulle conoscenze e competenze già acquisite nell'ambito della direttiva (UE) 2018/1972 per quanto riguarda le misure di sicurezza e le notifiche degli incidenti. L'ENISA può inoltre elaborare orientamenti sui requisiti di sicurezza e sugli obblighi di segnalazione per i fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico al fine di facilitare l'armonizzazione e la transizione e di ridurre al minimo le perturbazioni. Gli Stati membri possono conferire il ruolo di autorità competenti per le comunicazioni elettroniche alle autorità nazionali di regolamentazione ai sensi della direttiva (UE) 2018/1972 al fine di garantire la prosecuzione delle pratiche attuali e di sfruttare le conoscenze e l'esperienza acquisite a seguito con l'attuazione di tale direttiva.

(96) Vista la crescente importanza dei servizi di comunicazione interpersonale indipendenti dal numero quali definiti nella direttiva (UE) 2018/1972, è necessario assicurare che anche tali servizi siano soggetti ad adeguati requisiti di sicurezza in considerazione della loro specificità e della loro rilevanza economica. Dal momento che la superficie di attacco continua ad ampliarsi, i servizi di comunicazione interpersonale indipendenti dal numero, come i servizi di messaggistica, stanno diventando vettori di attacco diffusi. I responsabili di atti malevoli utilizzano piattaforme per comunicare e indurre le vittime ad aprire pagine web compromesse, aumentando così la probabilità di incidenti che interessano lo sfruttamento dei dati personali e, per estensione, la sicurezza dei sistemi informatici e di rete. I fornitori di servizi di comunicazione interpersonale indipendenti dal numero dovrebbero garantire un livello di sicurezza dei sistemi informatici e di rete adeguato ai rischi esistenti. Dato che i fornitori di servizi di comunicazione interpersonale indipendenti dal numero solitamente non esercitano un controllo effettivo sulla trasmissione dei segnali sulle reti, il grado di rischio per tali servizi può essere considerato, per certi aspetti, inferiore a quello dei servizi di comunicazione elettronica tradizionali. Lo stesso vale per i servizi di comunicazione interpersonale quali definiti nella direttiva (UE) 2018/1972 che utilizzano numeri e che non esercitano un controllo effettivo sulla trasmissione dei segnali.

(97) Il mercato interno dipende più che mai dal funzionamento di internet. I servizi di quasi tutti i soggetti essenziali e importanti dipendono dai servizi forniti via internet. Al fine di garantire l'erogazione senza intoppi dei servizi forniti dai soggetti essenziali e importanti, è fondamentale che tutti i fornitori di reti pubbliche di comunicazione elettronica dispongano di adeguate misure di gestione dei rischi di cibersicurezza e segnalino gli incidenti significativi connessi. Gli Stati membri dovrebbero garantire il mantenimento della sicurezza delle reti pubbliche di comunicazione elettronica e la protezione dei loro interessi vitali in materia di sicurezza contro il sabotaggio e lo spionaggio. Poiché la connettività internazionale migliora e accelera la digitalizzazione competitiva dell'Unione e della sua economia, gli incidenti che interessano i cavi di comunicazione sottomarini dovrebbero essere segnalati al CSIRT o, se del caso, all'autorità competente. La strategia nazionale per la cibersicurezza dovrebbe, se del caso, tenere conto della cibersicurezza dei cavi di comunicazione sottomarini e includere una mappatura dei potenziali rischi di cibersicurezza e misure di attenuazione per garantire il massimo livello di protezione.

(98) Al fine di salvaguardare la sicurezza delle reti pubbliche di comunicazione elettronica e dei servizi di comunicazione elettronica accessibili al pubblico, l'uso delle tecnologie di cifratura, in particolare la cifratura end-to-end, come anche concetti di sicurezza incentrati sui dati, quali la cartografia, la segmentazione, la marcatura, la politica di accesso e la gestione dell'accesso, nonché le decisioni di accesso automatizzato, dovrebbe essere promosso. Ove necessario, l'uso della cifratura, in particolare la cifratura end-to-end, dovrebbe essere reso obbligatorio per i fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico, conformemente ai principi di sicurezza e tutela della vita privata per impostazione predefinita e fin dalla progettazione ai fini della presente direttiva. L'uso della cifratura end-to-end dovrebbe essere conciliato con i poteri degli Stati membri di garantire la tutela della sicurezza pubblica e dei loro interessi essenziali in materia di sicurezza, nonché di consentire la prevenzione, l'indagine, l'accertamento e il perseguimento di reati in conformità al diritto dell'Unione. Tuttavia, ciò non dovrebbe indebolire la cifratura end-to-end, che è una tecnologia fondamentale per un'efficace protezione dei dati, della privacy e della sicurezza delle comunicazioni.

(99) Al fine di salvaguardare la sicurezza, e prevenire abusi e manipolazioni, delle reti pubbliche di comunicazione elettronica e dei servizi di comunicazione elettronica accessibili al pubblico, è opportuno promuovere il ricorso a standard in materia di inoltro sicuro per garantire l'integrità e la solidità delle funzioni di inoltro in tutto l'ecosistema dei fornitori di servizi di accesso a internet.

(100) Al fine di salvaguardare la funzionalità e l'integrità di internet e promuovere la sicurezza e la resilienza del DNS, i portatori di interessi pertinenti, tra cui soggetti del settore privato dell'Unione, fornitori di servizi di comunicazione elettronica accessibili al pubblico, in particolare fornitori di servizi di accesso a internet e fornitori di motori di ricerca online, dovrebbero essere incoraggiati ad adottare una strategia di diversificazione della risoluzione DNS. Inoltre, gli Stati membri dovrebbero incoraggiare lo sviluppo e l'utilizzo di un servizio europeo di risoluzione DNS pubblico e sicuro.

(101) La presente direttiva stabilisce un approccio in più fasi alla segnalazione degli incidenti significativi al fine di trovare il giusto equilibrio tra, da un lato, una segnalazione rapida che contribuisca ad attenuare la potenziale diffusione di incidenti e consenta ai soggetti essenziali e importanti di chiedere assistenza e, dall'altro, una segnalazione approfondita che tragga insegnamenti preziosi dai singoli incidenti e migliori nel tempo la resilienza informatica dei singoli soggetti e di interi settori. A tale proposito, la presente direttiva dovrebbe includere la segnalazione di incidenti che, sulla base di una valutazione iniziale condotta dal soggetto interessato, potrebbero causare gravi perturbazioni operative dei servizi o perdite finanziarie per tale soggetto, o interessare altre persone fisiche o giuridiche causando considerevoli danni materiali o immateriali. Detta valutazione iniziale dovrebbe tenere conto, tra l'altro, dei sistemi informatici e di rete interessati, in particolare della loro importanza nella fornitura dei servizi del soggetto, della gravità e delle caratteristiche tecniche di una minaccia informatica e delle eventuali vulnerabilità sottostanti che vengono sfruttate, nonché dell'esperienza del soggetto in caso di incidenti simili. Indicatori quali la misura in cui il funzionamento del servizio è interessato, la durata di un incidente o il numero di destinatari dei servizi interessati potrebbero svolgere un ruolo importante nel determinare se la perturbazione operativa del servizio è grave.

(102) Qualora vengano a conoscenza di un incidente significativo, i soggetti essenziali o importanti dovrebbero essere tenuti a presentare un preallarme senza indebito ritardo, e comunque entro 24 ore. Tale preallarme dovrebbe essere seguito da una notifica dell'incidente. I soggetti interessati dovrebbero presentare una notifica dell'incidente senza indebito ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, allo scopo, in particolare, di aggiornare le informazioni trasmesse nel preallarme e di indicare una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione. Una relazione finale dovrebbe essere presentata entro un mese dalla notifica dell'incidente. Il preallarme dovrebbe contenere soltanto le informazioni necessarie per informare il CSIRT, o se del caso l'autorità competente, dell'incidente significativo e consentire al soggetto interessato di chiedere assistenza, se necessario. Tale preallarme dovrebbe indicare, ove opportuno, se l'incidente significativo è sospettato di essere il risultato di atti illeciti o malevoli e se è probabile che abbia un impatto transfrontaliero. Gli Stati membri dovrebbero garantire che l'obbligo di presentare tale preallarme, o la successiva notifica dell'incidente, non sottragga le risorse del soggetto notificante alle attività relative alla gestione degli incidenti, che dovrebbero essere considerate prioritarie, per evitare che gli obblighi di segnalazione degli incidenti sottraggano risorse alla gestione della risposta agli incidenti o

compromettano altrimenti gli sforzi dei soggetti a tale riguardo. In caso di incidente in corso al momento della trasmissione della relazione finale, gli Stati membri dovrebbero provvedere affinché i soggetti interessati forniscano una relazione sui progressi in quel momento e una relazione finale entro un mese dalla gestione dell'incidente significativo.

(103) Se del caso, i soggetti essenziali e importanti dovrebbero comunicare senza indebito ritardo ai destinatari dei loro servizi le misure o le azioni correttive che possono adottare per attenuare i rischi che derivano da una minaccia informatica significativa. Tali soggetti dovrebbero, ove opportuno e in particolare quando è probabile che la minaccia informatica significativa si concretizzi, informare i destinatari dei loro servizi anche in merito alla minaccia stessa. L'obbligo di informare tali destinatari in merito alle minacce informatiche significative dovrebbe essere soddisfatto con la massima diligenza possibile, ma non dovrebbe esonerare tali soggetti dall'obbligo di adottare, a proprie spese, provvedimenti adeguati e immediati per prevenire eventuali minacce di questo tipo o porvi rimedio e ristabilire il normale livello di sicurezza del servizio. La fornitura ai destinatari dei servizi di tali informazioni riguardanti le minacce informatiche significative dovrebbe essere gratuita e avvenire in una lingua facilmente comprensibile.

(104) I fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico dovrebbero attuare la sicurezza fin dalla progettazione e per impostazione predefinita e informare i destinatari dei loro servizi di minacce informatiche significative e delle misure che questi ultimi possono adottare per proteggere la sicurezza dei loro dispositivi e delle loro comunicazioni, ad esempio attraverso l'uso di particolari tipi di programmi o tecnologie di cifratura.

(105) Un approccio proattivo alle minacce informatiche è una componente essenziale delle misure di gestione dei rischi di cibersicurezza che dovrebbe consentire alle autorità competenti di impedire efficacemente che le minacce informatiche si trasformino in incidenti che possono causare danni materiali o immateriali considerevoli. A tal fine, la notifica di minacce informatiche riveste un'importanza fondamentale. I soggetti sono pertanto incoraggiati a segnalare su base volontaria le minacce informatiche.

(106) Al fine di semplificare la comunicazione delle informazioni richieste a norma della presente direttiva e di ridurre gli oneri amministrativi per i soggetti, gli Stati membri dovrebbero fornire mezzi tecnici quali un punto di ingresso unico, sistemi automatizzati, moduli online, interfacce di facile utilizzo, modelli e piattaforme dedicate per l'uso dei soggetti, indipendentemente dal fatto che rientrino o meno nell'ambito di applicazione della presente direttiva, per la comunicazione delle pertinenti informazioni da segnalare. I finanziamenti dell'Unione a sostegno dell'attuazione della presente direttiva, in particolare nell'ambito del programma Europa digitale istituito dal regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio ([21]), potrebbero includere il sostegno a punti di ingresso unici. Inoltre, i soggetti si trovano spesso in una situazione in cui un particolare incidente, a causa delle sue caratteristiche, deve essere segnalato a varie autorità in conseguenza degli obblighi di notifica previsti da vari strumenti giuridici. Tali casi creano ulteriori oneri amministrativi e potrebbero anche generare incertezze in merito al formato e alle procedure di tali notifiche. Qualora sia istituito un punto di ingresso unico, gli Stati membri sono incoraggiati a utilizzare tale punto di ingresso anche per le notifiche degli incidenti di sicurezza previste da altre normative dell'Unione, quali il regolamento (UE) 2016/679 e la direttiva 2002/58/CE. L'uso di tale punto di accesso unico per la segnalazione di incidenti di sicurezza a norma del regolamento (UE) 2016/679 e della direttiva 2002/58/CE non dovrebbe pregiudicare l'applicazione delle disposizioni di cui al regolamento (UE) 2016/679 e alla direttiva 2002/58/CE, in particolare quelle relative all'indipendenza delle autorità ivi menzionate. L'ENISA, in collaborazione con il gruppo di cooperazione, dovrebbe elaborare modelli comuni di notifica mediante orientamenti per semplificare e razionalizzare le informazioni da segnalare richieste a norma del diritto dell'Unione e ridurre gli oneri amministrativi per i soggetti notificanti.

(107) Se si sospetta che un incidente sia connesso ad attività criminali gravi a norma del diritto dell'Unione o nazionale, gli Stati membri dovrebbero incoraggiare i soggetti essenziali e importanti, in base alle norme applicabili ai procedimenti penali in conformità al diritto dell'Unione, a segnalare alle autorità di contrasto pertinenti gli incidenti di cui si sospetta la natura criminale grave. Ove opportuno, e fatte salve le norme in materia di protezione dei dati personali applicabili a Europol, è auspicabile che il Centro europeo per la lotta alla criminalità informatica (EC3) e l'ENISA agevolino il coordinamento tra le autorità competenti e le autorità di contrasto dei diversi Stati membri.

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

(108) In molti casi gli incidenti compromettono i dati personali. In tale contesto, le autorità competenti dovrebbero cooperare e scambiarsi informazioni su tutte le questioni pertinenti con le autorità di cui al regolamento (UE) 2016/679 e alla direttiva 2002/58/CE.

(109) Il mantenimento di banche dati precise e complete dei dati di registrazione dei nomi di dominio («dati WHOIS») e la fornitura di un accesso legittimo a tali dati sono essenziali per garantire la sicurezza, la stabilità e la resilienza del DNS, che a sua volta contribuisce a un elevato livello comune di cibersicurezza in tutta l'Unione. A tal fine specifico, i registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero essere tenuti a trattare alcuni dati necessari a raggiungere tale scopo. Tale trattamento dovrebbe costituire un obbligo legale ai sensi dell'articolo 6, paragrafo 1, lettera c), del regolamento (UE) 2016/679. Il suddetto obbligo non pregiudica la possibilità di raccogliere dati di registrazione dei nomi di dominio per altri scopi, ad esempio sulla base di accordi contrattuali o di obblighi legali stabiliti in altre normative dell'Unione o nazionali. Tale obbligo mira a ottenere una serie completa e accurata di dati di registrazione e non dovrebbe comportare la raccolta degli stessi dati più volte. I registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero cooperare tra loro al fine di evitare la duplicazione di tale compito.

(110) La disponibilità e la tempestiva accessibilità dei dati di registrazione dei nomi di dominio ai legittimi richiedenti l'accesso sono essenziali per la prevenzione e la lotta agli abusi del DNS, nonché per la prevenzione, l'individuazione e la risposta agli incidenti. Per legittimo richiedente l'accesso si intende qualsiasi persona fisica o giuridica che presenta una richiesta sulla base del diritto dell'Unione o nazionale. Possono comprendere autorità competenti a norma della presente direttiva e autorità competenti a norma del diritto dell'Unione o nazionale in materia di prevenzione, indagine, accertamento o perseguimento di reati, e CERT o CSIRT. I registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero essere tenuti a consentire l'accesso legittimo a specifici dati di registrazione dei nomi di dominio, necessari ai fini della richiesta di accesso, ai legittimi richiedenti l'accesso, in conformità al diritto dell'Unione e nazionale. La richiesta dei legittimi richiedenti l'accesso dovrebbe essere corredata di una motivazione che consenta di valutare la necessità di accedere ai dati.

(111) Al fine di garantire la disponibilità di dati di registrazione dei nomi di dominio accurati e completi, i registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dovrebbero raccogliere i dati di registrazione dei nomi di dominio e garantirne l'integrità e la disponibilità. In particolare, i registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero stabilire politiche e procedure per raccogliere e mantenere i dati di registrazione dei nomi di dominio accurati e completi, nonché per prevenire e rettificare dati di registrazione inesatti in conformità al diritto dell'Unione in materia di protezione dei dati. Tali politiche e procedure dovrebbero tenere conto, nella misura del possibile, delle norme elaborate dalle strutture di governance multipartecipativa a livello internazionale. I registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero adottare e attuare procedure proporzionate per verificare i dati di registrazione dei nomi di dominio. Tali procedure dovrebbero rispecchiare le migliori prassi utilizzate nel settore e, per quanto possibile, i progressi compiuti nel settore dell'identificazione elettronica. Tra gli esempi di procedure di verifica figurano i controlli ex ante effettuati al momento della registrazione e i controlli ex post effettuati dopo la registrazione. I registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero, in particolare, verificare almeno uno degli strumenti di contatto del soggetto che procede alla registrazione.

(112) I registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero essere tenuti a rendere pubblicamente disponibili i dati di registrazione dei nomi di dominio che non rientrano nell'ambito di applicazione delle norme dell'Unione in materia di protezione dei dati, come i dati riguardanti le persone giuridiche, in linea con il preambolo del regolamento (UE) 2016/679. Per le persone giuridiche, i registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero rendere pubblicamente disponibili almeno il nome del soggetto che procede alla registrazione e il numero di telefono di contatto. Anche l'indirizzo di posta elettronica di contatto dovrebbe essere pubblicato, a condizione che non contenga dati personali come alias di posta elettronica o account funzionali. I registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero inoltre consentire l'accesso legittimo a specifici dati di registrazione dei nomi di dominio riguardanti le persone fisiche ai legittimi richiedenti l'accesso, in conformità al diritto dell'Unione in materia di protezione dei dati. Gli Stati membri dovrebbero imporre ai registri dei nomi di dominio di primo livello e ai soggetti che forniscono servizi di registrazione dei nomi di dominio di rispondere senza indebito ritardo alle richieste di divulgazione dei dati di registrazione dei nomi di dominio presentate da legittimi richiedenti l'accesso.

I registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio dovrebbero stabilire politiche e procedure per la pubblicazione e la divulgazione dei dati di registrazione, compresi accordi sul livello dei servizi, ai fini del trattamento delle richieste di accesso dei legittimi richiedenti l'accesso. Tali politiche e procedure dovrebbero tenere conto, nella misura del possibile, di eventuali orientamenti e delle norme elaborate dalle strutture di governance multipartecipativa a livello internazionale. La procedura di accesso potrebbe comprendere l'uso di un'interfaccia, di un portale o di un altro strumento tecnico per fornire un sistema efficiente per la richiesta dei dati di registrazione e l'accesso agli stessi. Al fine di promuovere pratiche armonizzate in tutto il mercato interno, la Commissione può, fatte salve le competenze del comitato europeo per la protezione dei dati, fornire orientamenti su tali procedure che tengano conto, nella misura del possibile, delle norme elaborate dalle strutture di governance multipartecipativa a livello internazionale. Gli Stati membri dovrebbero provvedere affinché tutte le modalità di accesso ai dati di registrazione dei nomi di dominio, a carattere personale e non, siano gratuite.

(113) I soggetti che rientrano nell'ambito di applicazione della presente direttiva dovrebbero essere considerati sotto la giurisdizione dello Stato membro nel quale sono stabiliti. Tuttavia, i fornitori di reti pubbliche di comunicazione elettronica o i fornitori di servizi di comunicazione elettronica accessibili al pubblico dovrebbero essere considerati sotto la giurisdizione dello Stato membro nel quale forniscono i loro servizi. I fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i soggetti che forniscono servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network dovrebbero essere considerati sotto la giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione. Gli enti della pubblica amministrazione dovrebbero rientrare nella giurisdizione dello Stato membro che li ha istituiti. Se fornisce servizi o è stabilito in più di uno Stato membro, il soggetto dovrebbe rientrare nella giurisdizione separata e concorrente di ciascuno di tali Stati membri. Le autorità competenti di tali Stati membri dovrebbero cooperare, prestarsi assistenza reciproca e, ove opportuno, condurre azioni comuni di vigilanza. Qualora esercitino la giurisdizione, gli Stati membri non dovrebbero imporre misure di esecuzione o comminare sanzioni più di una volta per lo stesso comportamento, in linea con il principio del ne bis in idem.

(114) Per tener conto della natura transfrontaliera dei servizi e delle attività dei fornitori di servizi DNS, dei registri dei nomi di dominio di primo livello, dei soggetti che forniscono servizi di registrazione dei nomi di dominio, dei fornitori di servizi di cloud computing, dei fornitori di servizi di data center, dei fornitori di reti di distribuzione dei contenuti, dei fornitori di servizi gestiti, dei fornitori di servizi di sicurezza gestiti, nonché dei fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network, tali soggetti dovrebbero essere posti sotto la giurisdizione di un solo Stato membro. La giurisdizione dovrebbe essere attribuita allo Stato membro in cui il soggetto interessato ha lo stabilimento principale nell'Unione. Il criterio dello stabilimento ai fini della presente direttiva implica l'esercizio effettivo dell'attività nel quadro di un'organizzazione stabile. A tale riguardo non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica. Il rispetto di tale criterio non dovrebbe dipendere dal fatto che i sistemi informatici e di rete siano situati fisicamente in un determinato luogo; la presenza e l'utilizzo dei sistemi in questione non costituiscono di per sé lo stabilimento principale e non sono pertanto criteri decisivi per la sua determinazione. Si dovrebbe considerare che lo stabilimento principale dovrebbe sia nello Stato membro in cui sono prevalentemente adottate nell'Unione le decisioni relative alle misure di gestione dei rischi di cibersicurezza. Ciò corrisponderà di norma alla sede dell'amministrazione centrale dei soggetti nell'Unione. Se non è possibile determinare detto Stato membro o se tali decisioni non sono adottate nell'Unione, si dovrebbe considerare che lo stabilimento principale sia nello Stato membro in cui sono effettuate le operazioni di cibersicurezza. Se non è possibile determinare detto Stato membro, si dovrebbe considerare che lo stabilimento principale sia nello Stato membro in cui il soggetto ha lo stabilimento con il maggior numero di dipendenti nell'Unione. Qualora i servizi siano forniti da un gruppo di imprese, si dovrebbe considerare lo stabilimento principale dell'impresa controllante come lo stabilimento principale del gruppo di imprese.

(115) Quando un servizio DNS ricorsivo accessibile al pubblico è offerto da un fornitore di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico solo come parte del servizio di accesso a internet, il soggetto dovrebbe essere considerato sotto la giurisdizione di tutti gli Stati membri in cui i suoi servizi sono forniti.

(116) Qualora un fornitore di servizi DNS, un registro dei nomi di dominio di primo livello, un soggetto che fornisce servizi di registrazione dei nomi di dominio, un fornitore di servizi di cloud computing, un fornitori di servizi di data center, un fornitore di reti di distribuzione dei contenuti, un fornitore di servizi gestiti, un fornitore di servizi di sicurezza gestiti o un fornitore di un mercato online, di un motore di ricerca online o di una piattaforma di servizi di social network non sia stabilito nell'Unione, ma offra servizi nell'Unione, esso dovrebbe designare un rappresentante nell'Unione. Per determinare se tale soggetto stia offrendo servizi nell'Unione, è opportuno verificare se il soggetto stia progettando di fornire servizi a persone in uno o più Stati membri. La semplice accessibilità nell'Unione del sito web del soggetto o di un intermediario, oppure di un indirizzo di posta elettronica o di altri dati di contatto, o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il soggetto è stabilito, dovrebbe essere considerata insufficiente per accertare tale intenzione. Tuttavia, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare servizi in tale lingua, o la menzione di clienti o utenti che si trovano nell'Unione, potrebbero evidenziare che il soggetto sta progettando di offrire servizi all'interno dell'Unione. Il rappresentante dovrebbe agire a nome del soggetto e le autorità competenti o i CSIRT dovrebbero poterlo contattare. Il rappresentante dovrebbe essere esplicitamente designato mediante mandato scritto del soggetto affinché agisca a suo nome con riguardo agli obblighi di quest'ultimo ai sensi della presente direttiva, compresa la segnalazione di incidenti.

(117) Al fine di garantire una panoramica chiara dei fornitori di servizi DNS, dei registri dei nomi di dominio di primo livello, dei soggetti che forniscono servizi di registrazione dei nomi di dominio, dei fornitori di servizi di cloud computing, dei fornitori di servizi di data center, dei fornitori di reti di distribuzione dei contenuti, dei fornitori di servizi gestiti, dei fornitori di servizi di sicurezza gestiti, nonché dei fornitori di mercati online, di motori di ricerca online o di piattaforme di servizi di social network, che offrono servizi nell'Unione rientranti nell'ambito di applicazione della presente direttiva, l'ENISA dovrebbe creare e mantenere un registro di tali entità, sulla base delle informazioni ricevute dagli Stati membri, se del caso attraverso i meccanismi nazionali istituiti per la loro registrazione. I punti di contatto unici dovrebbero trasmettere all'ENISA le informazioni ed eventuali modifiche apportate. Al fine di garantire l'accuratezza e la completezza delle informazioni che dovrebbero essere incluse in tale registro, gli Stati membri possono trasmettere all'ENISA le informazioni su tali soggetti disponibili in qualsiasi registro nazionale. L'ENISA e gli Stati membri dovrebbero adottare misure per agevolare l'interoperabilità di tali registri, garantendo nel contempo la protezione delle informazioni riservate o classificate. L'ENISA dovrebbe istituire adeguati protocolli di classificazione e gestione delle informazioni per garantire la sicurezza e la riservatezza delle informazioni divulgate e limitare l'accesso, l'archiviazione e la trasmissione di dette informazioni agli utenti destinatari.

(118) Qualora informazioni classificate in conformità al diritto nazionale o dell'Unione siano scambiate, comunicate o altrimenti condivise a norma della presente direttiva, dovrebbero essere applicate le corrispondenti norme sulla gestione delle informazioni classificate. Inoltre, l'ENISA dovrebbe predisporre l'infrastruttura, le procedure e le norme per il trattamento delle informazioni sensibili e classificate in conformità alle norme di sicurezza applicabili alla protezione delle informazioni classificate dell'UE.

(119) Di fronte a minacce informatiche che si fanno sempre più complesse e sofisticate, la validità delle misure di rilevamento e prevenzione dipende in larga misura da una costante condivisione tra i soggetti di informazioni di intelligence relative alle minacce e alle vulnerabilità. La condivisione delle informazioni contribuisce a una maggiore consapevolezza delle minacce informatiche che, a sua volta, accresce la capacità dei soggetti di impedire che tali minacce si trasformino in incidenti e consente ai soggetti di arginare in maniera più efficace gli effetti degli incidenti e di riprendersi in modo più efficiente. In assenza di orientamenti a livello dell'Unione, diversi fattori, tra cui in particolare l'incertezza sulla compatibilità con le norme in materia di concorrenza e responsabilità, sembrano aver ostacolato tale condivisione delle informazioni di intelligence.

(120) È quindi opportuno che i soggetti siano incoraggiati e assistiti dagli Stati membri al fine di sfruttare collettivamente, sul piano strategico, tattico e operativo, le conoscenze e le esperienze pratiche che hanno acquisito a livello individuale al fine di accrescere le loro capacità di prevenire e rilevare adeguatamente gli incidenti, riprendersi da essi, rispondervi o mitigarne gli impatti. È pertanto necessario consentire la creazione a livello dell'Unione di accordi volontari di condivisione delle informazioni in materia di cibersicurezza. A tal fine, gli Stati membri dovrebbero sostenere e incoraggiare attivamente anche i soggetti quali i soggetti che forniscono servizi di cibersicurezza e di ricerca, nonché i soggetti pertinenti che non rientrano nell'ambito di applicazione della presente direttiva, a partecipare a tali accordi di condivisione delle informazioni in materia di cibersicurezza. Tali accordi dovrebbero essere stabiliti in conformità delle norme dell'Unione in materia di concorrenza e di protezione dei dati.

(121) Il trattamento dei dati personali, nella misura necessaria e proporzionata al fine di garantire la sicurezza dei sistemi informatici e di rete da parte di soggetti essenziali e importanti, potrebbe essere considerato lecito in virtù del fatto che tale trattamento è conforme a un obbligo legale cui è soggetto il titolare del trattamento, conformemente ai requisiti di cui all'articolo 6, paragrafo 1, lettera c), e all'articolo 6, paragrafo 3, del regolamento (UE) 2016/679. Il trattamento dei dati personali potrebbe essere necessario anche per i legittimi interessi perseguiti dai soggetti essenziali e importanti, nonché dai fornitori di tecnologie e servizi di sicurezza che agiscono per conto di tali soggetti, a norma dell'articolo 6, paragrafo 1, lettera f), del regolamento (UE) 2016/679, anche qualora tale trattamento sia necessario per accordi di condivisione delle informazioni in materia di cibersicurezza o per la notifica volontaria di informazioni pertinenti a norma della presente direttiva. Le misure relative alla prevenzione, al rilevamento, all'individuazione, al contenimento e all'analisi degli incidenti e alla risposta agli stessi, le misure di sensibilizzazione in relazione a specifiche minacce informatiche, lo scambio di informazioni nel contesto della risoluzione e della divulgazione coordinata delle vulnerabilità, lo scambio volontario di informazioni su tali incidenti, sulle minacce informatiche e sulle vulnerabilità, sugli indicatori di compromissione, sulle tattiche, sulle tecniche e le procedure, sugli allarmi di cibersicurezza e sugli strumenti di configurazione potrebbero richiedere il trattamento di talune categorie di dati personali, quali indirizzi IP, localizzatori uniformi di risorse (URL), nomi di dominio, indirizzi di posta elettronica e, laddove rivelino dati personali, marcature temporali. Il trattamento dei dati personali da parte delle autorità competenti, dei punti di contatto unici e dei CSIRT potrebbe costituire un obbligo legale o essere considerato necessario per svolgere un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento ai sensi dell'articolo 6, paragrafo 1, lettera c) o e), e dell'articolo 6, paragrafo 3, del regolamento (UE) 2016/679, o per perseguire un interesse legittimo dei soggetti essenziali e importanti di cui all'articolo 6, paragrafo 1, lettera f), di tale regolamento. Inoltre, il diritto nazionale potrebbe stabilire norme che consentano alle autorità competenti, ai punti di contatto unici e ai CSIRT, nella misura necessaria e proporzionata al fine di garantire la sicurezza dei sistemi informatici e di rete dei soggetti essenziali e importanti, di trattare categorie particolari di dati personali conformemente all'articolo 9 del regolamento (UE) 2016/679, in particolare prevedendo misure adeguate e specifiche per tutelare i diritti e gli interessi fondamentali delle persone fisiche, comprese limitazioni tecniche al riutilizzo di tali dati e l'uso di misure all'avanguardia in materia di sicurezza e di tutela della vita privata, quali la pseudonimizzazione o la cifratura qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita.

(122) Al fine di rafforzare i poteri e le misure di vigilanza che contribuiscono a garantire l'effettiva conformità, la presente direttiva dovrebbe prevedere un elenco minimo di misure e mezzi di vigilanza attraverso i quali le autorità competenti possono vigilare sui soggetti essenziali e importanti. La presente direttiva dovrebbe inoltre stabilire una differenziazione del regime di vigilanza tra i soggetti essenziali e i soggetti importanti al fine di garantire un giusto equilibrio degli obblighi per tali soggetti e per le autorità competenti. Pertanto, i soggetti essenziali dovrebbero essere sottoposti a un regime di vigilanza completo, ex ante ed ex post, mentre i soggetti importanti dovrebbero essere sottoposti a un regime di vigilanza leggero, solo ex post. I soggetti importanti non dovrebbero quindi essere tenuti a documentare sistematicamente il rispetto delle misure di gestione dei rischi di cibersicurezza, mentre le autorità competenti dovrebbero attuare un approccio ex post reattivo alla vigilanza e, di conseguenza, non dovrebbero avere un obbligo generale di vigilanza su tali soggetti. La vigilanza ex post di soggetti importanti può essere innescata da elementi di prova, indicazioni o informazioni portati all'attenzione delle autorità competenti che tali autorità ritengono suggerire possibili violazioni della presente direttiva. Ad esempio, tali elementi di prova, indicazioni o informazioni potrebbero essere del tipo fornito alle autorità competenti da altre autorità, soggetti, cittadini, media o altre fonti o informazioni disponibili al pubblico, o emergere nel corso di altre attività svolte dalle autorità competenti nell'adempimento dei loro compiti.

(123) L'esecuzione dei compiti di vigilanza da parte delle autorità competenti non dovrebbe ostacolare inutilmente le attività commerciali del soggetto interessato. Nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti essenziali, tra cui lo svolgimento di ispezioni in loco e la vigilanza a distanza, le indagini sui casi di violazione della presente direttiva e lo svolgimento di audit sulla sicurezza o scansioni di sicurezza, le autorità competenti dovrebbero ridurre al minimo l'impatto sulle attività commerciali del soggetto interessato.

(124) Nell'esercizio della vigilanza ex ante, le autorità competenti dovrebbero poter decidere in modo proporzionato l'ordine di priorità nel ricorso alle misure e ai mezzi di vigilanza a loro disposizione. Ciò implica che le autorità competenti possano decidere l'ordine di priorità sulla base di metodologie di vigilanza che dovrebbero seguire un approccio basato sui rischi. Più specificamente, tali metodologie potrebbero includere criteri o parametri di riferimento per la classificazione dei soggetti essenziali in categorie di rischio e corrispondenti misure e mezzi di vigilanza raccomandati per categoria di rischio, quali l'uso, la frequenza o il tipo di ispezioni in loco, audit sulla sicurezza mirati o scansioni di sicurezza, il tipo di informazioni da richiedere e il livello di dettaglio di tali

informazioni. Tali metodologie di vigilanza potrebbero inoltre essere corredate da programmi di lavoro ed essere valutate e riesaminate periodicamente, anche per quanto riguarda aspetti quali l'assegnazione e il fabbisogno di risorse. In relazione agli enti della pubblica amministrazione, i poteri di vigilanza dovrebbero essere esercitati in linea con i quadri legislativi e istituzionali nazionali.

(125) Le autorità competenti dovrebbero provvedere affinché i loro compiti di vigilanza nei confronti dei soggetti essenziali e importanti siano svolti da professionisti formati, che dovrebbero disporre delle competenze necessarie per svolgere tali compiti, in particolare per quanto riguarda lo svolgimento di ispezioni in loco e la vigilanza a distanza, compresa l'individuazione di carenze nelle banche dati, nell'hardware, nei firewall, nella cifratura e nelle reti. Tali ispezioni e tale supervisione dovrebbero essere condotte in modo obiettivo.

(126) In casi debitamente giustificati in cui sia a conoscenza di una minaccia informatica significativa o di un rischio imminente, l'autorità competente dovrebbe essere in grado di adottare decisioni di esecuzione immediata al fine di prevenire un incidente o di rispondervi.

(127) Al fine di rendere efficace l'esecuzione, è opportuno stabilire un elenco minimo di competenze di esecuzione che possono essere esercitate in caso di violazione delle misure di gestione e segnalazione dei rischi di cibersicurezza previsti dalla presente direttiva, istituendo un quadro chiaro e coerente per tali misure di esecuzione in tutta l'Unione. Occorre tenere debitamente conto della natura, della gravità e della durata del danno materiale o immateriale causato, del carattere doloso o colposo della violazione della presente direttiva, delle azioni intraprese per prevenire o attenuare il danno materiale o immateriale, del grado di responsabilità o di eventuali violazioni precedenti pertinenti, del grado di cooperazione con l'autorità competente e di qualsiasi altro fattore aggravante o attenuante. Le misure di esecuzione, comprese le sanzioni amministrative pecuniarie, dovrebbero essere proporzionate e la loro imposizione dovrebbe essere soggetta a garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta dei diritti fondamentali dell'Unione europea («Carta»), inclusi il diritto a un ricorso effettivo e a un giusto processo, la presunzione di innocenza e i diritti della difesa.

(128) La presente direttiva non impone agli Stati membri di prevedere la responsabilità penale o civile delle persone fisiche incaricate di garantire la conformità di un soggetto alla presente direttiva per i danni subiti da terzi a seguito di una violazione della stessa.

(129) Al fine di garantire l'efficace applicazione degli obblighi stabiliti nella presente direttiva, ciascuna autorità competente dovrebbe avere il potere di imporre o chiedere l'imposizione di sanzioni amministrative pecuniarie.

(130) Qualora una sanzione amministrativa pecuniaria sia comminata a un soggetto essenziale o importante che è un'impresa, quest'ultima dovrebbe essere intesa quale impresa conformemente agli articoli 101 e 102 TFUE a tali fini. Qualora una sanzione amministrativa pecuniaria sia comminata a una persona che non sia impresa, l'autorità competente dovrebbe tenere conto del livello generale di reddito nello Stato membro come pure della situazione economica della persona nel valutare l'importo appropriato della sanzione pecuniaria. Dovrebbe spettare agli Stati membri determinare se e in che misura le autorità pubbliche debbano essere soggette a sanzioni amministrative pecuniarie. L'imposizione di una sanzione amministrativa pecuniaria non pregiudica l'applicazione di altri poteri da parte delle autorità competenti o di altre sanzioni previste dalle norme nazionali di recepimento della presente direttiva.

(131) Gli Stati membri dovrebbero poter stabilire le norme relative alle sanzioni penali in caso di violazione delle norme nazionali di recepimento della presente direttiva. Tuttavia, l'imposizione di sanzioni penali per le violazioni di tali norme nazionali e delle relative sanzioni amministrative non dovrebbe essere in contrasto con il principio del ne bis in idem quale interpretato dalla Corte di giustizia dell'Unione europea.

(132) Qualora la presente direttiva non armonizzi le sanzioni amministrative o ove necessario in altri casi, ad esempio in caso di violazione grave degli obblighi della presente direttiva, gli Stati membri dovrebbero attuare un sistema che preveda sanzioni effettive, proporzionate e dissuasive. La natura di tali sanzioni, e se esse siano penali o amministrative, dovrebbe essere determinata dalla legislazione nazionale.

(133) Al fine di rafforzare ulteriormente l'efficacia e il carattere dissuasivo delle misure di esecuzione applicabili alle violazioni della presente direttiva, le autorità competenti dovrebbero avere la facoltà di sospendere temporaneamente o di richiedere la sospensione temporanea di una certificazione o di un'autorizzazione relativa a una parte o alla totalità dei servizi pertinenti forniti o dalle attività effettuate da un soggetto essenziale e richiedere l'imposizione di un divieto temporaneo all'esercizio di funzioni dirigenziali da parte di qualsiasi persona fisica che svolga funzioni dirigenziali a livello di amministratore delegato o rappresentante legale. Data la loro gravità e l'impatto sulle attività dei soggetti e, in ultima analisi, sugli utenti, tali sospensioni o divieti temporanei dovrebbero essere applicati solo in proporzione alla gravità della violazione e tenendo conto delle circostanze di ciascun singolo caso, tra cui il carattere doloso o colposo della violazione e qualsiasi azione intrapresa per prevenire o attenuare il danno materiale o immateriale Tali sospensioni o divieti temporanei dovrebbero essere applicati solo come ultima ratio, vale a dire solo una volta esaurite le altre pertinenti misure di esecuzione previste dalla presente direttiva, e solo fino a quando il soggetto interessato non adotti le misure necessarie per rimediare alle carenze o per conformarsi alle prescrizioni dell'autorità competente per cui tali sospensioni o divieti temporanei sono stati applicati. L'imposizione di tali sospensioni o i divieti temporanei dovrebbe essere soggetta a garanzie procedurali appropriate in conformità ai principi generali del diritto dell'Unione e della Carta, inclusi il diritto a un ricorso effettivo e ad un giusto processo, la presunzione di innocenza e i diritti della difesa.

(134) Al fine di garantire l'adempimento, da parte dei soggetti, degli obblighi di cui alla presente direttiva, gli Stati membri dovrebbero cooperare e prestarsi reciproca assistenza per quanto riguarda le misure di vigilanza e di applicazione, in particolare quando un soggetto fornisce servizi in più di uno Stato membro o quando i suoi sistemi informatici e di rete sono situati in uno Stato membro diverso da quello in cui presta servizi. Nel fornire assistenza, l'autorità competente interpellata dovrebbe adottare misure di vigilanza o di esecuzione conformemente al diritto nazionale. Onde garantire il buon funzionamento dell'assistenza reciproca ai sensi della presente direttiva, le autorità competenti dovrebbero avvalersi del gruppo di cooperazione quale forum per esaminare i singoli casi e le richieste di assistenza.

(135) Al fine di garantire una vigilanza e un'esecuzione efficaci, in particolare quando la situazione ha una dimensione transfrontaliera, gli Stati membri che hanno ricevuto una richiesta di assistenza reciproca dovrebbero, nei limiti di tale richiesta, adottare misure di vigilanza e di esecuzione adeguate in relazione al soggetto oggetto di tale richiesta, e che fornisce servizi o che dispone di sistemi informatici e di una rete sul territorio di tale Stato membro.

(136) La presente direttiva dovrebbe stabilire norme di cooperazione tra le autorità competenti e le autorità di controllo nel quadro del regolamento (UE) 2016/679 per far fronte alle violazioni della presente direttiva relative ai dati personali.

(137) La presente direttiva dovrebbe mirare a garantire un elevato livello di responsabilità per le misure di gestione dei rischi di cibersicurezza e gli obblighi di segnalazione a livello di soggetti essenziali e importanti. Pertanto, gli organi di gestione dei soggetti essenziali e importanti dovrebbero approvare le misure di gestione dei rischi di cibersicurezza e sorvegliarne l'attuazione.

(138) Al fine di garantire un livello comune elevato di cibersicurezza in tutta l'Unione sulla base della presente direttiva, conformemente all'articolo 290 TFUE alla Commissione dovrebbe essere delegato il potere di adottare atti per quanto riguarda l'integrazione della presente direttiva specificando quali categorie di soggetti essenziali e importanti debbano essere tenute ad utilizzare determinati prodotti TIC, servizi TIC e processi TIC certificati o ad ottenere un certificato nell'ambito di un sistema europeo di certificazione della cibersicurezza. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016 ([22]). In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti hanno sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

([22]) GU L 123 del 12.5.2016, pag. 1.

(139) Al fine di garantire condizioni uniformi per l'attuazione della presente direttiva, dovrebbero essere attribuite alla Commissione competenze di esecuzione per stabilire le modalità procedurali necessarie per il funzionamento del gruppo di cooperazione e i requisiti tecnici e metodologici nonché settoriali relativi alle misure di gestione del rischio di cibersicurezza, e per specificare ulteriormente il tipo di informazioni, il formato e la procedura degli incidenti, delle minacce informatiche e delle notifiche quasi assenti e delle comunicazioni significative relative a minacce informatiche, nonché i casi in cui un incidente deve essere considerato significativo. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([23]).

(140) È opportuno che la Commissione riesamini la presente direttiva a scadenze regolari, dopo aver consultato le parti interessate, in particolare al fine valutare se sia opportuno proporre modifiche alla luce dei cambiamenti delle condizioni sociali, politiche, tecnologiche o del mercato. Nel quadro di tali riesami, la Commissione dovrebbe valutare la pertinenza delle dimensioni dei soggetti interessati, e i settori, dei sottosettori e dei tipi di soggetto di cui agli allegati della presente direttiva ai fini del funzionamento dell'economia e della società per quanto riguarda la cibersicurezza. La Commissione dovrebbe valutare, tra l'altro, se i fornitori, che ricadono nell'ambito di applicazione della presente direttiva, designati come piattaforme online di dimensioni molto grandi ai sensi dell'articolo 33 del regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio ([24]) possano essere identificati come soggetti essenziali ai sensi della presente direttiva.

(141) La presente direttiva istituisce nuovi compiti per l'ENISA, rafforzando in tal modo il suo ruolo, e potrebbe anche portare l'ENISA a dover svolgere i suoi compiti a norma del regolamento (UE) 2019/881 a un livello più alto di prima. Al fine di garantire che l'ENISA disponga delle risorse finanziarie e umane necessarie per svolgere le funzioni esistenti e nuove, nonché per soddisfare eventuali livelli più elevati di esecuzione di tali funzioni derivanti dal suo ruolo rafforzato, il suo bilancio dovrebbe essere aumentato di conseguenza. Inoltre, al fine di garantire un uso efficiente delle risorse, all'ENISA dovrebbe essere data maggiore flessibilità nel modo in cui è in grado di assegnare risorse internamente, in modo che possa svolgere i suoi compiti e soddisfare le aspettative in modo efficace.

(142) Poiché l'obiettivo della presente direttiva, vale a dire conseguire un elevato livello comune di cibersicurezza nell'Unione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo degli effetti dell'azione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. La presente direttiva si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(143) La presente direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti dalla Carta, in particolare il diritto al rispetto della vita privata e delle comunicazioni, la protezione dei dati personali, la libertà d'impresa, il diritto alla proprietà, il diritto a un ricorso effettivo e ad un giudice imparziale, la presunzione d'innocenza e i diritti della difesa. Il diritto a un ricorso effettivo si estende ai destinatari di servizi forniti da soggetti essenziali e importanti. La presente direttiva dovrebbe essere attuata in conformità a tali diritti e principi.

(144) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([25]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere l'11 marzo 2021 ([26]),

---

([23]) Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

([24]) Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) (GU L 277 del 27.10.2022, pag. 1).

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

([26]) GU C 183 dell'11.5.2021, pag. 3.

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto e ambito di applicazione

1. La presente direttiva stabilisce misure volte a garantire un livello comune elevato di cibersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno.

2. A tal fine, la presente direttiva stabilisce:

a) obblighi che impongono agli Stati membri di adottare strategie nazionali in materia di cibersicurezza e di designare o creare autorità nazionali competenti, autorità di gestione delle crisi informatiche, punti di contatto unici in materia di sicurezza (punti di contatto unici) e team di risposta agli incidenti di sicurezza informatica (CSIRT);

b) misure in materia di gestione dei rischi di cibersicurezza e obblighi di segnalazione per i soggetti di un tipo di cui all'allegato I o II nonché per soggetti identificati come critici ai sensi della direttiva (UE) 2022/2557;

c) norme e obblighi in materia di condivisione delle informazioni sulla cibersicurezza;

d) obblighi in materia di vigilanza ed esecuzione per gli Stati membri.

Articolo 2

Ambito di applicazione

1. La presente direttiva si applica ai soggetti pubblici o privati delle tipologie di cui all'allegato I o II che sono considerati medie imprese ai sensi all'articolo 2, paragrafo 1, dell'allegato alla raccomandazione 2003/361/CE, o che superano i massimali per le medie imprese di cui al paragrafo 1 di tale articolo, e che prestano i loro servizi o svolgono le loro attività all'interno dell'Unione.

L'articolo 3, paragrafo 4, dell'allegato a tale raccomandazione non si applica ai fini della presente direttiva.

2. La presente direttiva si applica anche ai soggetti, indipendentemente dalle loro dimensioni, delle tipologie di cui all'allegato I o II qualora:

a) i servizi siano forniti da:

   i) fornitori di reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica accessibili al pubblico;

   ii) prestatore di servizi di fiducia;

   iii) registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio;

b) il soggetto sia l'unico fornitore in uno Stato membro di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali;

c) una perturbazione del servizio fornito dal soggetto potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;

d) una perturbazione del servizio fornito dal soggetto potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;

e) il soggetto sia critico in ragione della sua particolare importanza a livello nazionale regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nello Stato membro;

f) il soggetto è un ente della pubblica amministrazione:

i) dell'amministrazione centrale quale definito da uno Stato membro conformemente al diritto nazionale; o

ii) a livello regionale quale definito da uno Stato membro conformemente al diritto nazionale che, a seguito di una valutazione basata sul rischio, fornisce servizi la cui perturbazione potrebbe avere un impatto significativo su attività sociali o economiche critiche.

3. La presente direttiva si applica ai soggetti, indipendentemente dalle loro dimensioni, identificati come soggetti critici ai sensi della direttiva (UE) 2022/2557.

4. La presente direttiva si applica ai soggetti, indipendentemente dalle loro dimensioni, che forniscono servizi di registrazione dei nomi di dominio.

5. Gli Stati membri possono prevedere che la presente direttiva si applichi a:

a) enti della pubblica amministrazione a livello locale;

b) istituti di istruzione, in particolare ove svolgano attività di ricerca critiche.

6. La presente direttiva lascia impregiudicata la responsabilità degli Stati membri di tutelare la sicurezza nazionale e il loro potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia dell'integrità territoriale dello Stato e il mantenimento dell'ordine pubblico.

7. La presente direttiva non si applica agli enti della pubblica amministrazione che svolgono le loro attività nei settori della sicurezza nazionale, della pubblica sicurezza o della difesa, del contrasto, comprese la prevenzione, le indagini, l'accertamento e il perseguimento dei reati.

8. Gli Stati membri possono esentare soggetti specifici che svolgono attività nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o del contrasto, compresi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati, o che forniscono servizi esclusivamente agli enti della pubblica amministrazione di cui al paragrafo 7 del presente articolo, dal rispetto degli obblighi di cui all'articolo 21 o all'articolo 23 per quanto riguarda tali attività o servizi. In tali casi, le misure di vigilanza e di applicazione di cui al capo VII non si applicano in relazione a tali attività o servizi specifici. Qualora i soggetti svolgano attività o prestino servizi esclusivamente del tipo di cui al presente paragrafo, gli Stati membri possono anche decidere di esentare tali enti dagli obblighi di cui agli articoli 3 e 27.

9. I paragrafi 7 e 8 non si applicano quando un soggetto agisce in qualità di prestatore di servizi fiduciari.

10. La presente direttiva non si applica ai soggetti che gli Stati membri hanno esentato dall'ambito di applicazione del regolamento (UE) 2022/2554 ai sensi dell'articolo 2, paragrafo 4, di tale regolamento.

11. Gli obblighi stabiliti nella presente direttiva non comportano la fornitura di informazioni la cui divulgazione sia contraria agli interessi essenziali degli Stati membri in materia di sicurezza nazionale, pubblica sicurezza o difesa.

12. La presente direttiva si applica fatti salvi il regolamento (UE) 2016/679, la direttiva 2002/58/CE, le direttive 2011/93/UE ([27]) e 2013/40/UE ([28]) del Parlamento europeo e del Consiglio e la direttiva (UE) 2022/2557.

13. Fatto salvo l'articolo 346 TFUE, le informazioni riservate ai sensi della normativa dell'Unione o nazionale, quale quella sulla riservatezza commerciale, sono scambiate con la Commissione e con altre autorità competenti conformemente alla presente direttiva solo nella misura in cui tale scambio sia necessario ai fini dell'applicazione della presente direttiva. Le informazioni scambiate sono limitate alle informazioni pertinenti e commisurate a tale scopo. Lo scambio di informazioni tutela la riservatezza di dette informazioni e protegge la sicurezza e gli interessi commerciali di soggetti interessati.

([27]) Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio (GU L 335 del 17.12.2011, pag. 1).

([28]) Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio (GU L 218 del 14.8.2013, pag. 8).

14. I soggetti, le autorità competenti, i punti di contatto unici e i CSIRT trattano i dati personali nella misura necessaria ai fini della presente direttiva e conformemente al regolamento (UE) 2016/679, in particolare tale trattamento si basa sull'articolo 6 dello stesso.

Il trattamento dei dati personali a norma della presente direttiva da parte dei fornitori di reti pubbliche di comunicazione elettronica o dei fornitori di comunicazioni elettroniche accessibili al pubblico viene effettuato in conformità della legislazione dell'Unione in materia di protezione dei dati e della legislazione dell'Unione in materia di riservatezza, segnatamente la direttiva 2002/58/CE.

Articolo 3

Soggetti essenziali e importanti

1. Ai fini della presente direttiva, sono considerati soggetti essenziali i seguenti:

a) soggetti di cui all'allegato I che superano i massimali per le medie imprese di cui all'articolo 2, paragrafo 1, dell'allegato della raccomandazione 2003/361/CE;

b) prestatori di servizi fiduciari qualificati e registri dei nomi di dominio di primo livello, nonché prestatori di servizi DNS, indipendentemente dalle loro dimensioni;

c) fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico che si considerano medie imprese ai sensi dell'articolo 2, dell'allegato alla raccomandazione 2003/361/CE;

d) i soggetti della pubblica amministrazione di cui all'articolo 2, paragrafo 2, lettera f), punto i);

e) qualsiasi altro soggetto di cui all'allegato I o II che uno Stato membro identifica come soggetti essenziali ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e);

f) soggetti identificati come soggetti critici ai sensi della direttiva (UE) 2022/2557, di cui all'articolo 2, paragrafo 3 della presente direttiva;

g) se lo Stato membro lo prevede, i soggetti che tale Stato membro ha identificato prima del 16 gennaio 2023 come operatori di servizi essenziali a norma della direttiva (UE) 2016/1148 o del diritto nazionale.

2. Ai fini della presente direttiva, sono considerati soggetti importanti i soggetti di una tipologia elencata negli allegati I o II che non sono considerati soggetti essenziali ai sensi del paragrafo 1 del presente articolo. Ciò comprende soggetti identificati dagli Stati membri come soggetti importanti ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e);

3. Entro il 17 aprile 2025, gli Stati membri definiscono un elenco dei soggetti essenziali ed importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio. Successivamente, gli Stati membri riesaminano l'elenco periodicamente, almeno ogni due anni e, se opportuno, lo aggiornano.

4. Ai fini della compilazione dell'elenco di cui al paragrafo 3, gli Stati membri impongono alle entità di cui a tale paragrafo di presentare alle autorità competenti almeno le informazioni seguenti:

a) il proprio nome;

b) l'indirizzo e i recapiti aggiornati, compresi gli indirizzi e-mail, le serie di IP e i numeri di telefono;

c) se del caso, i settori e sottosettori pertinenti di cui all'allegato I o II; e

d) se del caso, un elenco degli Stati membri in cui forniscono servizi che rientrano nell'ambito di applicazione della presente direttiva.

I soggetti di cui al paragrafo 3 notificano tempestivamente qualsiasi modifica delle informazioni trasmesse a norma del primo comma del presente paragrafo e in ogni caso entro due settimane dalla data della modifica.

La Commissione, assistita dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA), fornisce senza indebito ritardo orientamenti e modelli relativi agli obblighi di cui al presente paragrafo.

Gli Stati membri possono istituire meccanismi nazionali che consentano alle entità di registrarsi.

5. Entro il 17 aprile 2025 e successivamente ogni due anni, le autorità competenti notificano:

a) alla Commissione e al gruppo di coordinamento, il numero dei soggetti essenziali e importanti elencati ai sensi del paragrafo 3 per ciascun settore e sottosettore di cui all'allegato I o II; e

b) alla Commissione informazioni pertinenti sul numero di soggetti essenziali e importanti individuati ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e), sul settore e il sottosettore di cui all'allegato I o II cui appartengono, sul tipo di servizio che forniscono e sulla fornitura, tra quelli stabiliti all'articolo 2, paragrafo 2, lettere da b) a e), ai sensi dei quali sono stati individuati.

6. Sino al 17 aprile 2025 e su richiesta della Commissione, gli Stati membri possono notificare alla Commissione i nomi dei soggetti essenziali e importanti di cui al paragrafo 5, lettera b).

Articolo 4

Atti giuridici settoriali dell'Unione

1. Qualora gli atti giuridici settoriali dell'Unione facciano obbligo ai soggetti essenziali o importanti di adottare misure di gestione dei rischi di cibersicurezza o di notificare gli incidenti significativi, nella misura in cui gli effetti di tali obblighi siano almeno equivalenti a quelli degli obblighi di cui alla presente direttiva, a tali soggetti non si applicano le pertinenti disposizioni della presente direttiva, comprese le disposizioni relative alla vigilanza e all'esecuzione di cui al capo VII. Qualora gli atti giuridici settoriali dell'Unione non contemplino tutti i soggetti di un settore specifico che rientra nell'ambito di applicazione della presente direttiva, le pertinenti disposizioni della presente direttiva continuano ad applicarsi ai soggetti non contemplati da tali atti giuridici settoriali dell'Unione.

2. I requisiti di cui al paragrafo 1 del presente articolo sono considerati di effetto equivalente agli obblighi stabiliti dalla presente direttiva qualora:

a) gli effetti delle misure di gestione dei rischi di cibersicurezza siano almeno equivalenti a quelli delle misure di cui all'articolo 21, paragrafi 1 e 2; oppure

b) l'atto giuridico settoriale dell'Unione preveda l'accesso immediato, se del caso automatico e diretto, alle notifiche degli incidenti da parte dei CSIRT, delle autorità competenti o dei punti di contatto unici a norma della presente direttiva e qualora gli obblighi di notifica degli incidenti significativi abbiano un effetto almeno equivalente a quelli di cui all'articolo 23, paragrafi da 1 a 6, della presente direttiva.

3. La Commissione, entro il 17 luglio 2023, fornisce orientamenti che chiariscano l'applicazione dei paragrafi 1 e 2. La Commissione rivede tali orientamenti periodicamente. Nella preparazione di detti orientamenti, la Commissione tiene conto delle osservazioni del gruppo di cooperazione e dell'ENISA.

Articolo 5

Armonizzazione minima

La presente direttiva non impedisce agli Stati membri di adottare o mantenere disposizioni che garantiscano un livello più elevato di cibersicurezza, a condizione che tali disposizioni siano coerenti con gli obblighi degli Stati membri stabiliti dal diritto dell'Unione.

Articolo 6

Definizioni

Ai fini della presente direttiva si applicano le definizioni seguenti:

1) «sistema informatico e di rete»:

   a) una rete di comunicazione elettronica quale definita all'articolo 2, punto 1, della direttiva (UE) 2018/1972;

b) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base a un programma, un'elaborazione automatica di dati digitali; o

c) i dati digitali conservati, elaborati, estratti o trasmessi per mezzo degli elementi di cui alle lettere a) e b), ai fini del loro funzionamento, del loro uso, della loro protezione e della loro manutenzione;

2) «sicurezza dei sistemi informatici e di rete»: la capacità dei sistemi informatici e di rete di resistere, con un determinato livello di confidenza, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi;

3) «cibersicurezza»: la cibersicurezza quale definita all'articolo 2, punto 1), del regolamento (UE) 2019/881;

4) «strategia nazionale per la cibersicurezza»: un quadro coerente di uno Stato membro che prevede priorità e obiettivi strategici in materia di cibersicurezza e la governance per il loro conseguimento in tale Stato membro;

5) «quasi incidente»: un evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato;

6) «incidente»: un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi;

7) «incidente di cibersicurezza su vasta scala»: un incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri;

8) «gestione degli incidenti»: le azioni e le procedure volte a prevenire, rilevare, analizzare e contenere un incidente o a rispondervi e riprendersi da esso;

9) «rischio»: la potenziale perdita o perturbazione causata da un incidente; è espresso come combinazione dell'entità di tale perdita o perturbazione e della probabilità che l'incidente si verifichi;

10) «minaccia informatica»: una minaccia informatica quale definita all'articolo 2, punto 8), del regolamento (UE) 2019/881;

11) «minaccia informatica significativa»: una minaccia informatica che, in base alle sue caratteristiche tecniche, si presume possa avere un grave impatto sui sistemi informatici e di rete di un soggetto o degli utenti di tali servizi del soggetto causando perdite materiali o immateriali considerevoli;

12) «prodotto TIC»: un prodotto TIC quale definito all'articolo 2, punto 12), del regolamento (UE) 2019/881;

13) «servizio TIC»: un servizio TIC quale definito all'articolo 2, punto 13), del regolamento (UE) 2019/881;

14) «processo TIC»: un processo TIC quale definito all'articolo 2, punto 14), del regolamento (UE) 2019/881;

15) «vulnerabilità»: un punto debole, una suscettibilità o un difetto di prodotti TIC o servizi TIC che può essere sfruttato da una minaccia informatica;

16) «norma»: una norma quale definita all'articolo 2, punto 1), del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio ([29]);

17) «specifica tecnica»: una specifica tecnica quale definita all'articolo 2, punto 4), del regolamento (UE) n. 1025/2012;

([29]) Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12).

18) «punto di interscambio internet»: un'infrastruttura di rete che consente l'interconnessione di più di due reti indipendenti (sistemi autonomi), principalmente al fine di agevolare lo scambio del traffico internet, che fornisce interconnessione soltanto ai sistemi autonomi e che non richiede che il traffico internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo né altera o interferisce altrimenti con tale traffico;

19) «sistema dei nomi di dominio» o «DNS»: un sistema di nomi gerarchico e distribuito che consente l'identificazione di servizi e risorse su internet, permettendo ai dispositivi degli utenti finali di utilizzare i servizi di inoltro e connettività di internet al fine di accedere a tali servizi e risorse;

20) «fornitore di servizi DNS»: un soggetto che fornisce:

a) servizi di risoluzione dei nomi di dominio ricorsivi accessibili al pubblico per gli utenti finali di internet; o

b) servizi di risoluzione dei nomi di dominio autorevoli per uso da parte di terzi, fatta eccezione per i server dei nomi radice;

21) «registro dei nomi di dominio di primo livello» o «registro dei nomi TLD»: un soggetto cui è stato delegato uno specifico dominio di primo livello (TLD) e che è responsabile dell'amministrazione di tale TLD, compresa la registrazione dei nomi di dominio sotto tale TLD, e del funzionamento tecnico di tale TLD, compresi il funzionamento dei server dei nomi, la manutenzione delle banche dati e la distribuzione dei file di zona TLD tra i server dei nomi, indipendentemente dal fatto che una qualsiasi di tali operazioni sia effettuata dal soggetto stesso o sia esternalizzata, ma escludendo le situazioni in cui i nomi TLD sono utilizzati da un registro esclusivamente per uso proprio;

22) «soggetto che fornisce servizi di registrazione di nomi di dominio»: un registrar o un agente che agisce per conto di registrar, come un fornitore o un rivenditore di servizi di registrazione per la privacy o di proxy;

23) «servizio digitale»: un servizio quale definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio ([30]);

24) «servizio fiduciario»: un servizio fiduciario quale definito all'articolo 3, punto 16), del regolamento (UE) n. 910/2014;

25) «prestatore di servizi fiduciari»: un prestatore di servizi fiduciari quale definito all'articolo 3, punto 19), del regolamento (UE) n. 910/2014;

26) «servizio fiduciario qualificato»: un servizio fiduciario qualificato quale definito all'articolo 3, punto 17), del regolamento (UE) n. 910/2014;

27) «prestatore di servizi fiduciari qualificato»: un prestatore di servizi fiduciari qualificato quale definito all'articolo 3, punto 20), del regolamento (UE) n. 910/2014;

28) «mercato online»: un mercato online quale definito all'articolo 2, lettera n), della direttiva 2005/29/CE del Parlamento europeo e del Consiglio ([31]);

29) «motore di ricerca online»: un motore di ricerca online quale definito all'articolo 2, punto 5), del regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio ([32]);

30) «servizio di cloud computing»: un servizio digitale che consente l'amministrazione su richiesta di un pool scalabile ed elastico di risorse di calcolo condivisibili e l'ampio accesso remoto a quest'ultimo, anche ove tali risorse sono distribuite in varie ubicazioni.

([30]) Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (GU L 241 del 17.9.2015, pag. 1).

([31]) Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali delle imprese nei confronti dei consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio («direttiva sulle pratiche commerciali sleali») (GU L 149 dell'11.6.2005, pag. 22).

([32]) Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online (GU L 186 dell'11.7.2019, pag. 57).

31) «servizio di data center»: un servizio che comprende strutture, o gruppi di strutture, dedicate a ospitare, interconnettere e far funzionare in modo centralizzato apparecchiature informatiche e di rete che forniscono servizi di conservazione, elaborazione e trasporto di dati insieme a tutti gli impianti e le infrastrutture per la distribuzione dell'energia e il controllo ambientale;

32) «rete di distribuzione dei contenuti (*content delivery network*)»: una rete di server distribuiti geograficamente allo scopo di garantire l'elevata disponibilità, l'accessibilità o la rapida distribuzione di contenuti e servizi digitali agli utenti di internet per conto di fornitori di contenuti e servizi;

33) «piattaforma di servizi di social network»: una piattaforma che consente agli utenti finali di entrare in contatto, condividere, scoprire e comunicare gli uni con gli altri su molteplici dispositivi, in particolare, attraverso chat, post, video e raccomandazioni;

34) «rappresentante»: una persona fisica o giuridica stabilita nell'Unione espressamente designata ad agire per conto di un fornitore di servizi DNS, un registro dei nomi TLD, un soggetto che fornisce servizi di registrazione di nomi di dominio, un fornitore di servizi di cloud computing, un fornitore di servizi di data center, un fornitore di reti di distribuzione dei contenuti, un fornitore di servizi gestiti, un fornitore di servizi di sicurezza gestiti, o un fornitore di mercato online, di un motore di ricerca online o di una piattaforma di servizi di social network che non è stabilito nell'Unione, a cui l'autorità nazionale competente o un CSIRT può rivolgersi in luogo del soggetto per quanto riguarda gli obblighi di quest'ultimo a norma della presente direttiva;

35) «ente della pubblica amministrazione»: un soggetto riconosciuto come tale in uno Stato membro conformemente al diritto nazionale, che non comprende la magistratura, i parlamenti e le banche centrali, che soddisfa i criteri seguenti:

    a) è istituito allo scopo di soddisfare esigenze di interesse generale e non ha carattere industriale o commerciale;

    b) è dotato di personalità giuridica o è autorizzato per legge ad agire a nome di un altro soggetto dotato di personalità giuridica;

    c) è finanziato in modo maggioritario dallo Stato, da autorità regionali o da altri organismi di diritto pubblico, la sua gestione è soggetta alla vigilanza di tali autorità o organismi, oppure è dotato di un organo di amministrazione, di direzione o di vigilanza in cui più della metà dei membri è designata dallo Stato, da autorità regionali o da altri organismi di diritto pubblico;

    d) ha il potere di adottare, nei confronti di persone fisiche o giuridiche, decisioni amministrative o normative che incidono sui loro diritti relativi alla circolazione transfrontaliera delle merci, delle persone, dei servizi o dei capitali;

36) «rete pubblica di comunicazione elettronica»: una rete pubblica di comunicazione elettronica quale definita all'articolo 2, punto 8), della direttiva (UE) 2018/1972;

37) «servizio di comunicazione elettronica»: un servizio di comunicazione elettronica quale definito all'articolo 2, punto 4), della direttiva (UE) 2018/1972;

38) «soggetto»: una persona fisica o giuridica, costituita e riconosciuta come tale conformemente al diritto nazionale applicabile nel suo luogo di stabilimento, che può, agendo in nome proprio, esercitare diritti ed essere soggetta a obblighi;

39) «fornitore di servizi gestiti»: un soggetto che fornisce servizi relativi all'installazione, alla gestione, al funzionamento o alla manutenzione di prodotti, reti, infrastrutture, applicazioni TIC o di qualsiasi altro sistema informatico e di rete, tramite assistenza o amministrazione attiva effettuata nei locali dei clienti o a distanza;

40) «fornitore di servizi di sicurezza gestiti»: un fornitore di servizi di sicurezza gestiti che svolge o fornisce assistenza per attività relative alla gestione dei rischi di cibersicurezza;

41) «organismo di ricerca»: un soggetto che ha come obiettivo principale lo svolgimento di attività di ricerca applicata o di sviluppo sperimentale al fine di sfruttare i risultati di tale ricerca a fini commerciali, ma che non comprende gli istituti di istruzione.

CAPO II

QUADRI COORDINATI IN MATERIA DI CIBERSICUREZZA

Articolo 7

Strategia nazionale per la cibersicurezza

1. Ogni Stato membro adotta una strategia nazionale per la cibersicurezza che prevede gli obiettivi strategici e le risorse necessarie per conseguirli, nonché adeguate misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cibersicurezza. La strategia nazionale per la cibersicurezza comprende:

a) gli obiettivi e le priorità della strategia per la cibersicurezza dello Stato membro, che riguardano in particolare i settori di cui agli allegati I e II;

b) un quadro di governance per la realizzazione degli obiettivi e delle priorità di cui alla lettera a) del presente paragrafo, comprendente le misure strategiche di cui al paragrafo 2;

c) un quadro di governance che chiarisca i ruoli e le responsabilità dei pertinenti portatori di interessi a livello nazionale, a sostegno della cooperazione e del coordinamento a livello nazionale tra le autorità competenti, i punti di contatto unici e i CSIRT ai sensi della presente direttiva, nonché il coordinamento e la cooperazione tra tali organismi e le autorità competenti ai sensi degli atti giuridici settoriali dell'Unione;

d) un meccanismo per individuare le risorse e una valutazione dei rischi nello Stato membro in questione;

e) l'individuazione delle misure volte a garantire la preparazione e la risposta agli incidenti e il successivo recupero dagli stessi, inclusa la collaborazione tra i settori pubblico e privato;

f) un elenco delle diverse autorità e dei diversi portatori di interessi coinvolti nell'attuazione della strategia nazionale per la cibersicurezza;

g) un quadro strategico per il rafforzamento del coordinamento tra le autorità competenti a norma della presente direttiva e le autorità competenti a norma della direttiva (UE) 2022/2557 ai fini della condivisione delle informazioni sui rischi, le minacce e gli incidenti sia informatici che non informatici e dello svolgimento di compiti di vigilanza, se del caso;

h) un piano, comprendente le misure necessarie, per aumentare livello generale di consapevolezza dei cittadini in materia di cibersicurezza.

2. Nell'ambito della strategia nazionale per la cibersicurezza, gli Stati membri adottano in particolare misure strategiche riguardanti:

a) la cibersicurezza nella catena di approvvigionamento dei prodotti e dei servizi TIC utilizzati da soggetti per la fornitura dei loro servizi;

b) l'inclusione e la definizione di requisiti concernenti la cibersicurezza per i prodotti e i servizi TIC negli appalti pubblici, compresi i requisiti relativi alla certificazione della cibersicurezza, alla cifratura e l'utilizzo di prodotti di cibersicurezza open source;

c) la gestione delle vulnerabilità, ivi comprese la promozione e l'agevolazione della divulgazione coordinata delle vulnerabilità ai sensi dell'articolo 12, paragrafo 1;

d) il sostegno della disponibilità generale, dell'integrità e della riservatezza del carattere fondamentale pubblico di una rete internet aperta, compresa, se del caso, la cibersicurezza dei cavi di comunicazione sottomarini;

e) la promozione dello sviluppo e dell'integrazione di tecnologie avanzate pertinenti miranti ad attuare misure di avanguardia nella gestione dei rischi di cibersicurezza;

f) la promozione e lo sviluppo di attività di istruzione, formazione e sensibilizzazione, di competenze e di iniziative di ricerca e sviluppo in materia di cibersicurezza, nonché orientamenti sulle buone pratiche e sui controlli concernenti l'igiene informatica, destinati ai cittadini, ai portatori di interessi e ai soggetti;

g) il sostegno agli istituti accademici e di ricerca volto a sviluppare, rafforzare e promuovere la diffusione di strumenti di cibersicurezza e di infrastrutture di rete sicure;

h) la messa a punto di procedure pertinenti e strumenti adeguati di condivisione delle informazioni per sostenere la condivisione volontaria di informazioni sulla cibersicurezza tra soggetti, nel rispetto del diritto dell'Unione;

i) il rafforzamento dei valori di riferimento relativi alla ciberresilienza e all'igiene informatica delle PMI, in particolare quelle escluse dall'ambito di applicazione della presente direttiva, fornendo orientamenti e sostegno facilmente accessibili per le loro esigenze specifiche;

j) la promozione di una protezione informatica attiva.

3. Gli Stati membri notificano le loro strategie nazionali per la cibersicurezza alla Commissione entro tre mesi dall'adozione. Gli Stati membri possono omettere dalla notifica informazioni relative alla propria sicurezza nazionale.

4. Gli Stati membri valutano le proprie strategie nazionali per la cibersicurezza periodicamente e almeno ogni cinque anni sulla base di indicatori chiave di prestazione e, se necessario, le aggiornano. L'ENISA assiste gli Stati membri, su richiesta di questi ultimi, nell'elaborazione o aggiornamento di una strategia nazionale per la cibersicurezza e di indicatori chiave di prestazione per la relativa valutazione, onde allinearla ai requisiti e agli obblighi di cui alla presente direttiva.

Articolo 8

Autorità competenti e punti di contatto unici

1. Ogni Stato membro designa o istituisce una o più autorità competenti responsabili della cibersicurezza e dei compiti di vigilanza di cui al capo VII (autorità competenti).

2. Le autorità competenti di cui al paragrafo 1 controllano l'attuazione della presente direttiva a livello nazionale.

3. Ogni Stato membro designa o istituisce un punto di contatto unico. Se uno Stato membro designa o istituisce soltanto un'autorità competente a norma del paragrafo 1, quest'ultima è anche il punto di contatto unico per tale Stato membro.

4. Ogni punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità del relativo Stato membro con le autorità pertinenti degli altri Stati membri, e, ove opportuno, con la Commissione e l'ENISA, nonché per garantire la cooperazione intersettoriale con altre autorità competenti dello stesso Stato membro.

5. Gli Stati membri garantiscono che le proprie autorità competenti e i propri punti di contatto unici siano dotati di risorse adeguate per svolgere in modo efficiente ed efficace i compiti loro assegnati e conseguire in questo modo gli obiettivi della presente direttiva.

6. Ogni Stato membro notifica alla Commissione, senza indebiti ritardi, l'identità dell'autorità competente di cui al paragrafo 1 e del punto di contatto unico di cui al paragrafo 3, i compiti di tali autorità e qualsiasi ulteriore modifica dei medesimi. Ciascuno Stato membro rende pubblica l'identità della propria autorità competente. La Commissione elabora un elenco dei punti di contatto unici disponibili.

Articolo 9

Quadri nazionali di gestione delle crisi informatiche

1. Ogni Stato membro designa o istituisce una o più autorità competenti responsabili della gestione degli incidenti e delle crisi di cibersicurezza su vasta scala (autorità di gestione delle crisi informatiche). Gli Stati membri provvedono affinché tali autorità dispongano di risorse adeguate per svolgere i compiti loro assegnati in modo efficace ed efficiente. Gli Stati membri assicurano la coerenza con i quadri nazionali esistenti di gestione generale delle crisi.

2. Se uno Stato membro designa o istituisce più di un'autorità di gestione delle crisi informatiche ai sensi del paragrafo 1, esso indica chiaramente quale di tali autorità deve fungere da coordinatore per la gestione di incidenti e crisi di cibersicurezza su vasta scala.

3. Ogni Stato membro individua le capacità, le risorse e le procedure che possono essere impiegate in caso di crisi ai fini della presente direttiva.

4. Ogni Stato membro adotta un piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala in cui sono stabiliti gli obiettivi e le modalità della gestione degli incidenti e delle crisi di cibersicurezza su vasta scala. In tale piano sono definiti, in particolare:

a) gli obiettivi delle misure e delle attività nazionali di preparazione;

b) i compiti e le responsabilità delle autorità di gestione delle crisi informatiche;

c) le procedure di gestione delle crisi informatiche, tra cui la loro integrazione nel quadro nazionale generale di gestione delle crisi e i canali di scambio di informazioni;

d) le misure nazionali di preparazione, comprese le esercitazioni e le attività di formazione;

e) i pertinenti portatori di interessi del settore pubblico e privato e le infrastrutture coinvolte;

f) le procedure nazionali e gli accordi tra gli organismi e le autorità nazionali pertinenti al fine di garantire il sostegno e la partecipazione effettivi dello Stato membro alla gestione coordinata degli incidenti e delle crisi di cibersicurezza su vasta scala a livello dell'Unione.

5. Entro tre mesi dalla designazione o istituzione dell'autorità di gestione delle crisi informatiche di cui al paragrafo 1, ciascuno Stato membro notifica alla Commissione l'identità della propria autorità e qualsiasi ulteriore modifica alla stessa. Gli Stati membri presentano alla Commissione e alla rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) le informazioni pertinenti relative ai requisiti di cui al paragrafo 4 in merito ai propri piani nazionali di risposta agli incidenti e delle crisi di cibersicurezza su vasta scala entro tre mesi dall'adozione di tali piani. Gli Stati membri possono omettere informazioni se e nella misura in cui ciò sia necessario ai fini della loro sicurezza nazionale.

Articolo 10

Team di risposta agli incidenti di sicurezza informatica (CSIRT)

1. Ogni Stato membro designa o istituisce uno o più CSIRT. È possibile designare o istituire i CSIRT all'interno di un'autorità competente. I CSIRT sono conformi ai requisiti di cui all'articolo 11, paragrafo 1, si occupano almeno dei settori, dei sottosettori e dei tipi di soggetto di cui agli allegati I e II e sono responsabili della gestione degli incidenti conformemente a una procedura ben definita.

2. Gli Stati membri provvedono affinché ogni CSIRT disponga di risorse adeguate per svolgere efficacemente i suoi compiti di cui all'articolo 11, paragrafo 3.

3. Gli Stati membri provvedono affinché ogni CSIRT disponga di un'infrastruttura di informazione e comunicazione adeguata, sicura e resiliente attraverso la quale scambiare informazioni con i soggetti essenziali e importanti e con gli altri portatori di interesse pertinenti. A tal fine gli Stati membri provvedono affinché ogni CSIRT contribuisca allo sviluppo di strumenti sicuri per la condivisione delle informazioni.

4. I CSIRT cooperano e, se opportuno, scambiano informazioni pertinenti conformemente all'articolo 29 con comunità settoriali o intersettoriali di soggetti essenziali e importanti.

5. I CSIRT partecipano alle revisioni tra pari organizzate conformemente all'articolo 19.

6. Gli Stati membri garantiscono la collaborazione effettiva, efficiente e sicura dei loro CSIRT nella rete di CSIRT.

7. I CSIRT possono stabilire relazioni di cooperazione con team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi. Nell'ambito di tali relazioni di cooperazione, gli Stati membri facilitano uno scambio di informazioni efficace, efficiente e sicuro con tali team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi, utilizzando i pertinenti protocolli di condivisione delle informazioni, compreso il protocollo TLP (*Traffic Light Protocol*). I CSIRT possono scambiare informazioni pertinenti con team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi, compresi dati personali a norma del diritto dell'Unione in materia di protezione dei dati.

8. I CSIRT possono cooperare con team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi o con organismi equivalenti di paesi terzi, in particolare al fine di fornire loro assistenza in materia di cibersicurezza.

9. Ogni Stato membro notifica alla Commissione senza indebiti ritardi l'identità del CSIRT di cui al paragrafo 1 del presente articolo e del CSIRT designato come coordinatore conformemente all'articolo 12, paragrafo 1, i rispettivi compiti in relazione ai soggetti essenziali e importanti e qualsiasi ulteriore modifica dei medesimi.

10. Gli Stati membri possono chiedere l'assistenza dell'ENISA nello sviluppo dei CSIRT.

Articolo 11

Requisiti, capacità tecniche e compiti dei CSIRT

1. I CSIRT soddisfano i requisiti seguenti:

a) i CSIRT garantiscono un alto livello di disponibilità dei propri canali di comunicazione evitando singoli punti di vulnerabilità (*single points of failure*) e dispongono di vari mezzi che permettono loro di essere contattati e di contattare altri in qualsiasi momento; essi indicano chiaramente i canali di comunicazione e li rendono noti alla loro base di utenti e ai partner con cui collaborano;

b) i locali e i sistemi informatici di supporto dei CSIRT sono ubicati in siti sicuri;

c) i CSIRT sono dotati di un sistema adeguato di gestione e inoltro delle richieste, in particolare per facilitare i trasferimenti in maniera efficace ed efficiente;

d) i CSIRT garantiscono la riservatezza e l'affidabilità delle loro operazioni;

e) i CSIRT dispongono di personale sufficiente per garantire la disponibilità dei loro servizi in qualsiasi momento e garantiscono che il loro personale sia formato in modo appropriato;

f) i CSIRT sono dotati di sistemi ridondanti e spazi di lavoro di backup al fine di garantire la continuità dei loro servizi.

I CSIRT hanno la possibilità di partecipare a reti di cooperazione internazionale.

2. Gli Stati membri assicurano che i loro CSIRT dispongano congiuntamente delle capacità tecniche necessarie a svolgere i compiti di cui al paragrafo 3. Gli Stati membri provvedono affinché ai propri CSIRT siano assegnate risorse sufficienti per garantire un organico adeguato al fine di consentire ai CSIRT di sviluppare le proprie capacità tecniche.

3. I CSIRT svolgono i compiti seguenti:

a) monitorano e analizzano le minacce informatiche, le vulnerabilità e gli incidenti a livello nazionale, e, su richiesta, forniscono assistenza ai soggetti essenziali e importanti interessati per quanto riguarda il monitoraggio in tempo reale o prossimo al reale dei loro sistemi informatici e di rete;

b) emettono preallarmi, allerte e bollettini e divulgano informazioni ai soggetti essenziali e importanti interessati, nonché alle autorità competenti e agli altri pertinenti portatori di interessi, in merito a minacce informatiche, vulnerabilità e incidenti, se possibile in tempo prossimo al reale;

c) forniscono una risposta agli incidenti e forniscono assistenza ai soggetti essenziali e importanti interessati, se del caso;

d) raccolgono e analizzano dati forensi e forniscono un'analisi dinamica dei rischi e degli incidenti, nonché una consapevolezza situazionale riguardo alla cibersicurezza;

e) effettuano, su richiesta di un soggetto essenziale o importante, una scansione proattiva dei sistemi informatici e di rete del soggetto interessato per rilevare le vulnerabilità con potenziale impatto significativo;

f) partecipano alla rete di CSIRT e forniscono assistenza reciproca secondo le loro capacità e competenze agli altri membri della rete di CSIRT su loro richiesta.

g) se del caso, agiscono in qualità di coordinatore ai fini del processo di divulgazione coordinata delle vulnerabilità di cui all'articolo 12, paragrafo 1;

h) contribuiscono allo sviluppo di strumenti sicuri per la condivisione delle informazioni di cui all'articolo 10, paragrafo 3.

I CSIRT possono effettuare una scansione proattiva e non intrusiva dei sistemi informatici e di rete accessibili al pubblico di soggetti essenziali e importanti. Tale scansione è effettuata per individuare sistemi informatici e di rete vulnerabili o configurati in modo non sicuro e per informare i soggetti interessati. Tale scansione non ha alcun impatto negativo sul funzionamento dei servizi dei soggetti.

Nello svolgimento dei compiti di cui al primo comma, i CSIRT possono dare priorità a determinati compiti sulla base di un approccio basato sul rischio.

4. I CSIRT instaurano rapporti di cooperazione con i pertinenti portatori di interesse del settore privato al fine di perseguire gli obiettivi della presente direttiva.

5. Al fine di agevolare la cooperazione di cui al paragrafo 4, i CSIRT promuovono l'adozione e l'uso di pratiche, sistemi di classificazione e tassonomie standardizzati o comuni per quanto riguarda:

a) le procedure di gestione degli incidenti;

b) la gestione delle crisi; e

c) la divulgazione coordinata delle vulnerabilità ai sensi dell'articolo 12, paragrafo 1.

Articolo 12

Divulgazione coordinata delle vulnerabilità e banca dati europea delle vulnerabilità

1. Ogni Stato membro designa uno dei propri CSIRT come coordinatore ai fini della divulgazione coordinata delle vulnerabilità. Il CSIRT designato agisce da intermediario di fiducia agevolando, se necessario, l'interazione tra la persona fisica o giuridica che segnala la vulnerabilità e il fabbricante o fornitore di servizi TIC o prodotti TIC potenzialmente vulnerabili, su richiesta di una delle parti. I compiti del CSIRT designato come coordinatore comprendono:

a) l'individuazione e il contatto dei soggetti interessati;

b) l'assistenza alle persone fisiche o giuridiche che segnalano una vulnerabilità, e

c) la negoziazione dei tempi di divulgazione e la gestione delle vulnerabilità che interessano più soggetti.

Gli Stati membri provvedono affinché le persone fisiche o giuridiche possano segnalare in forma anonima, qualora lo richiedano, una vulnerabilità al CSIRT designato come coordinatore. Il CSIRT designato come coordinatore garantisce lo svolgimento di diligenti azioni per dare seguito alla segnalazione di vulnerabilità e assicura l'anonimato della persona fisica o giuridica segnalante. Se la vulnerabilità segnalata è suscettibile di avere un impatto significativo su soggetti in più di uno Stato membro, il CSIRT designato di ciascuno Stato membro interessato coopera, se del caso, con altri CSIRT designati in qualità di coordinatori nell'ambito della rete di CSIRT.

2. L'ENISA elabora e mantiene, previa consultazione del gruppo di cooperazione, una banca dati europea delle vulnerabilità. A tal fine l'ENISA istituisce e gestisce i sistemi informatici, le misure strategiche e le procedure adeguati e adotta le necessarie misure tecniche e organizzative per garantire la sicurezza e l'integrità della banca dati europea delle vulnerabilità, in particolare al fine di consentire ai soggetti, indipendentemente dal fatto che ricadano o meno nell'ambito di applicazione della presente direttiva, e ai relativi fornitori di sistemi informatici e di rete, di divulgare e registrare, su base volontaria, le vulnerabilità pubblicamente note presenti nei prodotti TIC o nei servizi TIC. Tutti i portatori di interessi hanno accesso alle informazioni sulle vulnerabilità contenute nella banca dati europea delle vulnerabilità. La banca dati contiene:

a) informazioni che illustrano la vulnerabilità;

b) i prodotti TIC o i servizi TIC interessati e la gravità della vulnerabilità in termini di circostanze nelle quali potrebbe essere sfruttata;

c) la disponibilità di relative patch e, qualora queste non fossero disponibili, gli orientamenti forniti dalle autorità nazionali competenti o dai CSIRT rivolti agli utenti dei prodotti TIC e dei servizi TIC vulnerabili sulle possibili modalità di attenuazione dei rischi derivanti dalle vulnerabilità divulgate.

Articolo 13

Cooperazione a livello nazionale

1. Se sono separati, le autorità competenti, il punto di contatto unico e i CSIRT dello stesso Stato membro collaborano per quanto concerne l'adempimento degli obblighi di cui alla presente direttiva.

2. Gli Stati membri provvedono affinché i loro CSIRT o, se del caso, le loro autorità competenti, ricevano le notifiche degli incidenti significativi a norma dell'articolo 23, nonché degli incidenti, delle minacce informatiche e dei quasi incidenti (*near miss*) a norma dell'articolo 30.

3. Gli Stati membri provvedono affinché i loro CSIRT o, se del caso, le loro autorità competenti informino i loro punti di contatto unico delle notifiche relative agli incidenti, alle minacce informatiche e ai quasi incidenti trasmesse a norma della presente direttiva.

4. Al fine di garantire l'efficace adempimento dei compiti e degli obblighi delle autorità competenti, dei punti di contatto unici e dei CSIRT, gli Stati membri, nella misura del possibile, provvedono affinché, all'interno di ciascuno Stato membro, vi sia un'adeguata cooperazione tra i suddetti organismi e le autorità di contrasto, le autorità di protezione dei dati, le autorità nazionali ai sensi dei regolamenti (CE) n. 300/2008 e (UE) 2018/1139, gli organismi di vigilanza a norma del regolamento (UE) n. 910/2014, le autorità competenti a norma del regolamento (UE) 2022/2554, le autorità nazionali di regolamentazione a norma della direttiva (UE) 2018/1972, le autorità competenti a norma della direttiva (UE) 2022/2557, nonché le autorità competenti ai sensi di altri atti giuridici settoriali dell'Unione.

5. Gli Stati membri provvedono affinché le loro autorità competenti a norma della presente direttiva e le loro autorità competenti a norma della direttiva (UE) 2022/2557 collaborino e si scambino periodicamente informazioni riguardo all'identificazione di soggetti critici, sui rischi, sulle minacce e sugli incidenti sia informatici che non informatici che interessano i soggetti essenziali identificati come critici a norma della direttiva (UE) 2022/2557, e sulle misure adottate in risposta a tali rischi, minacce e incidenti. Gli Stati membri provvedono inoltre affinché le loro autorità competenti a norma della presente direttiva e le loro autorità competenti a norma del regolamento (UE) n. 910/2014, del regolamento (UE) 2022/2554 e della direttiva (UE) 2018/1972 si scambino periodicamente informazioni pertinenti, anche per quanto riguarda gli incidenti e le minacce informatiche rilevanti.

6. Gli Stati membri semplificano la comunicazione mediante i mezzi tecnici per le notifiche di cui agli articoli 23 e 30.

CAPO III

COOPERAZIONE A LIVELLO DELL'UNIONE E INTERNAZIONALE

Articolo 14

Gruppo di cooperazione

1. Al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri, nonché di rafforzare la fiducia, è istituito un gruppo di cooperazione.

2. Il gruppo di cooperazione svolge i suoi compiti sulla base di programmi di lavoro biennali di cui al paragrafo 7.

3. Il gruppo di cooperazione è composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA. Il Servizio europeo per l'azione esterna partecipa alle attività del gruppo di cooperazione in qualità di osservatore. Le autorità europee di vigilanza (AEV) e le autorità competenti a norma del regolamento (UE) 2022/2554 possono partecipare alle attività del gruppo di cooperazione conformemente all'articolo 47, paragrafo 1, di tale regolamento.

Ove opportuno, il gruppo di cooperazione può invitare a partecipare ai suoi lavori il Parlamento europeo e i rappresentanti dei pertinenti portatori di interessi.

La Commissione ne assicura il segretariato.

4. Il gruppo di cooperazione svolge i compiti seguenti:

a) fornire orientamenti alle autorità competenti in merito al recepimento e all'attuazione della presente direttiva;

b) fornire orientamenti alle autorità competenti in merito allo sviluppo e all'attuazione di politiche in materia di divulgazione coordinata delle vulnerabilità di cui all'articolo 7, paragrafo 2, lettera c);

c) scambiare migliori prassi e informazioni relative all'attuazione della presente direttiva, anche per quanto riguarda minacce informatiche, incidenti, vulnerabilità, quasi incidenti, iniziative di sensibilizzazione, attività di formazione, esercitazioni e competenze, sviluppo di capacità, norme e specifiche tecniche, nonché l'identificazione dei soggetti essenziali e importanti ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e);

d) effettuare scambi di consulenza e cooperare con la Commissione per quanto riguarda le nuove iniziative strategiche in materia di cibersicurezza e la coerenza globale dei requisiti settoriali di cibersicurezza;

e) effettuare scambi di consulenza e cooperare con la Commissione per quanto riguarda i progetti di atti delegati o di esecuzione adottati a norma della presente direttiva;

f) scambiare migliori prassi e informazioni con le istituzioni, gli organismi, gli uffici e le agenzie pertinenti dell'Unione;

g) effettuare scambi di opinioni per quanto riguarda l'attuazione degli atti giuridici settoriali dell'Unione che contengono disposizioni in materia di cibersicurezza;

h) se del caso, discutere le relazioni sulle revisioni tra pari di cui all'articolo 19, paragrafo 9 ed elaborare conclusioni e raccomandazioni;

i) effettuare valutazioni coordinate dei rischi per la sicurezza di catene di approvvigionamento critiche conformemente all'articolo 22, paragrafo 1;

j) discutere i casi di assistenza reciproca, fra cui le esperienze e i risultati delle azioni di vigilanza comuni transfrontaliere di cui all'articolo 37;

k) su richiesta di uno o più Stati membri interessati, discutere le richieste specifiche di assistenza reciproca di cui all'articolo 37;

l) fornire orientamenti strategici alla rete di CSIRT ed EU–CyCLONe su specifiche questioni emergenti;

m) effettuare scambi di opinioni sulla politica in materia di azioni di follow-up a seguito incidenti e crisi di cibersicurezza su vasta scala sulla base degli insegnamenti tratti dalla rete di CSIRT e da EU-CyCLONe;

n) contribuire alle capacità di cibersicurezza in tutta l'Unione agevolando lo scambio di funzionari nazionali attraverso un programma di sviluppo delle capacità che coinvolga il personale delle autorità competenti o dei CSIRT;

o) organizzare riunioni congiunte periodiche con i pertinenti portatori di interessi del settore privato di tutta l'Unione per discutere le attività svolte dal gruppo di cooperazione e raccogliere contributi sulle sfide strategiche emergenti;

p) discutere le attività intraprese per quanto riguarda le esercitazioni di cibersicurezza, compreso il lavoro svolto dall'ENISA;

q) stabilire la metodologia e gli aspetti organizzativi delle revisioni tra pari di cui all'articolo 19, paragrafo 1, nonché stabilire, con l'assistenza della Commissione e dell'ENISA, la metodologia di autovalutazione per gli Stati membri a norma dell'articolo 19, paragrafo 4, ed elaborare, in collaborazione con la Commissione e l'ENISA, i codici di condotta su cui si basano i metodi di lavoro degli esperti di cibersicurezza designati a norma dell'articolo 19, paragrafo 6;

r) elaborare relazioni, ai fini del riesame di cui all'articolo 40, sull'esperienza acquisita a livello strategico e dalle revisioni tra pari;

s) discutere e svolgere periodicamente una valutazione dello stato di avanzamento delle minacce o degli incidenti informatici, come il ransomware.

Il gruppo di cooperazione presenta le relazioni di cui al primo comma, lettera r), alla Commissione, al Parlamento europeo e al Consiglio.

5. Gli Stati membri garantiscono la collaborazione effettiva, efficiente e sicura dei loro rappresentanti in seno al gruppo di cooperazione.

6. Il gruppo di cooperazione può richiedere alla rete di CSIRT una relazione tecnica su argomenti selezionati.

7. Entro il 1º febbraio 2024 e successivamente ogni due anni, il gruppo di cooperazione stabilisce un programma di lavoro sulle azioni da intraprendere per realizzare i propri obiettivi e compiti.

8. La Commissione può adottare atti di esecuzione che stabiliscono le modalità procedurali necessarie per il funzionamento del gruppo di cooperazione.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

La Commissione scambia pareri e coopera con il gruppo di cooperazione in merito ai progetti di atto di esecuzione di cui al primo comma del presente paragrafo, conformemente al paragrafo 4, lettera e).

9. Il gruppo di cooperazione si riunisce periodicamente, e in ogni caso una volta all'anno, con il gruppo per la resilienza dei soggetti critici istituito a norma della direttiva (UE) 2022/2557 al fine di promuovere e agevolare la cooperazione strategica e lo scambio di informazioni.

Articolo 15

Rete di CSIRT

1. Al fine di contribuire allo sviluppo della fiducia e di promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri, è istituita una rete dei CSIRT nazionali.

2. La rete di CSIRT è composta da rappresentanti dei CSIRT designati o istituiti a norma dell'articolo 10 e della squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'Unione (CERT-UE). La Commissione partecipa alla rete di CSIRT in qualità di osservatore. L'ENISA ne assicura il segretariato e fornisce attivamente assistenza alla cooperazione fra i CSIRT.

3. La rete di CSIRT svolge i compiti seguenti:

a) scambiare informazioni per quanto riguarda le capacità dei CSIRT;

b) agevolare la condivisione, il trasferimento e lo scambio di tecnologia e delle misure, delle politiche, degli strumenti, dei processi, delle migliori pratiche e dei quadri pertinenti fra i CSIRT;

c) scambiare informazioni pertinenti per quanto riguarda gli incidenti, i quasi incidenti, le minacce informatiche, i rischi e le vulnerabilità;

d) scambiare informazioni in merito alle pubblicazioni e alle raccomandazioni in materia di cibersicurezza;

e) garantire l'interoperabilità per quanto riguarda le specifiche e i protocolli per lo scambio di informazioni;

f) su richiesta di un membro della rete di CSIRT potenzialmente interessato da un incidente, scambiare e discutere informazioni relative a tale incidente e alle minacce informatiche, ai rischi e alle vulnerabilità associati;

g) su richiesta di un membro della rete di CSIRT, discutere e, ove possibile, attuare una risposta coordinata a un incidente identificato nella giurisdizione di tale Stato membro;

h) fornire assistenza agli Stati membri nel far fronte a incidenti transfrontalieri a norma della presente direttiva;

i) cooperare e scambiare migliori pratiche con i CSIRT designati in qualità di coordinatori di cui all'articolo 12, paragrafo 1, nonché fornire loro assistenza per quanto riguarda la gestione della divulgazione coordinata di vulnerabilità che potrebbero avere un impatto significativo su soggetti in più di uno Stato membro;

j) discutere e individuare ulteriori forme di cooperazione operativa, anche in relazione a:

   i) categorie di minacce informatiche e incidenti;

   ii) preallarmi;

   iii) assistenza reciproca;

   iv) principi e modalità di coordinamento in risposta a rischi e incidenti transfrontalieri;

   v) contributi al piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala di cui all'articolo 9, paragrafo 4, su richiesta di uno Stato membro;

k) informare il gruppo di cooperazione sulle proprie attività e sulle ulteriori forme di cooperazione operativa discusse a norma della lettera j) e, se necessario, chiedere orientamenti in merito;

l) fare il punto sui risultati delle esercitazioni di cibersicurezza, comprese quelle organizzate dall'ENISA;

m) su richiesta di un singolo CSIRT, discutere le capacità e lo stato di preparazione di tale CSIRT;

n) cooperare e scambiare informazioni con i centri operativi di sicurezza regionali e a livello dell'UE al fine di migliorare la consapevolezza situazionale comune sugli incidenti e le minacce informatiche in tutta l'Unione;

o) se del caso, discutere le relazioni sulle revisioni tra pari di cui all'articolo 19, paragrafo 9;

p) fornire orientamenti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni del presente articolo in materia di cooperazione operativa.

4. Entro il 17 gennaio 2025, e successivamente ogni due anni, ai fini del riesame di cui all'articolo 40, la rete di CSIRT valuta i progressi compiuti nella cooperazione operativa ed elabora una relazione. Nella relazione, in particolare, vengono elaborate conclusioni e raccomandazioni sulla base del risultato delle revisioni tra pari di cui all'articolo 19, che sono effettuate in relazione ai CSIRT nazionali. Tale relazione è trasmessa al gruppo di cooperazione.

5. La rete di CSIRT adotta il proprio regolamento interno.

6. La rete di CSIRT ed EU-CyCLONe concordano le modalità procedurali e cooperano su tale base.

Articolo 16

Rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe)

1. EU-CyCLONe è istituita al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala e di garantire il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione.

2. EU-CyCLONe è composta da rappresentanti delle autorità di gestione delle crisi informatiche degli Stati membri e, nei casi in cui un incidente di cibersicurezza su vasta scala potenziale o in corso abbia o abbia probabilità di avere un impatto significativo sui servizi e sulle attività che rientrano nell'ambito di applicazione della presente direttiva, della Commissione. Negli altri casi, la Commissione partecipa alle attività di EU-CyCLONe in qualità di osservatore.

L'ENISA assicura il segretariato di EU-CyCLONe e sostiene lo scambio sicuro di informazioni, oltre a fornire gli strumenti necessari per sostenere la cooperazione tra gli Stati membri garantendo uno scambio sicuro di informazioni.

Ove opportuno, EU-CyCLONe può invitare i rappresentanti dei pertinenti portatori di interessi a partecipare ai suoi lavori in qualità di osservatori.

3. EU-CyCLONe svolge i compiti seguenti:

a) aumentare il livello di preparazione per la gestione di crisi e incidenti su vasta scala;

b) sviluppare una conoscenza situazionale condivisa in merito agli incidenti e alle crisi di cibersicurezza su vasta scala;

c) valutare le conseguenze e l'impatto dei pertinenti incidenti e delle pertinenti crisi di cibersicurezza su vasta scala e proporre possibili misure di attenuazione;

d) coordinare la gestione degli incidenti e delle crisi di cibersicurezza su vasta scala e sostenere il processo decisionale a livello politico in merito a tali incidenti e crisi;

e) discutere, su richiesta di uno Stato membro interessato, i piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala di cui all'articolo 9, paragrafo 4.

4. EU-CyCLONe adotta il proprio regolamento interno.

5. EU-CyCLONe riferisce periodicamente al gruppo di cooperazione in merito alla gestione degli incidenti e delle crisi di cibersicurezza su vasta scala, nonché in merito alle tendenze, concentrandosi in particolare sul relativo impatto sui soggetti essenziali e importanti.

6. EU-CyCLONe coopera con la rete di CSIRT sulla base di modalità procedurali concordate previste all'articolo 15, paragrafo 6.

7. Entro il 17 luglio 2024 e successivamente ogni 18 mesi, EU-CyCLONe presenta al Parlamento europeo e al Consiglio una relazione di valutazione del proprio lavoro.

Articolo 17

Cooperazione internazionale

Ove opportuno, l'Unione può concludere accordi internazionali, conformemente all'articolo 218 TFUE, con paesi terzi o organizzazioni internazionali, che consentano e organizzino la loro partecipazione ad attività particolari del gruppo di cooperazione, della rete di CSIRT e di EU-CyCLONe. Tali accordi sono conformi al diritto dell'Unione in materia di protezione dei dati.

Articolo 18

Relazione sullo stato della cibersicurezza nell'Unione

1. L'ENISA, in collaborazione con la Commissione e con il gruppo di cooperazione, pubblica una relazione biennale sullo stato della cibersicurezza nell'Unione e la presenta al Parlamento europeo. La relazione è resa disponibile, fra l'altro, in un formato leggibile meccanicamente e comprende gli aspetti seguenti:

a) una valutazione del rischio di cibersicurezza a livello dell'Unione, che tenga conto del panorama delle minacce informatiche;

b) una valutazione dello sviluppo delle capacità di cibersicurezza nei settori pubblico e privato nell'Unione;

c) una valutazione del livello generale di consapevolezza in materia di cibersicurezza e di igiene informatica tra i cittadini e i soggetti, comprese le piccole e medie imprese;

d) una valutazione aggregata del risultato delle revisioni tra pari di cui all'articolo 19;

e) una valutazione aggregata del livello di maturità delle capacità e delle risorse di cibersicurezza nell'Unione, comprese quelle a livello settoriale, nonché del livello di allineamento delle strategie nazionali di cibersicurezza degli Stati membri.

2. La relazione contiene raccomandazioni strategiche specifiche, finalizzate a porre rimedio alle carenze e ad aumentare il livello di cibersicurezza nell'Unione, e una sintesi delle conclusioni tratte per quel determinato periodo nelle relazioni sulla situazione tecnica della cibersicurezza nell'Unione per quanto riguarda gli incidenti e le minacce informatiche, elaborate dall'ENISA conformemente all'articolo 7, paragrafo 6, del regolamento (UE) 2019/881.

3. L'ENISA, in collaborazione con la Commissione, il gruppo di cooperazione e la rete di CSIRT, elabora la metodologia, ivi comprese le variabili pertinenti — come ad esempio indicatori quantitativi e qualitativi — della valutazione aggregata di cui al paragrafo 1, lettera e).

Articolo 19

Revisioni tra pari

1. Con l'assistenza della Commissione e dell'ENISA nonché, se del caso, della rete CSIRT ed entro il 17 gennaio 2025, il gruppo di cooperazione stabilisce la metodologia e gli aspetti organizzativi delle revisioni tra pari con l'obiettivo di trarre insegnamenti dalle esperienze condivise, rafforzare la fiducia reciproca, conseguire un livello comune elevato di cibersicurezza e migliorare le capacità e le politiche di cibersicurezza degli Stati membri necessarie per attuare la presente direttiva. La partecipazione alle revisioni tra pari è volontaria. Le revisioni tra pari sono condotte da esperti di cibersicurezza. Gli esperti di cibersicurezza sono designati da almeno due Stati membri, diversi dallo Stato membro oggetto di revisione.

Le revisioni tra pari riguardano almeno uno degli aspetti seguenti:

a) il livello di attuazione delle misure di gestione e delle prescrizioni in materia di segnalazione dei rischi di cibersicurezza enunciate agli articoli 21 e 23;

b) il livello delle capacità, comprese le risorse finanziarie, tecniche e umane disponibili, e l'efficacia dello svolgimento dei compiti delle autorità competenti;

c) le capacità operative dei CSIRT;

d) il livello di attuazione dell'assistenza reciproca di cui all'articolo 37;

e) il livello di attuazione degli accordi per la condivisione delle informazioni in materia di cibersicurezza di cui all'articolo 29;

f) le questioni specifiche di natura transfrontaliera o intersettoriale.

2. La metodologia di cui al paragrafo 1 comprende criteri obiettivi, non discriminatori, equi e trasparenti sulla base dei quali gli Stati membri designano esperti di cibersicurezza idonei a eseguire le revisioni tra pari. La Commissione e l'ENISA partecipano alle revisioni tra pari in qualità di osservatori.

3. Gli Stati membri possono individuare questioni specifiche di cui al paragrafo 1, lettera f), ai fini di una revisione tra pari.

4. Prima dell'inizio di una revisione tra pari di cui al paragrafo 1, gli Stati membri notificano agli Stati membri partecipanti il suo ambito di applicazione, comprese le questioni specifiche individuate ai sensi del paragrafo 3.

5. Prima dell'inizio della revisione tra pari, gli Stati membri possono effettuare un'autovalutazione degli aspetti oggetto della revisione e fornire tale autovalutazione agli esperti di cibersicurezza designati. Il gruppo di cooperazione, con l'assistenza della Commissione e dell'ENISA, stabilisce la metodologia per l'autovalutazione degli Stati membri.

6. Le revisioni tra pari comportano visite in loco fisiche o virtuali e scambi di informazioni a distanza. In linea con il principio di buona collaborazione, lo Stato membro sottoposto alla revisione tra pari fornisce agli esperti di cibersicurezza designati le informazioni necessarie per la valutazione, fatta salva la legislazione nazionale o dell'Unione in materia di protezione di informazioni riservate o classificate e di salvaguardia delle funzioni essenziali dello Stato, quali la sicurezza nazionale. Il gruppo di cooperazione, in collaborazione con la Commissione e con l'ENISA, elabora codici di condotta adeguati, su cui si basano i metodi di lavoro degli esperti di cibersicurezza designati. Le informazioni ottenute mediante la revisione tra pari sono utilizzate unicamente a tal fine. Gli esperti di cibersicurezza che partecipano alla revisione tra pari non divulgano a terzi le eventuali informazioni sensibili o riservate ottenute nel corso di tale revisione tra pari.

7. Una volta sottoposti a revisione tra pari, i medesimi aspetti esaminati in uno Stato membro non sono più soggetti a ulteriori revisioni tra pari in tale Stato membro per i due anni successivi alla conclusione della revisione, a meno che non sia diversamente richiesto o stabilito dallo Stato membro su proposta del gruppo di cooperazione.

8. Gli Stati membri provvedono affinché gli eventuali rischi di conflitto di interessi riguardanti gli esperti di cibersicurezza designati siano rivelati agli altri Stati membri, al gruppo di cooperazione, alla Commissione e all'ENISA prima dell'inizio della revisione tra pari. Lo Stato membro che è sottoposto alla revisione tra pari può opporsi alla designazione di particolari esperti di cibersicurezza per motivi debitamente giustificati, comunicati allo Stato membro designante.

9. Gli esperti di cibersicurezza che partecipano alle revisioni tra pari elaborano relazioni sui risultati e sulle conclusioni delle revisioni tra pari. Gli Stati membri sottoposti a revisione tra pari possono formulare osservazioni sui progetti di relazione che li riguardano e tali osservazioni sono allegate alle relazioni. Le relazioni contengono raccomandazioni che consentono di migliorare gli aspetti sottoposti alla revisione tra pari. Le relazioni sono presentate al gruppo di cooperazione e alla rete di CSIRT, se del caso. Uno Stato membro sottoposto alla revisione tra pari può decidere di rendere pubblica la sua relazione o una sua versione espunta.

CAPO IV

MISURE DI GESTIONE DEL RISCHIO DI CIBERSICUREZZA E OBBLIGHI DI SEGNALAZIONE

Articolo 20

Governance

1. Gli Stati membri provvedono affinché gli organi di gestione dei soggetti essenziali e importanti approvino le misure di gestione dei rischi di cibersicurezza adottate da tali soggetti per conformarsi all'articolo 21, sovraintendano alla sua attuazione e possano essere ritenuti responsabili di violazione da parte dei soggetti di tale articolo.

L'applicazione del presente paragrafo lascia impregiudicato il diritto nazionale per quanto riguarda le norme in materia di responsabilità applicabili alle istituzioni pubbliche, nonché la responsabilità dei dipendenti pubblici e dei funzionari eletti o nominati.

2. Gli Stati membri provvedono affinché i membri dell'organo di gestione dei soggetti essenziali e importanti siano tenuti a seguire una formazione e incoraggiano i soggetti essenziali e importanti a offrire periodicamente una formazione analoga ai loro dipendenti, per far sì che questi acquisiscano conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi di cibersicurezza e il loro impatto sui servizi offerti dal soggetto.

Articolo 21

Misure di gestione dei rischi di cibersicurezza

1. Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi.

Tenuto conto delle conoscenze più aggiornate in materia e, se del caso, delle pertinenti norme europee e internazionali, nonché dei costi di attuazione, le misure di cui al primo comma assicurano un livello di sicurezza dei sistemi informatici e di rete adeguato ai rischi esistenti. Nel valutare la proporzionalità di tali misure, si tiene debitamente conto del grado di esposizione del soggetto a rischi, delle dimensioni del soggetto e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico.

2. Le misure di cui al paragrafo 1 sono basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti e comprendono almeno gli elementi seguenti:

a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;

b) gestione degli incidenti;

c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;

d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;

e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;

f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;

g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza;

h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;

i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;

j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

3. Gli Stati membri provvedono affinché, nel valutare quali misure di cui al paragrafo 2, lettera d), del presente articolo, siano adeguate, i soggetti tengano conto delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di cibersicurezza dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. Gli Stati membri provvedono inoltre affinché, nel valutare quali misure di cui al paragrafo 2, lettera d), siano adeguate, i soggetti siano tenuti a tenere conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate a norma dell'articolo 22, paragrafo 1.

4. Gli Stati membri provvedono affinché, qualora un soggetto constati di non essere conforme alle misure di cui al paragrafo 2, esso adotti, senza indebito ritardo, tutte le misure correttive necessarie, appropriate e proporzionate.

5. Entro il 17 ottobre 2024, la Commissione adotta atti di esecuzione che stabiliscono i requisiti tecnici e metodologici delle misure di cui al paragrafo 2 per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network, nonché i prestatori di servizi fiduciari.

La Commissione può adottare atti di esecuzione che stabiliscono i requisiti tecnici e metodologici, nonché, se necessario, i requisiti settoriali relativi alle misure di cui al paragrafo 2 per quanto riguarda i soggetti essenziali e importanti diversi da quelli di cui al primo comma del presente paragrafo.

Nell'elaborare gli atti di esecuzione di cui al primo e secondo comma del presente paragrafo, la Commissione segue, nella misura del possibile, le norme europee e internazionali, nonché le pertinenti specifiche tecniche. La Commissione scambia pareri e coopera con il gruppo di cooperazione e con l'ENISA in merito ai progetti di atto di esecuzione conformemente all'articolo 14, paragrafo 4, lettera e).

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

Articolo 22

Valutazioni coordinate a livello dell'Unione del rischio per la sicurezza delle catene di approvvigionamento critiche

1. Il gruppo di cooperazione, in collaborazione con la Commissione e l'ENISA, può effettuare valutazioni coordinate dei rischi per la sicurezza di specifiche catene di approvvigionamento critiche di servizi TIC, sistemi TIC o prodotti TIC, tenendo conto dei fattori di rischio tecnici e, se opportuno, non tecnici.

2. La Commissione, previa consultazione del gruppo di cooperazione e dell'ENISA, nonché, ove necessario, dei pertinenti portatori di interessi, identifica i servizi TIC, i sistemi TIC o i prodotti TIC critici specifici che possono essere oggetto della valutazione coordinata del rischio per la sicurezza di cui al paragrafo 1.

Articolo 23

Obblighi di segnalazione

1. Ciascuno Stato membro provvede affinché i soggetti essenziali e importanti notifichino senza indebito ritardo al proprio CSIRT o, se opportuno, alla propria autorità competente, conformemente al paragrafo 4, eventuali incidenti che hanno un impatto significativo sulla fornitura dei loro servizi quali indicati al paragrafo 3 (incidente significativo). Se opportuno, i soggetti interessati notificano senza indebito ritardo ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi. Ciascuno Stato membro provvede affinché tali soggetti comunichino, tra l'altro, qualunque informazione che consenta al CSIRT o, se opportuno, all'autorità competente di determinare l'eventuale impatto transfrontaliero dell'incidente. La sola notifica non espone il soggetto che la effettua a una maggiore responsabilità.

Qualora i soggetti interessati notifichino all'autorità competente un incidente significativo conformemente al primo comma, lo Stato membro provvede affinché l'autorità competente inoltri la notifica al CSIRT dopo averla ricevuta.

In caso di incidente significativo transfrontaliero o intersettoriale, gli Stati membri provvedono affinché i loro punti di contatto unici ricevano in tempo utile informazioni pertinenti notificate conformemente al paragrafo 4.

2. Se opportuno, gli Stati membri provvedono affinché i soggetti essenziali e importanti comunichino senza indebito ritardo ai destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa qualsiasi misura o azione correttiva che tali destinatari sono in grado di adottare in risposta a tale minaccia. Se opportuno, i soggetti informano tali destinatari anche della minaccia informatica significativa stessa.

3. Un incidente è considerato significativo se:

a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;

b) si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

4. Gli Stati membri provvedono affinché, ai fini della notifica a norma del paragrafo 1, i soggetti interessati trasmettano al CSIRT o, se opportuno, all'autorità competente:

a) senza indebito ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo, un preallarme che, se opportuno, indichi se l'incidente significativo è sospettato di essere il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;

b) senza indebito ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, se opportuno, aggiorni le informazioni di cui alla lettera a) e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;

c) su richiesta di un CSIRT o, se opportuno, di un'autorità competente, una relazione intermedia sui pertinenti aggiornamenti della situazione;

d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda:

   i) una descrizione dettagliata dell'incidente, comprensiva della sua gravità e del suo impatto;

   ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;

   iii) le misure di attenuazione adottate e in corso;

   iv) se opportuno, l'impatto transfrontaliero dell'incidente;

e) in caso di incidente in corso al momento della trasmissione della relazione finale di cui alla lettera d), gli Stati membri provvedono affinché i soggetti interessati forniscano una relazione sui progressi in quel momento e una relazione finale entro un mese dalla gestione dell'incidente.

In deroga al primo comma, lettera b), un prestatore di servizi fiduciari, in relazione a incidenti significativi che abbiano un impatto sulla fornitura dei suoi servizi fiduciari, informa il CSIRT o, se opportuno, l'autorità competente senza indebito ritardo e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo.

5. Senza indebito ritardo e ove possibile entro 24 ore dal ricevimento del preallarme di cui al paragrafo 4, lettera a), il CSIRT o l'autorità competente fornisce una risposta al soggetto notificante, comprendente un riscontro iniziale sull'incidente significativo e, su richiesta del soggetto, orientamenti o consulenza operativa sull'attuazione di possibili misure di attenuazione. Se il CSIRT non è il destinatario iniziale della notifica di cui al paragrafo 1, gli orientamenti sono forniti dall'autorità competente in cooperazione con il CSIRT. Su richiesta del soggetto interessato, il CSIRT fornisce ulteriore supporto tecnico. Qualora si sospetti che l'incidente significativo abbia carattere criminale, il CSIRT o l'autorità competente fornisce anche orientamenti sulla segnalazione dell'incidente significativo alle autorità di contrasto.

6. Se opportuno, e in particolare se l'incidente significativo interessa due o più Stati membri, il CSIRT, l'autorità competente o il punto di contatto unico ne informa senza indebito ritardo gli altri Stati membri interessati e l'ENISA. Tali informazioni includono o il tipo di informazioni ricevute a norma del paragrafo 4. Nel fare ciò, il CSIRT, l'autorità competente o il punto di contatto unico tutelano, in conformità al diritto dell'Unione o nazionale, la sicurezza e gli interessi commerciali del soggetto nonché la riservatezza delle informazioni fornite.

7. Qualora sia necessario sensibilizzare il pubblico per evitare un incidente significativo o affrontare un incidente significativo in corso, o qualora la divulgazione dell'incidente significativo sia altrimenti nell'interesse pubblico, dopo aver consultato il soggetto interessato il CSIRT di uno Stato membro o, se del caso, la sua autorità competente e, se opportuno, i CSIRT o le autorità competenti degli altri Stati membri interessati, possono informare il pubblico riguardo all'incidente significativo o imporre al soggetto di farlo.

8. Su richiesta del CSIRT o dell'autorità competente, il punto di contatto unico inoltra le notifiche ricevute a norma del paragrafo 1 ai punti di contatto unici degli altri Stati membri interessati.

9. Il punto di contatto unico trasmette ogni tre mesi all'ENISA una relazione di sintesi che comprende dati anonimizzati e aggregati sugli incidenti significativi, sugli incidenti, sulle minacce informatiche e sui quasi incidenti notificati conformemente al paragrafo 1 del presente articolo e all'articolo 30. Al fine di contribuire alla fornitura di informazioni comparabili, l'ENISA può adottare orientamenti tecnici sui parametri delle informazioni da includere nella relazione di sintesi. Ogni sei mesi l'ENISA informa il gruppo di cooperazione e la rete di CSIRT delle sue constatazioni in merito alle notifiche ricevute.

10. I CRSIRT o, se opportuno, le autorità competenti forniscono alle autorità competenti a norma della direttiva (UE) 2022/2557 le informazioni sugli incidenti significativi, sugli incidenti, sulle minacce informatiche e sui quasi incidenti notificati conformemente al paragrafo 1 del presente articolo e all'articolo 30 dai soggetti identificati come soggetti critici a norma della direttiva (UE) 2022/2557.

11. La Commissione può adottare atti di esecuzione che specifichino ulteriormente il tipo di informazioni, il relativo formato e la procedura di trasmissione di una notifica a norma del paragrafo 1 del presente articolo e dell'articolo 30 e di una comunicazione trasmessa a norma del paragrafo 2 del presente articolo.

Entro il 17 ottobre 2024 la Commissione adotta, per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, nonché i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network, atti di esecuzione che specifichino ulteriormente i casi in cui un incidente debba essere considerato significativo come indicato al paragrafo 3. La Commissione può adottare tali atti di esecuzione in relazione ad altri soggetti essenziali e importanti.

La Commissione scambia pareri e coopera con il gruppo di cooperazione in merito ai progetti di atto di esecuzione di cui al primo e secondo comma del presente paragrafo conformemente all'articolo 14, paragrafo 4, lettera e).

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.

Articolo 24

Uso dei sistemi europei di certificazione della cibersicurezza

1. Al fine di dimostrare il rispetto di determinate prescrizioni di cui all'articolo 21, gli Stati membri possono imporre ai soggetti essenziali e importanti di utilizzare determinati prodotti TIC, servizi TIC e processi TIC, sviluppati dal soggetto essenziale o importante o acquistati da terze parti, che siano certificati nell'ambito dei sistemi europei di certificazione della cibersicurezza adottati a norma dell'articolo 49 del regolamento (UE) 2019/881. Inoltre, gli Stati membri incoraggiano i soggetti essenziali e importanti a utilizzare servizi fiduciari qualificati.

2. Alla Commissione è conferito il potere di adottare atti delegati a norma dell'articolo 38 al fine di integrare la presente direttiva specificando quali categorie di soggetti essenziali e importanti sono tenute a utilizzare determinati prodotti TIC, servizi TIC e processi TIC certificati o a ottenere un certificato nell'ambito di un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 49 del regolamento (UE) 2019/881. Tali atti delegati sono adottati qualora siano stati individuati livelli insufficienti di cibersicurezza e includono un periodo di attuazione.

Prima di adottare tali atti delegati, la Commissione effettua una valutazione d'impatto e procede a consultazioni conformemente all'articolo 56 del regolamento (UE) 2019/881.

3. Qualora non siano disponibili sistemi di europei di certificazione della cibersicurezza adeguati ai fini del paragrafo 2 del presente articolo, la Commissione può chiedere all'ENISA, previa consultazione del gruppo di cooperazione e del gruppo europeo per la certificazione della cibersicurezza, di preparare una proposta di sistema a norma dell'articolo 48, paragrafo 2, del regolamento (UE) 2019/881.

Articolo 25

Normazione

1. Per promuovere l'attuazione convergente dell'articolo 21, paragrafi 1 e 2, gli Stati membri, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia, incoraggiano l'uso di norme e specifiche tecniche europee e internazionali relative alla sicurezza dei sistemi informatici e di rete.

2. L'ENISA, in cooperazione con gli Stati membri e, se opportuno, previa consultazione dei pertinenti portatori di interessi, elabora documenti di consulenza e orientamento riguardanti tanto i settori tecnici da prendere in considerazione in relazione al paragrafo 1, quanto le norme già esistenti, comprese le norme nazionali, che potrebbero essere applicate a tali settori.

CAPO V

GIURISDIZIONE E REGISTRAZIONE

Articolo 26

Giurisdizione e territorialità

1. I soggetti che rientrano nell'ambito di applicazione della presente direttiva sono considerati sotto la giurisdizione dello Stato membro nel quale sono stabiliti, ad eccezione dei casi seguenti:

a) i fornitori di reti pubbliche di comunicazione elettronica o i fornitori di servizi di comunicazione elettronica accessibili al pubblico, che sono considerati sotto la giurisdizione dello Stato membro nel quale forniscono i loro servizi;

b) i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i soggetti che forniscono servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online o di piattaforme di servizi di social network, che sono considerati sotto la giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione a norma del paragrafo 2;

c) gli enti della pubblica amministrazione, che sono considerati sotto la giurisdizione dello Stato membro che li ha istituiti.

2. Ai fini della presente direttiva, si considera che un soggetto di cui al paragrafo 1, lettera b), abbia il proprio stabilimento principale nell'Unione nello Stato membro in cui sono prevalentemente adottate le decisioni relative alle misure di gestione del rischio di cibersicurezza. Se non è possibile determinare detto Stato membro o se tali decisioni non sono adottate nell'Unione, lo stabilimento principale è considerato essere nello Stato membro in cui sono effettuate le operazioni di cibersicurezza. Se non è possibile determinare detto Stato membro, si considera che lo stabilimento principale sia nello Stato membro in cui il soggetto interessato ha lo stabilimento con il maggior numero di dipendenti nell'Unione.

3. Se un soggetto di cui al paragrafo 1, lettera b), non è stabilito nell'Unione, ma offre servizi nell'Unione, esso designa un rappresentante nell'Unione. Il rappresentante è stabilito in uno degli Stati membri in cui sono offerti i servizi. Tale soggetto è considerato sotto la giurisdizione dello Stato membro in cui è stabilito il suo rappresentante. Nell'assenza di un rappresentante nell'Unione designato a norma del presente paragrafo, qualsiasi Stato membro in cui il soggetto fornisce servizi può avviare un'azione legale nei confronti del soggetto per violazione degli obblighi della presente direttiva.

4. La designazione di un rappresentante da parte di un soggetto di cui al paragrafo 1, lettera b), fa salve le azioni legali che potrebbero essere avviate nei confronti del soggetto stesso.

5. Gli Stati membri che hanno ricevuto una richiesta di assistenza reciproca in relazione a un soggetto di cui al paragrafo 1, lettera b), possono, entro i limiti della richiesta, adottare misure di vigilanza e di esecuzione adeguate in relazione al soggetto interessato che fornisce servizi o che ha un sistema informatico e di rete nel loro territorio.

Articolo 27

Registro dei soggetti

1. L'ENISA crea e mantiene un registro di fornitori di servizi DNS, registri dei nomi di dominio di primo livello, soggetti che forniscono servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, fornitori di servizi di data center, fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, fornitori di servizi di sicurezza gestiti, nonché fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network sulla base delle informazioni ricevute dai punti di contatto unici conformemente al paragrafo 4. Su richiesta, l'ENISA consente alle autorità competenti di accedere a tale registro, assicurando nel contempo la tutela della riservatezza delle informazioni, se del caso.

2. Gli Stati membri esigono che i soggetti di cui al paragrafo 1 trasmettano entro il 17 gennaio 2025, le informazioni seguenti alle autorità competenti:

a) il proprio nome;

b) il settore, il sottosettore e il tipo di soggetto di cui all'allegato I o II, se del caso;

c) l'indirizzo dello stabilimento principale e degli altri stabilimenti legali del soggetto nell'Unione o, se non è stabilito nell'Unione, del suo rappresentante a norma dell'articolo 26, paragrafo 3;

d) i dati di contatto aggiornati, compresi gli indirizzi e-mail e i numeri di telefono del soggetto, e, se opportuno, del suo rappresentante a norma dell'articolo 26, paragrafo 3;

e) gli Stati membri in cui il soggetto fornisce i suoi servizi; e

f) le serie di IP del soggetto.

3. Gli Stati membri provvedono affinché i soggetti di cui al paragrafo 1 notifichino all'autorità competente qualsiasi modifica dei dettagli trasmessi a norma del paragrafo 2 tempestivamente e, in ogni caso, entro tre mesi dalla data della modifica.

4. In seguito alla ricezione delle informazioni di cui ai paragrafi 2 e 3, ad eccezione di quelle di cui al paragrafo 2, lettera f), il punto di contatto unico dello Stato membro interessato, senza ritardo, le inoltra all'ENISA.

5. Se opportuno, le informazioni di cui ai paragrafi 2 e 3 del presente articolo sono trasmesse attraverso il meccanismo nazionale di cui all'articolo 3, paragrafo 4, quarto comma.

Articolo 28

Banca dati dei dati di registrazione dei nomi di dominio

1. Per contribuire alla sicurezza, alla stabilità e alla resilienza del DNS, gli Stati membri impongono ai registri dei nomi di TLD e ai soggetti che forniscono servizi di registrazione dei nomi di dominio di raccogliere e mantenere dati di registrazione dei nomi di dominio accurati e completi in un'apposita banca dati con la dovuta diligenza, conformemente al diritto dell'Unione in materia di protezione dei dati per quanto riguarda i dati personali.

2. Ai fini del paragrafo 1, gli Stati membri esigono che la banca dati dei dati di registrazione dei nomi di dominio contenga le informazioni necessarie per identificare e contattare i titolari dei nomi di dominio e i punti di contatto che amministrano i nomi di dominio sotto i TLD. Tali informazioni includono:

a) il nome di dominio;

b) la data di registrazione;

c) il nome, l'indirizzo e-mail di contatto e il numero di telefono del soggetto che procede alla registrazione;

d) l'indirizzo e-mail di contatto e il numero di telefono del punto di contatto che amministra il nome di dominio qualora siano diversi da quelli del soggetto che procede alla registrazione.

3. Gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio predispongano politiche e procedure, incluse procedure di verifica, per garantire che le banche dati di cui al paragrafo 1 comprendano informazioni accurate e complete. Gli Stati membri esigono che tali politiche e procedure siano rese pubbliche.

4. Gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD rendano pubblicamente disponibili, senza indebito ritardo dopo la registrazione di un nome di dominio, i dati di registrazione dei nomi di dominio che non sono dati personali.

5. Gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio, su richiesta legittima e debitamente motivata di legittimi richiedenti l'accesso, forniscano l'accesso a specifici dati di registrazione dei nomi di dominio, nel rispetto del diritto dell'Unione in materia di protezione dei dati. Gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio rispondano senza indebito ritardo e comunque entro 72 ore dalla ricezione delle richieste di accesso. Gli Stati membri esigono che le politiche e le procedure relative alla divulgazione di tali dati siano rese pubbliche.

6. Il rispetto degli obblighi di cui ai paragrafi da 1 a 5 non comportano una duplicazione della raccolta di dati di registrazione dei nomi di dominio. A tal fine, gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio collaborino tra loro.

CAPO VI

CONDIVISIONE DELLE INFORMAZIONI

Articolo 29

Accordi di condivisione delle informazioni sulla cibersicurezza

1. Gli Stati membri provvedono affinché i soggetti che rientrano nell'ambito di applicazione della presente direttiva e, se del caso, altri soggetti che non rientrano nell'ambito di applicazione della presente direttiva siano in grado di scambiarsi, su base volontaria, pertinenti informazioni sulla cibersicurezza, comprese informazioni relative a minacce informatiche, quasi incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli attori delle minacce, allarmi di cibersicurezza e raccomandazioni concernenti la configurazione degli strumenti di cibersicurezza per individuare le minacce informatiche, se tale condivisione di informazioni:

a) mira a prevenire o rilevare gli incidenti, a riprendersi dagli stessi o ad attenuarne l'impatto;

b) aumenta il livello di cibersicurezza, in particolare sensibilizzando in merito alle minacce informatiche, limitando o inibendo la capacità di diffusione di tali minacce e sostenendo una serie di capacità di difesa, la risoluzione e la divulgazione delle vulnerabilità, tecniche di rilevamento, contenimento e prevenzione delle minacce, strategie di attenuazione o fasi di risposta e recupero, oppure promuovendo la ricerca collaborativa sulle minacce informatiche tra soggetti pubblici e privati.

2. Gli Stati membri provvedono affinché lo scambio di informazioni avvenga nell'ambito di comunità di soggetti essenziali e importanti e, se opportuno, dei loro fornitori o fornitori di servizi. Tale scambio è attuato mediante accordi di condivisione delle informazioni sulla cibersicurezza che tengono conto della natura potenzialmente sensibile delle informazioni condivise.

3. Gli Stati membri facilitano la conclusione degli accordi di condivisione delle informazioni sulla cibersicurezza di cui al paragrafo 2 del presente articolo. Gli Stati membri possono specificare gli elementi operativi, compreso l'uso di piattaforme TIC dedicate e di strumenti di automazione, i contenuti e le condizioni degli accordi di condivisione delle informazioni. Nello stabilire i dettagli relativi alla partecipazione delle autorità pubbliche a tali accordi, gli Stati membri possono imporre condizioni per le informazioni messe a disposizione dalle autorità competenti o dai CSIRT. Gli Stati membri offrono assistenza per l'applicazione di tali accordi conformemente alle loro misure strategiche di cui all'articolo 7, paragrafo 2, lettera h).

4. Gli Stati membri provvedono affinché i soggetti essenziali e importanti notifichino alle autorità competenti la loro partecipazione agli accordi di condivisione delle informazioni sulla cibersicurezza di cui al paragrafo 2 al momento della conclusione di tali accordi o, se opportuno, del loro ritiro da tali accordi, una volta che questo è divenuto effettivo.

5. L'ENISA offre assistenza per la conclusione di accordi di condivisione delle informazioni sulla cibersicurezza di cui al paragrafo 2 fornendo orientamenti e provvedendo allo scambio delle migliori pratiche.

Articolo 30

Notifica volontaria di informazioni pertinenti

1. Gli Stati membri provvedono affinché, in aggiunta all'obbligo di notifica di cui all'articolo 23, possano essere trasmesse, su base volontaria, notifiche ai CSIRT o, se opportuno, alle autorità competenti, da parte dei:

a) soggetti essenziali e importanti, per quanto riguarda gli incidenti, le minacce informatiche e i quasi incidenti;

b) soggetti diversi da quelli di cui alla lettera a), indipendentemente dal fatto che ricadano o meno nell'ambito di applicazione della presente direttiva, per quanto riguarda gli incidenti significativi, le minacce informatiche e i quasi incidenti.

2. Gli Stati membri trattano le notifiche di cui al paragrafo 1 del presente articolo secondo la procedura di cui all'articolo 23. Gli Stati membri possono trattare le notifiche obbligatorie prioritariamente rispetto alle notifiche volontarie.

Se necessario, i CSIRT e, se del caso, le autorità competenti forniscono ai punti di contatto unici le informazioni sulle notifiche ricevute a norma del presente articolo, garantendo nel contempo la riservatezza e la tutela adeguata delle informazioni fornite dal soggetto notificante. Fatti salvi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati, la segnalazione volontaria non ha l'effetto di imporre al soggetto notificante alcun obbligo aggiuntivo a cui non sarebbe stato sottoposto se non avesse trasmesso la notifica.

CAPO VII

VIGILANZA ED ESECUZIONE

Articolo 31

Aspetti generali relativi alla vigilanza e all'esecuzione

1. Gli Stati membri provvedono affinché le proprie autorità competenti monitorino efficacemente e adottino le misure necessarie a garantire il rispetto della presente direttiva.

2. Gli Stati membri possono consentire alle proprie autorità competenti di conferire priorità ai compiti di vigilanza. Tale priorità si fonda su un approccio basato sul rischio. A tal fine, nell'esercizio dei rispettivi compiti di vigilanza di cui agli articoli 32 e 33, le autorità competenti possono stabilire metodologie di vigilanza che consentano di conferire priorità a tali compiti secondo un approccio basato sul rischio.

3. Le autorità competenti operano in stretta cooperazione con le autorità di controllo ai sensi del regolamento (UE) 2016/679 nei casi di incidenti che comportano violazioni di dati personali, senza pregiudicare la competenza e i compiti delle autorità di controllo di cui a tale regolamento.

4. Fatti salvi i quadri legislativi e istituzionali nazionali, gli Stati membri provvedono affinché nel vigilare sul rispetto, da parte degli enti della pubblica amministrazione, della presente direttiva e nell'imporre misure di esecuzione in caso di violazione della presente direttiva, le autorità competenti dispongano dei poteri adeguati per svolgere tali compiti con indipendenza operativa rispetto agli enti della pubblica amministrazione sottoposti a vigilanza. Gli Stati membri possono decidere di imporre misure di vigilanza e di esecuzione adeguate, proporzionate ed efficaci in relazione a tali enti conformemente ai quadri legislativi e istituzionali nazionali.

Articolo 32

Misure di vigilanza e di esecuzione relative a soggetti essenziali

1. Gli Stati membri provvedono affinché le misure di vigilanza o di esecuzione imposte ai soggetti essenziali per quanto riguarda gli obblighi di cui alla presente direttiva siano effettive, proporzionate e dissuasive, tenuto conto delle circostanze di ciascun singolo caso.

2. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti importanti, abbiano il potere di sottoporre tali soggetti come minimo a:

a) ispezioni in loco e vigilanza a distanza, compresi controlli casuali, effettuati da professionisti formati;

b) audit sulla sicurezza periodici e mirati effettuati da un organismo indipendente o da un'autorità competente;

c) audit ad hoc, ivi incluso in casi giustificati da un incidente significativo o da una violazione della presente direttiva da parte del soggetto essenziale;

d) scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato;

e) richieste di informazioni necessarie a valutare le misure di gestione dei rischi di cibersicurezza adottate dal soggetto interessato, comprese le politiche di cibersicurezza documentate, nonché il rispetto dell'obbligo di trasmettere informazioni alle autorità competenti a norma dell'articolo 27;

f) richieste di accesso a dati, documenti e altre informazioni necessari allo svolgimento dei compiti di vigilanza;

g) richieste di dati che dimostrino l'attuazione di politiche di cibersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova.

Gli audit sulla sicurezza mirati di cui al primo comma, lettera b), si basano su valutazioni del rischio effettuate dall'autorità competente o dal soggetto sottoposto ad audit o su altre informazioni disponibili in materia di rischi.

I risultati di eventuali audit sulla sicurezza mirati sono messi a disposizione dell'autorità competente. I costi di tale audit sulla sicurezza mirato svolto da un organismo indipendente sono a carico del soggetto sottoposto ad audit, salvo in casi debitamente giustificati in cui l'autorità competente decida altrimenti.

3. Nell'esercizio dei loro poteri di cui al paragrafo 2, lettera e), f) o g), le autorità competenti dichiarano la finalità della richiesta e specificano le informazioni richieste.

4. Gli Stati membri provvedono affinché le proprie autorità competenti, nell'esercizio dei rispettivi poteri di esecuzione nei confronti dei soggetti essenziali, abbiano il potere come minimo di:

a) emanare avvertimenti relativi a violazioni della presente direttiva da parte dei soggetti interessati;

b) adottare istruzioni vincolanti, ivi incluso per quanto riguarda le misure richieste per evitare il verificarsi di un incidente o porvi rimedio, nonché i termini per l'attuazione di tali misure e per riferire in merito alla loro attuazione, o un'ingiunzione che impongano ai soggetti interessati di porre rimedio alle carenze individuate o alle violazioni della direttiva;

c) imporre ai soggetti interessati di porre termine al comportamento che viola la presente direttiva e di astenersi dal ripeterlo;

d) imporre ai soggetti interessati di provvedere affinché le loro misure di gestione del rischio di cibersicurezza siano conformi all'articolo 21 o di adempiere gli obblighi di segnalazione di cui all'articolo 23 in una maniera ed entro un termine specificati;

e) imporre ai soggetti interessati di informare le persone fisiche o giuridiche cui forniscono servizi o per cui svolgono attività che sono potenzialmente interessati da una minaccia informatica significativa in merito alla natura della minaccia, nonché in merito alle eventuali misure protettive o correttive che possano essere adottate da tali persone fisiche o giuridiche in risposta a tale minaccia;

f) imporre ai soggetti interessati di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza entro un termine ragionevole;

g) designare un funzionario addetto alla sorveglianza con compiti ben definiti nell'arco di un periodo di tempo determinato al fine di vigilare sul rispetto degli articoli 18 e 20;

h) imporre ai soggetti interessati di rendere pubblici gli aspetti delle violazioni della presente direttiva in una maniera specificata;

i) imporre o chiedere l'imposizione, da parte degli organismi o degli organi giurisdizionali pertinenti secondo il diritto nazionale, di una sanzione amministrativa pecuniaria a norma dell'articolo 34, in aggiunta a qualsiasi delle misure di cui al presente paragrafo, lettere da a) a h).

5. Qualora le misure di esecuzione adottate a norma del paragrafo 4, lettere da a) a d), e lettera f), si rivelino inefficaci, gli Stati membri provvedono affinché le proprie autorità competenti abbiano il potere di fissare un termine entro il quale il soggetto essenziale è tenuto ad adottare le misure necessarie a porre rimedio alle carenze o a conformarsi alle prescrizioni di tali autorità. Se le misure richieste non sono adottate entro il termine stabilito, gli Stati membri provvedono affinché le proprie autorità competenti abbiano il potere di:

a) sospendere temporaneamente o chiedere a un organismo di certificazione o autorizzazione, oppure a un organo giurisdizionale, secondo il diritto nazionale, di sospendere temporaneamente un certificato o un'autorizzazione relativi a una parte o alla totalità dei servizi o delle attività pertinenti svolti dal soggetto essenziale;

b) chiedere che gli organismi o gli organi giurisdizionali pertinenti, secondo il diritto nazionale, vietino temporaneamente a qualsiasi persona che svolga funzioni dirigenziali a livello di amministratore delegato o rappresentante legale in tale soggetto essenziale di svolgere funzioni dirigenziali in tale soggetto.

Le sospensioni o i divieti temporanei a norma del presente paragrafo sono applicati solo finché il soggetto interessato non adotta le misure necessarie a porre rimedio alle carenze o a conformarsi alle prescrizioni dell'autorità competente per le quali le misure di esecuzione sono state applicate. L'imposizione di tali sospensioni o divieti temporanei è soggetta a garanzie procedurali appropriate in conformità ai principi generali del diritto dell'Unione e della Carta, inclusi il diritto a un ricorso effettivo e ad un giusto processo, la presunzione di innocenza e i diritti della difesa.

Le misure di esecuzione previste dal presente paragrafo non sono applicabili agli enti della pubblica amministrazione che sono soggetti alla presente direttiva.

6. Gli Stati membri provvedono affinché qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante legale sulla base del potere di rappresentarlo, dell'autorità di prendere decisioni per suo conto o dell'autorità di esercitare un controllo su di esso abbia il potere di garantirne il rispetto della presente direttiva. Gli Stati membri provvedono affinché tali persone fisiche possano essere ritenute responsabili dell'inadempimento dei loro doveri di garantire il rispetto della presente direttiva.

Per quanto riguarda gli enti della pubblica amministrazione, il presente paragrafo lascia impregiudicato il diritto nazionale in materia di responsabilità dei dipendenti pubblici e dei funzionari eletti o nominati.

7. Nell'adottare qualsiasi misura di esecuzione di cui al paragrafo 4 o 5, le autorità competenti rispettano i diritti della difesa e tengono conto delle circostanze di ciascun singolo caso e almeno degli elementi seguenti:

a) la gravità della violazione e l'importanza delle disposizioni violate, essendo le violazioni seguenti, tra l'altro, da considerarsi gravi:

   i) le violazioni ripetute;

   ii) la mancata notifica di incidenti significativi o il mancato rimedio a tali incidenti;

   iii) il mancato rimedio alle carenze a seguito di istruzioni vincolanti emesse dalle autorità competenti;

   iv) l'ostacolo degli audit o delle attività di monitoraggio imposte dall'autorità competente a seguito del rilevamento di una violazione;

   v) la fornitura di informazioni false o gravemente inesatte relative alle misure in materia di gestione o segnalazione del rischio di cibersicurezza di cui agli articoli 21 e 23;

b) la durata della violazione;

c) eventuali precedenti violazioni pertinenti commesse dal soggetto interessato;

d) qualsiasi danno materiale o immateriale causato, incluse le perdite finanziarie o economiche, gli effetti sugli altri servizi e il numero di utenti interessati;

e) un'eventuale condotta intenzionale o negligenza da parte dell'autore della violazione;

f) qualsiasi misure adottata dal soggetto per prevenire o attenuare il danno materiale o immateriale;

g) qualsiasi adesione a codici di condotta o meccanismi di certificazione approvati;

h) il livello di collaborazione delle persone fisiche o giuridiche ritenute responsabili con le autorità competenti.

8. Le autorità competenti espongono nei particolari la motivazione delle loro misure di esecuzione. Prima di adottare tali misure le autorità competenti notificano ai soggetti interessati le loro conclusioni preliminari. Esse concedono inoltre a tali soggetti un tempo ragionevole per presentare osservazioni, salvo in casi debitamente giustificati in cui ciò impedirebbe di agire con immediatezza per prevenire un incidente o rispondervi.

9. Gli Stati membri provvedono affinché le loro autorità competenti di cui alla presente direttiva informino le autorità competenti pertinenti all'interno dello stesso Stato membro a norma della direttiva (UE) 2022/2557 quando esercitano i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi stabiliti dalla presente direttiva da parte di un soggetto identificato come critico a norma della direttiva (UE) 2022/2557. Se del caso, le autorità competenti di cui alla direttiva (UE) 2022/2557 possono chiedere alle autorità competenti di cui alla presente direttiva di esercitare i propri poteri di vigilanza e di esecuzione in relazione a un soggetto che è stato individuato come soggetto critico ai sensi della direttiva (UE) 2022/2557.

10. Gli Stati membri provvedono affinché le loro autorità competenti ai sensi della presente direttiva cooperino con le pertinenti autorità competenti dello Stato membro interessato a norma del regolamento (UE) 2022/2554. In particolare, gli Stati membri provvedono affinché le loro autorità competenti a norma della presente direttiva informino il forum di sorveglianza istituito ai sensi dell'articolo 32, paragrafo 1, del regolamento (UE) 2022/2554 quando esercitano i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi previsti dalla presente direttiva da parte di un soggetto essenziale designato come fornitore terzo critico di servizi di TIC a norma dell'articolo 31 del regolamento (UE) 2022/2554

Articolo 33

Vigilanza ed esecuzione relative a soggetti essenziali

1. Se ricevono elementi di prova, indicazioni o informazioni secondo cui un soggetto importante non rispetta presumibilmente la presente direttiva, in particolare dagli articoli 21 e 23 della medesima, gli Stati membri provvedono affinché le autorità competenti intervengano, se necessario, mediante misure di vigilanza ex post. Gli Stati membri provvedono affinché tali misure siano efficaci, proporzionate e dissuasive, tenendo conto delle circostanze di ogni singolo caso.

2. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti importanti, abbiano il potere di sottoporre tali soggetti come minimo a:

a) ispezioni in loco e vigilanza ex post a distanza, effettuate da professionisti formati;

b) audit sulla sicurezza mirati svolti da un organismo indipendente o da un'autorità competente;

c) scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario, con la cooperazione del soggetto interessato;

(d) richieste di qualsiasi informazione necessaria a valutare ex post le misure di gestione dei rischi di cibersicurezza adottate dal soggetto, comprese le politiche di cibersicurezza documentate, nonché il rispetto degli obblighi di trasmettere informazioni alle autorità competenti a norma dell'articolo 27;

e) richieste di accesso a dati, documenti e/o informazioni necessari allo svolgimento dei propri compiti di vigilanza;

f) richieste di dati che dimostrino l'attuazione di politiche di cibersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova.

Gli audit sulla sicurezza mirati di cui al primo comma, lettera b), si basano su valutazioni del rischio effettuate dall'autorità competente o dal soggetto sottoposto ad audit o su altre informazioni disponibili in materia di rischi.

I risultati di eventuali audit sulla sicurezza mirati sono messi a disposizione dell'autorità competente. I costi di tale audit sulla sicurezza mirato svolto da un organismo indipendente sono a carico del soggetto sottoposto a audit, salvo in casi debitamente giustificati in cui l'autorità competente decida altrimenti.

3. Nell'esercizio dei loro poteri a norma del paragrafo 2, lettere d), e) o f), le autorità competenti dichiarano la finalità della richiesta e specificano le informazioni richieste.

4. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi poteri di esecuzione nei confronti dei soggetti importanti, abbiano il potere come minimo di:

a) emanare avvertimenti relativi a violazioni della presente direttiva da parte dei soggetti interessati;

b) adottare istruzioni vincolanti o un'ingiunzione che impongano a tali soggetti di porre rimedio alle carenze individuate o alle violazioni degli obblighi della presente direttiva;

c) imporre ai soggetti interessati di porre termine alle condotte in violazione della presente direttiva e di astenersi dal ripeterle;

d) imporre ai soggetti interessati di provvedere affinché le loro misure di gestione dei rischi di cibersicurezza siano conformi all'articolo 21 o i loro obblighi di segnalazione conformi alle prescrizioni di cui all'articolo 23 in una maniera ed entro un termine specificati;

e) imporre ai soggetti interessati di informare le persone fisiche o giuridiche cui forniscono servizi o per cui svolgono attività potenzialmente interessati da una minaccia informatica significativa in merito alla natura della minaccia e alle eventuali misure protettive o correttive che possano essere adottate da tali persone fisiche o giuridiche in risposta a tale minaccia;

f) imporre agli interessati di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza entro un termine ragionevole;

g) imporre ai soggetti interessati di rendere pubblici gli aspetti delle violazioni della presente direttiva in una maniera specificata;

h) imporre o chiedere l'imposizione, da parte degli organismi o degli organi giurisdizionali pertinenti secondo la legislazione nazionale, di una sanzione amministrativa pecuniaria a norma dell'articolo 34, in aggiunta a una qualsiasi delle misure di cui al presente paragrafo, lettere da a) a g).

5. L'articolo 32, paragrafi 6, 7 e 8, si applica mutatis mutandis alle misure di vigilanza ed esecuzione di cui al presente articolo per soggetti importanti.

6. Gli Stati membri provvedono affinché le loro autorità competenti ai sensi della presente direttiva cooperino con le pertinenti autorità competenti dello Stato membro interessato a norma del regolamento (UE) 2022/2554. In particolare, gli Stati membri provvedono affinché le loro autorità competenti a norma della presente direttiva informino il forum di sorveglianza istituito ai sensi dell'articolo 32, paragrafo 1, del regolamento (UE) 2022/2554 quando esercitano i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi previsti dalla presente direttiva da parte di un soggetto importante designato come fornitore terzo critico di servizi di TIC a norma dell'articolo 31 del regolamento (UE) 2022/2554.

Articolo 34

Condizioni generali per imporre sanzioni amministrative pecuniarie ai soggetti essenziali e importanti

1. Gli Stati membri provvedono affinché le sanzioni amministrative pecuniarie imposte ai soggetti essenziali e importanti a norma del presente articolo in relazione alle violazioni della presente direttiva siano effettive, proporzionate e dissuasive, tenendo conto delle circostanze di ogni singolo caso.

2. Le sanzioni amministrative pecuniarie sono imposte in aggiunta a qualsiasi delle misure di cui all'articolo 32, paragrafo 4, lettere da a) a h), all'articolo 32, paragrafo 5, e all'articolo 33, paragrafo 4, lettere da a) a g).

3. Nel decidere se imporre una sanzione amministrativa pecuniaria e il relativo importo in ciascun singolo caso si tiene debitamente conto almeno degli elementi di cui all'articolo 32, paragrafo 7.

4. Gli Stati membri provvedono affinché, ove violino l'articolo 21 o 23, i soggetti essenziali siano soggetti, conformemente ai paragrafi 2 e 3 del presente articolo, a sanzioni pecuniarie amministrative pari a un massimo di almeno 10 000 000 EUR o a un massimo di almeno il 2 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto essenziale appartiene, se tale importo è superiore.

5. Gli Stati membri provvedono affinché, ove violino l'articolo 21 o 23, i soggetti importanti siano soggetti, conformemente ai paragrafi 2 e 3 del presente articolo, a sanzioni pecuniarie amministrative pari a un massimo di almeno 7 000 000 EUR o a un massimo di almeno l'1,4 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto importante appartiene, se tale importo è superiore.

6. Gli Stati membri possono prevedere la facoltà di infliggere penalità di mora al fine di imporre a un soggetto essenziale o importante di cessare una violazione della presente direttiva conformemente a una precedente decisione dell'autorità competente.

7. Fatti salvi i poteri delle autorità competenti a norma degli articoli 32 e 33, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere imposte sanzioni amministrative pecuniarie agli enti della pubblica amministrazione.

8. Se l'ordinamento giuridico di uno Stato membro non prevede sanzioni amministrative pecuniarie, lo Stato membro in questione provvede affinché il presente articolo possa applicarsi in maniera tale che l'azione sanzionatoria sia avviata dall'autorità competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità competenti. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Lo Stato membro notifica alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro il 17 ottobre 2024 e ne comunicano senza ritardo ogni successiva modifica.

Articolo 35

Violazioni che comportano una violazione dei dati personali

1. Qualora le autorità competenti, in sede di vigilanza o di esecuzione, vengano a conoscenza del fatto che la violazione degli obblighi di cui agli articoli 21 e 23 della presente direttiva da parte di un soggetto essenziale o importante possa comportare una violazione dei dati personali, quale definita all'articolo 4, punto 12), del regolamento (UE) 2016/679, che deve essere notificata a norma dell'articolo 33 del medesimo regolamento, ne informano senza indebito ritardo le autorità di controllo competenti a norma dell'articolo 55 o 56 di tale regolamento.

2. Qualora le autorità di controllo di cui all'articolo 55 o 56 del regolamento (UE) 2016/679 impongano una sanzione amministrativa pecuniaria a norma dell'articolo 58, paragrafo 2, lettera i), del medesimo regolamento, le autorità competenti non impongono una sanzione amministrativa pecuniaria a norma dell'articolo 34 della presente direttiva per una violazione di cui al presente articolo, paragrafo 1, imputabile al medesimo comportamento punito con l'ammenda amministrativa pecuniaria a norma dell'articolo 58, paragrafo 2, lettera i), del regolamento (UE) 2016/679. Le autorità competenti possono tuttavia imporre le misure di esecuzione di cui all'articolo 32, paragrafo 4, lettere da a) a h), all'articolo 32, paragrafo 5, e all'articolo 33, paragrafo 4, lettere da a) a g) della presente direttiva.

3. Qualora l'autorità di controllo competente a norma del regolamento (UE) 2016/679 sia stabilita in uno Stato membro diverso rispetto all'autorità competente, l'autorità competente informa l'autorità di controllo stabilita nel proprio Stato membro della potenziale violazione dei dati personali di cui al paragrafo 1.

Articolo 36

Sanzioni

Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione delle misure nazionali adottate in attuazione della presente direttiva e adottano tutte le misure necessarie per assicurarne l'applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive. Gli Stati membri comunicano alla Commissione, entro il 17 gennaio 2025, tali norme e misure e la informano, immediatamente, di qualsiasi modifica apportata successivamente.

Articolo 37

Assistenza reciproca

1. Se un soggetto fornisce servizi in più di uno Stato membro o fornisce servizi in uno o più Stati membri e i suoi sistemi informatici e di rete sono ubicati in uno o più altri Stati membri, le autorità competenti degli Stati membri interessati cooperano e si assistono reciprocamente in funzione delle necessità. Tale cooperazione comprende, almeno, gli aspetti seguenti:

a) le autorità competenti che applicano misure di vigilanza o di esecuzione in uno Stato membro informano e consultano, attraverso il punto di contatto unico, le autorità competenti degli altri Stati membri interessati in merito alle misure di vigilanza ed esecuzione adottate;

b) un'autorità competente può chiedere a un'altra autorità competente di adottare misure di vigilanza o esecuzione;

c) un'autorità competente, dopo aver ricevuto una richiesta giustificata da un'altra autorità competente, fornisce a tale altra autorità competente un'assistenza reciproca proporzionata alle proprie risorse affinché le misure di vigilanza o esecuzione possano essere attuate in maniera efficace, efficiente e coerente.

L'assistenza reciproca di cui al primo comma. Lettera c), può riguardare richieste di informazioni e misure di vigilanza, comprese richieste di effettuare ispezioni in loco o vigilanza a distanza o audit sulla sicurezza mirati. Un'autorità competente destinataria di una richiesta di assistenza non può respingerla a meno che non abbia stabilito che essa non è competente per fornire l'assistenza richiesta, che l'assistenza richiesta non è proporzionata ai compiti di vigilanza svolti dall'autorità competente o che la richiesta riguarda informazioni o comporta attività che, se divulgate o svolte, sarebbero contrari agli interessi essenziali della sicurezza nazionale, la pubblica sicurezza o la difesa dello Stato membro in questione. Prima di respingere tale richiesta, l'autorità competente consulta le altre autorità competenti interessate e, su richiesta di uno degli Stati membri interessati, la Commissione e l'ENISA,

2. Se opportuno e di comune accordo le autorità competenti di diversi Stati membri possono svolgere le attività di vigilanza comuni.

CAPO VIII

ATTI DELEGATI E ATTI DI ESECUZIONE

Articolo 38

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare atti delegati di cui all'articolo 24, paragrafo 2, è conferito alla Commissione per un periodo di cinque anni a decorrere dal 16 gennaio 2023.

3. La delega di potere di cui all'articolo 24, paragrafo 2, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016.

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato a norma dell'articolo 24, paragrafo 2, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 39

Procedura di comitato

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

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

3. Laddove il parere del comitato debba essere ottenuto con procedura scritta, questa si conclude senza esito quando, entro il termine per la formulazione del parere, il presidente del comitato decida in tal senso o un membro del comitato lo richieda.

CAPO IX

DISPOSIZIONI FINALI

Articolo 40

Riesame

Entro il 17 ottobre 2027 e successivamente ogni 36 mesi, la Commissione riesamina il funzionamento della presente direttiva e presenta una relazione in proposito al Parlamento europeo e al Consiglio. La relazione valuta in particolare la pertinenza delle dimensioni dei soggetti interessati, e i settori, sottosettori e tipologie di soggetti di cui agli allegati I e II per il funzionamento dell'economia e della società in relazione alla cibersicurezza. A tal fine e allo scopo di intensificare ulteriormente la cooperazione strategica e operativa, la Commissione tiene conto delle relazioni del gruppo di cooperazione e della rete di CSIRT sull'esperienza acquisita a livello strategico e operativo. La relazione è corredata, se necessario, di una proposta legislativa.

Articolo 41

Recepimento

1. Entro il 17 ottobre 2024, gli Stati membri adottano e pubblicano le misure necessarie per conformarsi alla presente direttiva. Essi comunicano immediatamente alla Commissione il testo di tali disposizioni.

Essi applicano tali disposizioni a decorrere dal 18 ottobre 2024.

2. Le disposizioni di cui al paragrafo 1 adottate dagli Stati membri contengono un riferimento alla presente direttiva o sono corredate di tale riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono stabilite dagli Stati membri.

Articolo 42

Modifica del regolamento (UE) n. 910/2014

Nel regolamento (UE) n. 910/2014, l'articolo 19 è soppresso con effetto a decorrere dal 18 ottobre 2024.

Articolo 43

Modifica della direttiva (UE) 2018/1972

Nella direttiva (UE) 2018/1972, gli articoli 40 e 41 sono soppressi. con effetto a decorrere dal 18 ottobre 2024.

Articolo 44

Abrogazione

La direttiva (UE) 2016/1148 è abrogata con effetto a decorrere dal 18 ottobre 2024.

I riferimenti alla direttiva abrogata si intendono fatti alla presente direttiva e vanno letti secondo la tavola di concordanza di cui all'allegato III.

Articolo 45

Entrata in vigore

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

Articolo 46

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Strasburgo, 14 dicembre 2022

Per il Parlamento europeo	*Per il Consiglio*
La presidente	*Il presidente*
R. METSOLA	M. BEK

ALLEGATO I

SETTORI AD ALTA CRITICITÀ

Settore	Sottosettore	Tipo di soggetto
1. Energia	a) Energia elettrica	— Impresa elettrica quale definita all'articolo 2, punto 57), della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio ([1]) che esercita attività di «fornitura» quale definita all'articolo 2, punto 12), di tale direttiva
		— Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 29), della direttiva (UE) 2019/944
		— Gestori del sistema di trasmissione quali definiti all'articolo 2, punto 35), della direttiva (UE) 2019/944
		— Produttori quali definiti all'articolo 2, punto 38), della direttiva (UE) 2019/944
		— Gestori del mercato elettrico designato quali definiti all'articolo 2, punto 8), del regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio ([2]) — Partecipanti al mercato dell'energia elettrica quali definiti all'articolo 2, punto 25), del regolamento (UE) 2019/943 che forniscono servizi di aggregazione, gestione della domanda o stoccaggio di energia quali definiti all'articolo 2, punti 18), 20) e 59) della direttiva (UE) 2019/944 — Gestori di un punto di ricarica responsabili della gestione e del funzionamento di un punto di ricarica che fornisce un servizio di ricarica a utenti finali, anche in nome e per conto di un fornitore di servizi di mobilità
	b) Teleriscaldamento e teleraffrescamento	— Gestori di teleriscaldamento o teleraffrescamento quali definiti all'articolo 2, punto 19), della direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio ([3])
	c) Petrolio	— Gestori di oleodotti
		— Gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio
		— Organismi centrali di stoccaggio quali definiti all'articolo 2, lettera f), della direttiva 2009/119/CE del Consiglio ([4])
	d) Gas	— Imprese fornitrici quali definite all'articolo 2, punto 8), della direttiva 2009/73/CE del Parlamento europeo e del Consiglio ([5])
		— Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 6), della direttiva 2009/73/CE
		— Gestori del sistema di trasporto quali definiti all'articolo 2, punto 4), della direttiva 2009/73/CE
		— Gestori dell'impianto di stoccaggio quali definiti all'articolo 2, punto 10), della direttiva 2009/73/CE
		— Gestori del sistema GNL quali definiti all'articolo 2, punto 12), della direttiva 2009/73/CE
		— Imprese di gas naturale quali definite all'articolo 2, punto 1), della direttiva 2009/73/CE;
		— Gestori di impianti di raffinazione e trattamento di gas naturale
	e) Idrogeno	— Gestori di impianti di produzione, stoccaggio e trasporto di idrogeno

Settore	Sottosettore	Tipo di soggetto
2. Trasporti	a) Trasporto aereo	— Vettori aerei quali definiti all'articolo 3, punto 4), del regolamento (CE) n. 300/2008 utilizzati a fini commerciali
		— Gestori aeroportuali quali definiti all'articolo 2, punto 2), della direttiva 2009/12/CE del Parlamento europeo e del Consiglio ([6]), aeroporti quali definiti all'articolo 2, punto 1), di tale direttiva, compresi gli aeroporti centrali di cui all'allegato II, sezione 2, del regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio ([7]), e soggetti che gestiscono impianti annessi situati in aeroporti
		— Operatori attivi nel controllo della gestione del traffico che forniscono un servizio di controllo del traffico aereo quali definiti all'articolo 2, punto 1), del regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio ([8])
	b) Trasporto ferroviario	— Gestori dell'infrastruttura quali definiti all'articolo 3, punto 2), della direttiva 2012/34/UE del Parlamento europeo e del Consiglio ([9])
		— Imprese ferroviarie quali definiti all'articolo 3, punto 1), della direttiva 2012/34/UE, compresi gli operatori degli impianti di servizio quali definiti all'articolo 3, punto 12), di tale direttiva
	c) Trasporto per vie d'acqua	— Compagnie di navigazione per il trasporto per vie d'acqua interne, marittimo e costiero di passeggeri e merci quali definite per il trasporto marittimo all'allegato I del regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio ([10]), escluse le singole navi gestite da tale compagnia
		— Organi di gestione dei porti quali definiti all'articolo 3, punto 1), della direttiva 2005/65/CE del Parlamento europeo e del Consiglio ([11]), compresi i relativi impianti portuali quali definiti all'articolo 2, punto 11), del regolamento (CE) n. 725/2004, e soggetti che gestiscono opere e attrezzature all'interno di porti
		— Gestori di servizi di assistenza al traffico marittimo (VTS) quali definiti all'articolo 3, lettera o), della direttiva 2002/59/CE del Parlamento europeo e del Consiglio ([12])
	d) Trasporto su strada	— Autorità stradali quali definite all'articolo 2, punto 12), del regolamento delegato (UE) 2015/962 della Commissione ([13]) responsabili del controllo della gestione del traffico, esclusi i soggetti pubblici per i quali la gestione del traffico o la gestione di sistemi di trasporto intelligenti costituiscono soltanto una parte non essenziale della loro attività generale
		— Gestori di sistemi di trasporto intelligenti quali definiti all'articolo 4, punto 1), della direttiva 2010/40/UE del Parlamento europeo e del Consiglio ([14])
3. Settore bancario		Enti creditizi quali definiti all'articolo 4, punto 1), del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio ([15])
4. Infrastrutture dei mercati finanziari		— Gestori delle sedi di negoziazione quali definiti all'articolo 4, punto 24), della direttiva 2014/65/UE del Parlamento europeo e del Consiglio ([16])
		— Controparti centrali (CCP) quali definite all'articolo 2, punto 1), del regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio ([17])

Settore	Sottosettore	Tipo di soggetto
5. Settore sanitario		— Prestatori di assistenza sanitaria quali definiti all'articolo 3, lettera g), della direttiva 2011/24/UE del Parlamento europeo e del Consiglio ([18])
		— Laboratori di riferimento dell'UE quali definiti all'articolo 15 del regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio ([19])
		— Soggetti che svolgono attività di ricerca e sviluppo relative ai medicinali quali definiti all'articolo 1, punto 2), della direttiva 2001/83/CE del Parlamento europeo e del Consiglio ([20]) — Soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici di cui alla sezione C, divisione 21, della NACE Rev. 2 — Soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica (elenco dei dispositivi critici per l'emergenza di sanità pubblica) di cui all'articolo 22 del regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio ([21])
6. Acqua potabile		Fornitori e distributori di acque destinate al consumo umano, quali definiti all'articolo 2, punto 1, lettera a), della direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio ([22]), ma esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano è una parte non essenziale dell'attività generale di distribuzione di altri prodotti e beni
7. Acque reflue		Imprese che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche o industriali quali definite all'articolo 2, punti da 1), 2) e 3), della direttiva 91/271/CEE del Consiglio ([23]), escluse le imprese per cui la raccolta, lo smaltimento o il trattamento di acque reflue urbane, domestiche o industriali è una parte non essenziale della loro attività generale
8. Infrastrutture digitali		— Fornitori di punti di interscambio internet
		— Fornitori di servizi DNS, esclusi gli operatori dei server dei nomi radice
		— Registri dei nomi di dominio di primo livello (TLD)
		— Fornitori di servizi di cloud computing
		— Fornitori di servizi di data center
		— Fornitori di reti di distribuzione dei contenuti (content delivery network)
		— Fornitori di servizi fiduciari
		— Fornitori di reti pubbliche di comunicazione
		— Fornitori di servizi di comunicazione elettronica accessibili al pubblico
9. Gestione dei servizi TIC (business-to-business)		— Fornitori di servizi gestiti — Fornitori di servizi di sicurezza gestiti

Settore	Sottosettore	Tipo di soggetto
10. Pubblica amministrazione		— Enti della pubblica amministrazione delle amministrazioni centrali quali definiti da uno Stato membro conformemente al diritto nazionale
		— Enti della pubblica amministrazione a livello regionale quali definiti da uno Stato membro conformemente al diritto nazionale
11. Spazio		Operatori di infrastrutture terrestri possedute, gestite e operate dagli Stati membri o da privati, che sostengono la fornitura di servizi spaziali, esclusi i fornitori di reti pubbliche di comunicazione elettronica

([1]) Direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio, del 5 giugno 2019, relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la direttiva 2012/27/UE (GU L 158 del 14.6.2019, pag. 125).
([2]) Regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio, del 5 giugno 2019, sul mercato interno dell'energia elettrica (GU L 158 del 14.6.2019, pag. 54).
([3]) Direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, sulla promozione dell'uso dell'energia da fonti rinnovabili (GU L 328 del 21.12.2018, pag. 82).
([4]) Direttiva 2009/119/CE del Consiglio, del 14 settembre 2009, che stabilisce l'obbligo per gli Stati membri di mantenere un livello minimo di scorte di petrolio greggio e/o di prodotti petroliferi (GU L 265 del 9.10.2009, pag. 9).
([5]) Direttiva 2009/73/CE del Parlamento europeo e del Consiglio, del 13 luglio 2009, relativa a norme comuni per il mercato interno del gas naturale e che abroga la direttiva 2003/55/CE (GU L 211 del 14.8.2009, pag. 94).
([6]) Direttiva 2009/12/CE del Parlamento europeo e del Consiglio, dell'11 marzo 2009, concernente i diritti aeroportuali (GU L 70 del 14.3.2009, pag. 11).
([7]) Regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio, dell'11 dicembre 2013, sugli orientamenti dell'Unione per lo sviluppo della rete transeuropea dei trasporti e che abroga la decisione n. 661/2010/UE (GU L 348 del 20.12.2013, pag. 1).
([8]) Regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che stabilisce i principi generali per l'istituzione del cielo unico europeo («regolamento quadro») (GU L 96 del 31.3.2004, pag. 1).
([9]) Direttiva 2012/34/UE del Parlamento europeo e del Consiglio, del 21 novembre 2012, che istituisce uno spazio ferroviario europeo unico (GU L 343 del 14.12.2012, pag. 32).
([10]) Regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio, del 31 marzo 2004, relativo al miglioramento della sicurezza delle navi e degli impianti portuali (GU L 129 del 29.4.2004, pag. 6).
([11]) Direttiva 2005/65/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa al miglioramento della sicurezza dei porti (GU L 310 del 25.11.2005, pag. 28).
([12]) Direttiva 2002/59/CE del Parlamento europeo e del Consiglio, del 27 giugno 2002, relativa all'istituzione di un sistema comunitario di monitoraggio del traffico navale e d'informazione e che abroga la direttiva 93/75/CEE del Consiglio (GU L 208 del 5.8.2002, pag. 10)
([13]) Regolamento delegato (UE) 2015/962 della Commissione, del 18 dicembre 2014, che integra la direttiva 2010/40/UE del Parlamento europeo e del Consiglio relativamente alla predisposizione in tutto il territorio dell'Unione europea di servizi di informazione sul traffico in tempo reale (GU L 157 del 23.6.2015, pag. 21).
([14]) Direttiva 2010/40/UE del Parlamento europeo e del Consiglio, del 7 luglio 2010, sul quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto (GU L 207 del 6.8.2010, pag. 1).
([15]) Regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e che modifica il regolamento (UE) n. 648/2012 (GU L 176 del 27.6.2013, pag. 1).
([16]) Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE (GU L 173 del 12.6.2014, pag. 349).
([17]) Regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio, del 4 luglio 2012, sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni (GU L 201 del 27.7.2012, pag. 1).
([18]) Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (GU L 88 del 4.4.2011, pag. 45).

([19]) Regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio, del 23 novembre 2022, relativo alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 1082/2013/UE (GU L 314 del 6.12.2022, pag. 26).

([20]) Direttiva 2001/83/CE del Parlamento europeo e del Consiglio, del 6 novembre 2001, recante un codice comunitario relativo ai medicinali per uso umano (GU L 311 del 28.11.2001, pag. 67).

([21]) Regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio del 25 gennaio 2022 relativo a un ruolo rafforzato dell'Agenzia europea per i medicinali nella preparazione alle crisi e nella loro gestione in relazione ai medicinali e ai dispositivi medici (GU L 20 del 31.1.2022, pag. 1).

([22]) Direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio del 16 dicembre 2020 concernente la qualità delle acque destinate al consumo umano (GU L 435 del 23.12.2020, pag. 1).

([23]) Direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, concernente il trattamento delle acque reflue urbane (GU L 135 del 30.5.1991, pag. 40).

ALLEGATO II

ALTRI SETTORI CRITICI

Settore	Sottosettore	Tipo di soggetto
1. Servizi postali e di corriere		Fornitori di servizi postali quali definiti all'articolo 2, punto 1 *bis*), della direttiva 97/67/CE, tra cui i fornitori di servizi di corriere
2. Gestione dei rifiuti		Imprese che si occupano della gestione dei rifiuti quali definite all'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio ([1]), escluse quelle per cui la gestione dei rifiuti non è la principale attività economica
3. Fabbricazione, produzione e distribuzione di sostanze chimiche		Imprese che si occupano della fabbricazione di sostanze e della distribuzione di sostanze o miscele di cui all'articolo 3, punti 9) e 14), del regolamento (CE) n. 1907/2006 del Parlamento europeo e del Consiglio ([2]) e imprese che si occupano della produzione di articoli quali definite all'articolo 3, punto 3), del medesimo regolamento, da sostanze o miscele
4. Produzione, trasformazione e distribuzione di alimenti		Imprese alimentari quali definite all'articolo 3, punto 2), del regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio ([3]) che si occupano della distribuzione all'ingrosso e della produzione industriale e trasformazione
5. Fabbricazione	a) Fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro	Soggetti che fabbricano dispositivi medici quali definiti all'articolo 2, punto 1), del regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio ([4]) e soggetti che fabbricano dispositivi medico-diagnostici in vitro quali definiti all'articolo 2, punto 2), del regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio ([5]) ad eccezione dei soggetti che fabbricano dispositivi medici di cui all'allegato I, punto 5), quinto trattino, della presente direttiva
	b) Fabbricazione di computer e prodotti di elettronica e ottica	Imprese che svolgono attività economiche di cui alla sezione C, divisione 26, della NACE Rev. 2
	c) Fabbricazione di apparecchiature elettriche	Imprese che svolgono attività economiche di cui alla sezione C, divisione 27, della NACE Rev. 2
	d) Fabbricazione di macchinari e apparecchiature n.c.a.	Imprese che svolgono attività economiche di cui alla sezione C, divisione 28, della NACE Rev. 2
	e) Fabbricazione di autoveicoli, rimorchi e semirimorchi	Imprese che svolgono attività economiche di cui alla sezione C, divisione 29, della NACE Rev. 2
	f) Fabbricazione di altri mezzi di trasporto	Imprese che svolgono attività economiche di cui alla sezione C, divisione 30, della NACE Rev. 2

Settore	Sottosettore	Tipo di soggetto
6. Fornitori di servizi digitali		— Fornitori di mercati online
		— Fornitori di motori di ricerca online
		— Fornitori di piattaforme di servizi di social network
7. Ricerca		Organizzazioni di ricerca

([1]) Direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008, relativa ai rifiuti e che abroga alcune direttive (GU L 312 del 22.11.2008, pag. 3).

([2]) Regolamento (CE) n. 1907/2006 del Parlamento europeo e del Consiglio, del 18 dicembre 2006, concernente la registrazione, la valutazione, l'autorizzazione e la restrizione delle sostanze chimiche (REACH), che istituisce un'agenzia europea per le sostanze chimiche, che modifica la direttiva 1999/45/CE e che abroga il regolamento (CEE) n. 793/93 del Consiglio e il regolamento (CE) n. 1488/94 della Commissione, nonché la direttiva 76/769/CEE del Consiglio e le direttive della Commissione 91/155/CEE, 93/67/CEE, 93/105/CE e 2000/21/CE (GU L 396 del 30.12.2006, pag. 1).

([3]) Regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio, del 28 gennaio 2002, che stabilisce i principi e i requisiti generali della legislazione alimentare, istituisce l'Autorità europea per la sicurezza alimentare e fissa procedure nel campo della sicurezza alimentare (GU L 31 dell'1.2.2002, pag. 1).

([4]) Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio (GU L 117 del 5.5.2017, pag. 1).

([5]) Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione (GU L 117 del 5.5.2017, pag. 176).

ALLEGATO III

TAVOLA DI CONCORDANZA

Direttiva (UE) 2016/1148	Presente direttiva
Articolo 1, paragrafo 1	Articolo 1, paragrafo 1
Articolo 1, paragrafo 2	Articolo 1, paragrafo 2
Articolo 1, paragrafo 3	—
Articolo 1, paragrafo 4	Articolo 2, paragrafo 12
Articolo 1, paragrafo 5	Articolo 2, paragrafo 13
Articolo 1, paragrafo 6	Articolo 2, paragrafi 6 e 11
Articolo 1, paragrafo 7	Articolo 4
Articolo 2	Articolo 2, paragrafo 14
Articolo 3	Articolo 5
Articolo 4	Articolo 6
Articolo 5	—
Articolo 6	—
Articolo 7, paragrafo 1	Articolo 7, paragrafi 1 e 2
Articolo 7, paragrafo 2	Articolo 7, paragrafo 4
Articolo 7, paragrafo 3	Articolo 7, paragrafo 3
Articolo 8, paragrafi da 1 a 5	Articolo 8, paragrafi da 1 a 5
Articolo 8, paragrafo 6	Articolo 13, paragrafo 4
Articolo 8, paragrafo 7	Articolo 8, paragrafo 6
Articolo 9, paragrafi 1, 2 e 3	Articolo 10, paragrafi 1, 2 e 3
Articolo 9, paragrafo 4	Articolo 10, paragrafo 9
Articolo 9, paragrafo 5	Articolo 10, paragrafo 10
Articolo 10, paragrafi 1, 2 e 3, primo comma	Articolo 13, paragrafi 1, 2 e 3
Articolo 10, paragrafo 3, secondo comma	Articolo 23, paragrafo 9
Articolo 11, paragrafo 1	Articolo 14, paragrafi 1 e 2
Articolo 11, paragrafo 2	Articolo 14, paragrafo 3
Articolo 11, paragrafo 3	Articolo 14, paragrafo 4, primo comma, lettere da a) a q) e s), e paragrafo 7
Articolo 11, paragrafo 4	Articolo 14, paragrafo 4, primo comma, lettera r), e secondo comma
Articolo 11, paragrafo 5	Articolo 14, paragrafo 8
Articolo 12, paragrafi da 1 a 5	Articolo 15, paragrafi da 1 a 5
Articolo 13	Articolo 17
Articolo 14, paragrafi 1 e 2	Articolo 21, paragrafi da 1 a 4
Articolo 14, paragrafo 3	Articolo 23, paragrafo 1
Articolo 14, paragrafo 4	Articolo 23, paragrafo 3
Articolo 14, paragrafo 5	Articolo 23, paragrafi 5, 6 e 8

Direttiva (UE) 2016/1148	Presente direttiva
Articolo 14, paragrafo 6	Articolo 23, paragrafo 7
Articolo 14, paragrafo 7	Articolo 23, paragrafo 11
Articolo 15, paragrafo 1	Articolo 31, paragrafo 1
Articolo 15, paragrafo 2, primo comma, lettera a)	Articolo 32, paragrafo 2, lettera e)
Articolo 15, paragrafo 2, primo comma, lettera b)	Articolo 32, paragrafo 2, lettera g)
articolo 15, paragrafo 2, secondo comma	Articolo 32, paragrafo 3
Articolo 15, paragrafo 3	Articolo 32, paragrafo 4, lettera b)
Articolo 15, paragrafo 4	Articolo 31, paragrafo 3
Articolo 16, paragrafi 1 e 2	Articolo 21, paragrafi da 1 e 4
Articolo 16, paragrafo 3	Articolo 23, paragrafo 1
Articolo 16, paragrafo 4	Articolo 23, paragrafo 3
Articolo 16, paragrafo 5	—
Articolo 16, paragrafo 6	Articolo 23, paragrafo 6
Articolo 16, paragrafo 7	Articolo 23, paragrafo 7
Articolo 16, paragrafi 8 e 9	Articolo 21, paragrafo 5, e articolo 23, paragrafo 11
Articolo 16, paragrafo 10	—
Articolo 16, paragrafo 11	Articolo 2, paragrafi 1, 2 e 3
Articolo 17, paragrafo 1	-Articolo 33, paragrafo 1
Articolo 17, paragrafo 2, lettera a)	Articolo 32, paragrafo 2, lettera e)
Articolo 17, paragrafo 2, lettera b)	Articolo 32, paragrafo 4, lettera b)
Articolo 17, paragrafo 3	Articolo 37, paragrafo 1, lettere a) e b)
Articolo 18, paragrafo 1	Articolo 26, paragrafo 1, lettera b), e paragrafo 2
Articolo 18, paragrafo 2	Articolo 26, paragrafo 3
Articolo 18, paragrafo 3	Articolo 26, paragrafo 4
Articolo 19	Articolo 25
Articolo 20	Articolo 30
Articolo 21	Articolo 36
Articolo 22	Articolo 39
Articolo 23	Articolo 40
Articolo 24	—
Articolo 25	Articolo 41
Articolo 26	Articolo 45
Articolo 27	Articolo 46
Allegato I, punto 1	Articolo 11, paragrafo 1
Allegato I, punto 2, lettera a), punti da i) a iv)	Articolo 11, paragrafo 2, lettere da a) a d)

Direttiva (UE) 2016/1148	Presente direttiva
Allegato I, punto 2, lettera a), punto v)	Articolo 11, paragrafo 2, lettera f)
Allegato I, punto 2, lettera b)	Articolo 11, paragrafo 4
Allegato I, punto 2, lettera c), punti i) e ii)	Articolo 11, paragrafo 5, lettera a)
Allegato II	Allegato I
Allegato III, punti 1 e 2	Allegato II, punto 6
Allegato III, punto 3	Allegato I, punto 8