

Bruxelles, 22 gennaio 2026
(OR. en)

5627/26

**Fascicolo interistituzionale:
2026/0012 (COD)**

**CYBER 30
JAI 91
DATAPROTECT 23
TELECOM 30
MI 59
IND 50
CADREFIN 27
FIN 104
BUDGET 4
CODEC 93**

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	21 gennaio 2026
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2026) 13 final
Oggetto:	Proposta di DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO che modifica la direttiva (UE) 2022/2555 per quanto riguarda le misure di semplificazione e l'allineamento alla [proposta di regolamento sulla cibersicurezza 2]

Si trasmette in allegato, per le delegazioni, il documento COM(2026) 13 final.

All.: COM(2026) 13 final



COMMISSIONE
EUROPEA

Strasburgo, 20.1.2026
COM(2026) 13 final

2026/0012 (COD)

Proposta di

DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

**che modifica la direttiva (UE) 2022/2555 per quanto riguarda le misure di
semplificazione e l'allineamento alla [proposta di regolamento sulla cibersecurity 2]**

{SWD(2026) 11-12} - {SEC(2026) 11}

(Testo rilevante ai fini del SEE)

RELAZIONE

1. CONTESTO DELLA PROPOSTA

• **Motivi e obiettivi della proposta**

La presente proposta fa parte di un pacchetto di misure che mira ad allineare il quadro dell'Unione in materia di cibersicurezza alle esigenze dei portatori di interessi in un contesto di minacce informatiche sempre più sofisticate e in una realtà geopolitica complessa. I soggetti essenziali e importanti dei settori critici sono sempre più spesso bersaglio di attacchi informatici¹, mentre gli autori delle minacce statali sfruttano le tecnologie emergenti come l'intelligenza artificiale (IA) per espandere ulteriormente e ottimizzare i loro attacchi. In tale contesto, la resilienza delle infrastrutture critiche di fronte alle minacce informatiche è riconosciuta come un pilastro strategico delle nostre democrazie e della sicurezza economica dell'Unione. Sia la strategia europea per l'Unione della preparazione² che la strategia europea di sicurezza interna (ProtectEU)³ hanno messo la cibersicurezza al centro dell'agenda dell'Unione per la resilienza. Analogamente nella comunicazione "Rafforzare la sicurezza economica dell'UE"⁴ la necessità di impedire l'accesso a informazioni e dati sensibili che potrebbero compromettere la sicurezza economica dell'Unione e di prevenire e attenuare le perturbazioni delle infrastrutture critiche dell'Unione che incidono sulla sua economia figurano come obiettivi prioritari, per i quali sono essenziali misure di cibersicurezza efficaci. La relazione Draghi ha inoltre evidenziato la necessità di aumentare la sicurezza e ridurre le dipendenze come una delle principali aree di intervento necessarie nell'Unione⁵. Nella sua comunicazione "Un'Europa più semplice e più rapida"⁶, la Commissione ha annunciato il proprio impegno a favore di un programma ambizioso volto a promuovere politiche innovative e orientate al futuro che rafforzino la competitività dell'Unione e riducano l'onere normativo che grava sui cittadini, sulle imprese e sulle amministrazioni, mantenendo nel contempo gli standard più elevati nella promozione dei suoi valori.

In tale contesto, la presente proposta di direttiva che modifica la direttiva (UE) 2022/2555 per quanto riguarda le misure di semplificazione e l'allineamento alla [proposta di regolamento del Parlamento europeo e del Consiglio relativo all'Agenzia dell'Unione europea per la cibersicurezza (ENISA), al quadro europeo di certificazione della cibersicurezza e alla sicurezza delle catene di approvvigionamento delle TIC e che abroga il regolamento (UE) 2019/881 ("regolamento sulla cibersicurezza 2")] mira ad affrontare il problema della complessità e della diversità delle politiche in materia di cibersicurezza che incidono sulla postura di cibersicurezza dell'Unione, in particolare introducendo chiarimenti e semplificando la conformità alle norme per i soggetti regolamentati.

L'obiettivo della presente direttiva dovrebbe essere considerato parte degli obiettivi generali del pacchetto di revisione del regolamento sulla cibersicurezza che comprende la proposta di regolamento del Parlamento europeo e del Consiglio relativo all'Agenzia dell'Unione europea per la cibersicurezza (ENISA), al quadro europeo di certificazione della cibersicurezza e alla

¹ ENISA, *ENISA Threat Landscape 2025*.

² JOIN(2025) 130 final.

³ COM(2025) 148 final.

⁴ JOIN(2025) 977 final.

⁵ Commissione europea, *The future of European Competitiveness*, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-fl52a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.

⁶ COM(2025) 47 final.

sicurezza della catena di approvvigionamento delle TIC e che abroga il regolamento (UE) 2019/881. Tale proposta di regolamento mira ad affrontare: i) il disallineamento tra il quadro strategico dell'Unione in materia di cibersicurezza e le esigenze dei portatori di interessi in un panorama di minacce sempre più ostili; ii) lo stallo nell'attuazione del quadro europeo di certificazione della cibersicurezza (ECCF); iii) la complessità e la diversità delle politiche in materia di cibersicurezza che incidono sulla postura di cibersicurezza dell'Unione; e iv) l'aumento dei rischi per la sicurezza delle catene di approvvigionamento delle TIC. Per quanto riguarda la complessità e la diversità delle politiche in materia di cibersicurezza che incidono sulla postura di cibersicurezza dell'Unione, il pacchetto di revisione del regolamento sulla cibersicurezza propone, nell'ambito di una riforma del quadro europeo di certificazione della cibersicurezza, di promuovere la certificazione come strumento di conformità per le imprese e di consentire lo sviluppo di un sistema sulla postura di cibersicurezza dei soggetti al fine di ridurre i costi di conformità per i soggetti interessati dalla direttiva NIS 2 e da altre normative pertinenti dell'Unione in materia di cibersicurezza. Questo approccio semplificherà notevolmente gli obblighi normativi per i soggetti che devono rispettare molteplici requisiti di conformità e garantirà un uso più efficace delle risorse tra le autorità nazionali.

La relazione della proposta di regolamento sulla cibersicurezza 2 delinea i problemi chiave alla base della proposta, nonché gli obiettivi specifici per affrontarli. La proposta di direttiva affronterà l'obiettivo specifico 4 (SPO4) della valutazione d'impatto della revisione del regolamento sulla cibersicurezza, vale a dire stabilire meccanismi e condizioni per contribuire a semplificare la conformità ai requisiti in materia di cibersicurezza e, in tal modo, rendere la loro attuazione più coerente ed efficace. Le modifiche mirate della direttiva NIS 2 sono volte a semplificare la conformità e a garantire un'attuazione razionalizzata e coerente di aspetti specifici del quadro in materia di cibersicurezza, anche per quanto riguarda l'ambito di applicazione, le definizioni, la segnalazione di ransomware e la vigilanza dei soggetti che forniscono servizi transfrontalieri.

La proposta di direttiva che modifica la direttiva (UE) 2022/2555 per quanto riguarda le misure di semplificazione e l'allineamento al [regolamento sulla cibersicurezza 2] rientra nell'ambito del programma di controllo dell'adeguatezza e dell'efficacia della regolamentazione (REFIT). Insieme alla revisione del regolamento sulla cibersicurezza, contribuisce in modo significativo a migliorare la chiarezza, eliminare le inefficienze e allineare le procedure tra i quadri giuridici. Contribuisce inoltre al corretto funzionamento del mercato interno, garantendo nel contempo la sicurezza e l'autonomia strategica dell'Unione.

- **Coerenza con le disposizioni vigenti nel settore normativo interessato**

L'Unione ha ampliato i suoi strumenti giuridici e strategici con l'adozione di una serie di strumenti giuridici e misure strategiche: i) la direttiva NIS 2, che rafforza la cibersicurezza delle infrastrutture critiche; ii) le misure di sicurezza fisica definite nella sua "direttiva sorella", la direttiva sulla resilienza dei soggetti critici; iii) il regolamento sulla ciberresilienza, che rafforza la cibersicurezza dei prodotti; iv) il regolamento sulla cibersolidarietà, che crea capacità di risposta a livello dell'UE; v) il programma dell'UE per la cibersicurezza⁷, che sostiene la cooperazione a livello dell'UE in materia di gestione delle crisi; vi) il pacchetto di strumenti per la cibersicurezza del 5G, che sostiene la cibersicurezza delle reti 5G; vii) il piano d'azione europeo sulla cibersicurezza degli ospedali e dei prestatori di assistenza sanitaria⁸, che contribuisce a migliorare la loro cibersicurezza; e viii) l'Accademia per le

⁷ COM(2025) 66 final.

⁸ COM(2025) 10 final.

competenze in materia di cibersicurezza⁹, che affronta la crescente sfida del divario di talenti nel settore della cibersicurezza.

Il suddetto quadro giuridico in materia di cibersicurezza è stato integrato da una legislazione settoriale, vale a dire il regolamento sulla resilienza operativa digitale (regolamento DORA) per il settore finanziario, il codice di rete relativo a disposizioni settoriali per gli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica per il sottosettore dell'energia elettrica e le norme sulla sicurezza delle informazioni (parte IS¹⁰) per il sottosettore del trasporto aereo.

La presente proposta di direttiva, analogamente alla proposta di regolamento che accompagna, fa parte di una serie più ampia di iniziative giuridiche e strategiche adottate dall'Unione per migliorare la resilienza dei soggetti contro le minacce informatiche e alla sicurezza. Si concentra su modifiche mirate della direttiva NIS 2 che mirano, tra l'altro, a chiarire alcuni aspetti relativi all'ambito di applicazione, alle definizioni e alle norme giurisdizionali, a ridurre l'onere di vigilanza dei soggetti essenziali e importanti e a facilitare la vigilanza dei soggetti transfrontalieri rafforzando il ruolo dell'ENISA nel sostegno alla cooperazione operativa. Inoltre, insieme alla proposta di regolamento, la presente proposta dà luogo a una forte sinergia derivante dallo sviluppo della certificazione della postura di cibersicurezza per la direttiva NIS 2 e potenzialmente anche per semplificare la conformità ad altri atti giuridici pertinenti dell'Unione, quale il regolamento generale sulla protezione dei dati (GDPR), fatti salvi i loro requisiti specifici di certificazione. Tali misure di semplificazione dovrebbero sbloccare risorse per rafforzare la preparazione operativa in materia di cibersicurezza dei soggetti nei settori critici dell'Unione.

- **Coerenza con le altre normative dell'Unione**

La presente proposta rafforza i requisiti di sicurezza per i soggetti che forniscono i portafogli delle imprese di cui alla proposta di regolamento del Parlamento europeo e del Consiglio sull'istituzione dei portafogli europei delle imprese¹¹. La Commissione garantirà inoltre la coerenza con le prossime iniziative, come il regolamento sulle reti digitali. La presente proposta è in linea con la proposta di regolamento sulla semplificazione della legislazione digitale (omnibus digitale), che comprende, tra l'altro, modifiche della direttiva NIS 2 come pure di altri atti giuridici dell'Unione. L'omnibus digitale propone di agevolare il rispetto degli obblighi di segnalazione in materia di cibersicurezza, a norma tra l'altro della direttiva NIS 2, segnalando gli incidenti tramite un punto di accesso unico che sarà sviluppato e gestito dall'ENISA. La presente proposta è inoltre in linea con la proposta di regolamento del Parlamento europeo e del Consiglio sulla sicurezza, la resilienza e la sostenibilità delle attività spaziali nell'Unione¹².

La proposta è inoltre in linea con la relazione sul futuro della competitività europea di Mario Draghi, come sottolineato in precedenza.

⁹ COM(2023) 207 final.

¹⁰ Regolamento di esecuzione (UE) 2023/203 della Commissione e regolamento delegato (UE) 2022/1645 della Commissione.

¹¹ COM(2025) 838 final.

¹² COM(2025) 335 final.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

- **Base giuridica**

La base giuridica della presente direttiva è l'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE), il cui obiettivo è instaurare e garantire il funzionamento del mercato interno mediante il rafforzamento delle misure relative al ravvicinamento delle normative nazionali. La presente proposta modifica la direttiva (UE) 2022/2555, adottata a norma dell'articolo 114 TFUE.

- **Sussidiarietà (per la competenza non esclusiva)**

Il principio di sussidiarietà impone di valutare la necessità e il valore aggiunto dell'azione dell'Unione. Il rispetto del principio di sussidiarietà in questo settore era già stato riconosciuto al momento dell'adozione della direttiva (UE) 2022/2555, che è modificata dalla presente proposta.

La presente proposta semplifica la conformità alla legislazione dell'Unione in materia di cibersecurity, riducendo i costi di conformità e l'incertezza giuridica per i soggetti interessati e agevolando e migliorando il tasso di conformità ai requisiti in materia di cibersecurity. Contribuisce inoltre a creare condizioni di parità negli approcci alla vigilanza e ai controlli di conformità in tutti gli Stati membri.

- **Proporzionalità**

Le norme proposte nella presente direttiva non vanno al di là di quanto necessario per conseguire in modo soddisfacente gli obiettivi specifici. L'allineamento e la razionalizzazione dell'ambito di applicazione, delle misure di sicurezza e degli obblighi di segnalazione previsti sono relativi alle richieste degli Stati membri e delle imprese di migliorare il quadro attuale.

- **Scelta dell'atto giuridico**

La proposta modificherà l'attuale direttiva NIS 2 e razionalizzerà ulteriormente gli obblighi imposti alle imprese, garantendo pertanto un livello più elevato di armonizzazione in tutta l'Unione. La scelta dello strumento giuridico per la presente proposta è coerente con il testo giuridico che modifica, ossia la direttiva NIS 2. La presente proposta si basa sull'obiettivo della direttiva NIS 2 di offrire agli Stati membri la flessibilità necessaria per tenere conto delle specificità nazionali.

3. RISULTATI DELLE VALUTAZIONI EX POST, DELLE CONSULTAZIONI DEI PORTATORI DI INTERESSI E DELLE VALUTAZIONI D'IMPATTO

- **Valutazioni ex post / Vaglio di adeguatezza della legislazione vigente**

Cfr. la relazione della [proposta di regolamento sulla cibersecurity 2].

- **Consultazioni dei portatori di interessi**

Cfr. la relazione della [proposta di regolamento sulla cibersecurity 2].

- **Assunzione e uso di perizie**

Cfr. la relazione della [proposta di regolamento sulla cibersecurity 2].

- **Valutazione d'impatto**

Cfr. la relazione e la relazione sulla valutazione d'impatto che accompagnano la [proposta di regolamento sulla cibersecurity 2].

- **Efficienza normativa e semplificazione**

Cfr. la relazione della [proposta di regolamento sulla cibersicurezza 2].

- **Diritti fondamentali**

Cfr. la relazione della [proposta di regolamento sulla cibersicurezza 2].

4. INCIDENZA SUL BILANCIO

Cfr. la scheda legislativa e finanziaria della [proposta di regolamento sulla cibersicurezza 2].

5. ALTRI ELEMENTI

- **Piani attuativi e modalità di monitoraggio, valutazione e informazione**

A norma dell'articolo 40 della direttiva NIS 2, ogni 36 mesi la Commissione riesaminerà il funzionamento della direttiva e presenterà una relazione in proposito al Parlamento europeo e al Consiglio.

- **Illustrazione dettagliata delle singole disposizioni della proposta**

La proposta mira a semplificare il rispetto degli obblighi di cibersicurezza e a sbloccare risorse per rafforzare la preparazione operativa in materia di cibersicurezza dei soggetti nei settori critici dell'Unione.

La proposta introduce modifiche mirate della direttiva NIS 2 per semplificare aspetti specifici del quadro in materia di cibersicurezza, aumentare la certezza del diritto e armonizzarne l'attuazione.

Affinché per i soggetti e i fornitori sia più facile dimostrare la conformità alla direttiva NIS 2, in linea con la proposta di regolamento che accompagna la presente proposta, i soggetti regolamentati dalla direttiva NIS 2 potranno ottenere certificati nell'ambito dei sistemi organizzativi di certificazione della cibersicurezza sviluppati nell'ambito dell'ECCF.

Per semplificare ulteriormente la conformità alle misure di gestione dei rischi di cibersicurezza da parte dei soggetti multinazionali oggetto della vigilanza delle autorità competenti di diversi Stati membri, all'ENISA è affidato un nuovo ruolo di sostegno agli Stati membri nella vigilanza di tali soggetti, facilitando l'assistenza reciproca e creando una migliore panoramica dei soggetti che rientrano nell'ambito di applicazione della direttiva NIS 2.

La proposta prevede inoltre che la Commissione adotti orientamenti sull'applicazione dei requisiti in materia di sicurezza della catena di approvvigionamento che i soggetti che rientrano nell'ambito di applicazione della direttiva NIS 2 trasmettono ai loro fornitori, al fine di garantire la certezza del diritto ed evitare l'indebita trasmissione degli obblighi a soggetti che non rientrano nell'ambito di applicazione della direttiva NIS 2.

Altre modifiche mirate della direttiva NIS 2 comprendono:

- il chiarimento dell'ambito di applicazione e delle definizioni;
- l'esclusione dei fornitori di servizi DNS di piccole e micro dimensioni dall'ambito di applicazione;
- l'introduzione della massima armonizzazione per gli atti di esecuzione a norma dell'articolo 21, paragrafo 5 (che specifica le misure di gestione dei rischi di

cibersicurezza) al fine di agevolare la conformità per i soggetti e la vigilanza per le autorità;

- l'introduzione di una nuova categoria di piccole imprese a media capitalizzazione, in linea con la raccomandazione della Commissione del 2025 relativa alla definizione delle piccole imprese a media capitalizzazione¹⁸; i soggetti che si qualificano come piccole imprese a media capitalizzazione devono essere designati come soggetti importanti, riducendo il loro onere di conformità e l'onere di vigilanza per le autorità competenti;
- l'obbligo per gli Stati membri di adottare politiche per la migrazione verso la crittografia post-quantum (PQC) nell'ambito della rispettiva strategia nazionale in materia di cibersicurezza; nonché
- l'introduzione di una raccolta armonizzata di dati sugli attacchi ransomware.

Proposta di

DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

che modifica la direttiva (UE) 2022/2555 per quanto riguarda le misure di semplificazione e l'allineamento alla [proposta di regolamento sulla cibersecurity 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 del Comitato economico e sociale europeo¹,
visto il parere del Comitato delle regioni²,
deliberando secondo la procedura legislativa ordinaria,
considerando quanto segue:

- (1) La direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio³ stabilisce misure volte a garantire un livello comune elevato di cibersecurity nell'Unione in modo da migliorare il funzionamento del mercato interno. Dall'entrata in vigore della direttiva (UE) 2022/2555 sono stati compiuti progressi nell'aumentare il livello di ciberresilienza dell'Unione. Durante l'attuazione da parte degli Stati membri sono nel contempo emerse alcune sfide, anche in relazione all'ambito di applicazione della direttiva, all'attuazione degli obblighi di gestione dei rischi e di segnalazione degli incidenti di cibersecurity e alla vigilanza dei soggetti transfrontalieri. Sulla base della [proposta di regolamento sulla cibersecurity 2], è opportuno apportare modifiche mirate alla direttiva (UE) 2022/2555 per far fronte a tali sfide, semplificando aspetti specifici al fine di aumentare la certezza del diritto e garantire un'attuazione uniforme della direttiva (UE) 2022/2555.
- (2) Al fine di ridurre l'onere di conformità per i soggetti e l'onere di vigilanza per le autorità competenti, è opportuno introdurre nella direttiva (UE) 2022/2555 una nuova categoria di piccole imprese a media capitalizzazione, in linea con la raccomandazione (UE) 2025/1099 della Commissione⁴. I soggetti delle tipologie di cui all'allegato I

¹ GU C, [...], [...], ELI: [...].

² GU C, [...], [...], ELI: [...].

³ Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersecurity nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>).

⁴ Raccomandazione (UE) 2025/1099 della Commissione, del 21 maggio 2025, relativa alla definizione delle piccole imprese a media capitalizzazione (GU L, 2025/1099, 28.5.2025, ELI: <http://data.europa.eu/eli/reco/2025/1099/oj>).

della direttiva (UE) 2022/2555 che si qualificano come piccole imprese a media capitalizzazione ai sensi di tale raccomandazione dovrebbero di norma essere designati come soggetti importanti. Inoltre, al fine di sostenere l'obiettivo della Commissione di ridurre i costi amministrativi del 25 % nel complesso e del 35 % per le piccole e medie imprese, ai fornitori di servizi di sistema dei nomi di dominio dovrebbe essere applicata la regola generale della soglia di dimensione di cui alla direttiva (UE) 2022/2555, in base alla quale tutti i soggetti che si considerano medie imprese ai sensi dell'articolo 2 dell'allegato della raccomandazione 2003/361/CE della Commissione⁵, o che superano i massimali per le medie imprese di cui al paragrafo 1 di tale articolo, rientrano nell'ambito di applicazione della direttiva (UE) 2022/2555.

- (3) Durante l'attuazione della direttiva (UE) 2022/2555 sono state riscontrate difficoltà nell'interpretazione delle disposizioni relative al suo ambito di applicazione. È pertanto opportuno chiarire alcune disposizioni relative all'ambito di applicazione riguardanti i prestatori di assistenza sanitaria, i produttori di energia elettrica, le imprese di idrogeno e i soggetti del settore chimico, al fine di garantire la certezza del diritto e ridurre l'onere di conformità sia per i soggetti che per le autorità nazionali.
- (4) Al fine di garantire la proporzionalità per quanto riguarda i produttori di energia elettrica ai sensi dell'articolo 2, punto 38), della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio⁶, solo i produttori di energia elettrica con una capacità di generazione totale superiore a 1 MW dovrebbero essere considerati soggetti essenziali o importanti ai sensi della direttiva (UE) 2022/2555, a condizione che rispettino la regola della soglia di dimensione. Ciò dovrebbe comprendere i produttori di energia elettrica in cui un singolo impianto di produzione di energia elettrica supera 1 MW, nonché i produttori di energia elettrica che gestiscono diversi impianti di produzione che insieme hanno una capacità di produzione superiore a 1 MW. Tale approccio consente di trovare un equilibrio tra la necessità di individuare i soggetti in cui l'interferenza con il loro sistema informativo e di rete potrebbe comportare una perdita, una non controllabilità o un controllo esterno della capacità di generazione che è di per sé rilevante per la sicurezza e la stabilità della rete elettrica e la necessità di non imporre un onere amministrativo sproporzionato alle imprese a norma della direttiva (UE) 2022/2555.
- (5) I portafogli europei di identità digitale di cui al regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio⁷ sono una componente essenziale dell'infrastruttura digitale dell'Unione, che consente l'identificazione e l'autenticazione sicure e lo scambio di documenti elettronici, compresi gli attestati elettronici di attributi. Dato il loro ruolo cruciale per il pubblico e per la fornitura di servizi pubblici e privati, qualsiasi incidente di cibersicurezza che colpisca tali portafogli potrebbe avere un ampio impatto. Per garantire la fornitura dei loro servizi, i fornitori di portafogli europei di identità digitale dovrebbero essere tenuti ad attuare misure

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, ELI: <http://data.europa.eu/eli/reco/2003/361/oj>).

⁶ 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, ELI: <http://data.europa.eu/eli/dir/2019/944/oj>).

⁷ 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, ELI: <http://data.europa.eu/eli/reg/2014/910/oj>).

tecniche, operative e organizzative adeguate per gestire i rischi di cibersicurezza, prevenire gli incidenti e rispondervi e cooperare con le autorità competenti conformemente alla direttiva (UE) 2022/2555. Essi dovrebbero pertanto essere inclusi tra i soggetti contemplati da tale direttiva indipendentemente dalle loro dimensioni ed essere classificati come soggetti essenziali. I portafogli europei delle imprese offrono funzionalità e servizi simili adattati alle esigenze degli operatori economici e degli organismi del settore pubblico, sulla base del quadro UE relativo a un'identità digitale, e sono altrettanto fondamentali per la sicurezza e l'integrità dell'economia digitale. Di conseguenza, i fornitori di portafogli europei delle imprese istituiti a norma della [proposta di regolamento sull'istituzione dei portafogli europei delle imprese]⁸ dovrebbero essere soggetti agli stessi requisiti e obblighi in materia di cibersicurezza dei fornitori di portafogli europei di identità digitale, al fine di garantire un livello coerente ed elevato di sicurezza in tutto l'ecosistema dell'identità digitale.

- (6) Le infrastrutture sottomarine di trasmissione dei dati includono non solo i cavi, ma anche qualsiasi infrastruttura connessa al loro funzionamento. Tali infrastrutture comprendono le stazioni di approdo e le parti terrestri del cavo sottomarino a esse collegate, come le rotte terrestri da pozzetti in spiaggia a stazioni di approdo, centri dati o punti di presenza. Le infrastrutture sottomarine di trasmissione dei dati sono solitamente gestite da soggetti già contemplati dalla direttiva (UE) 2022/2555, compresi i fornitori di reti e servizi pubblici di comunicazione elettronica o i fornitori di servizi di cloud computing. Le infrastrutture sottomarine di trasmissione dei dati possono tuttavia essere gestite anche da altri tipi di soggetti che attualmente non rientrano nell'ambito di applicazione della direttiva (UE) 2022/2555, come le infrastrutture sottomarine di trasmissione dei dati gestite da fornitori di reti di comunicazione elettronica che non sono pubbliche o da soggetti che affidano in locazione la gestione dell'infrastruttura sottomarina di trasmissione dei dati, in tutto o in parte, a fornitori di reti pubbliche di comunicazione elettronica. In considerazione dei crescenti rischi per l'infrastruttura sottomarina di trasmissione dei dati e dell'alta criticità che ne deriva, è necessario garantire che tutti i tipi di gestori di infrastrutture sottomarine di trasmissione dei dati siano disciplinati dalla direttiva (UE) 2022/2555. Altre infrastrutture marittime critiche, come i cavi elettrici sottomarini e i gasdotti, le condotte per l'idrogeno e gli oleodotti, sono in genere già disciplinate dalla direttiva (UE) 2022/2555 in quanto gestite dai gestori dei sistemi di trasmissione nei sottosettori dell'energia elettrica, del gas, dell'idrogeno e del petrolio.
- (7) Al fine di consentire ai soggetti che forniscono servizi in diversi Stati membri di beneficiare di approcci di vigilanza più coerenti e meno onerosi in tutto il mercato interno, tali soggetti dovrebbero essere in grado di dimostrare la conformità a obblighi specifici o a tutti gli obblighi di gestione dei rischi di cibersicurezza di cui alla direttiva (UE) 2022/2555 ottenendo un certificato sulla postura di cibersicurezza nell'ambito di un sistema europeo di certificazione della cibersicurezza. Lo sviluppo di tale sistema beneficerà dell'adozione di atti di esecuzione sui requisiti tecnici, metodologici e settoriali relativi alle misure di gestione dei rischi di cibersicurezza a norma della direttiva (UE) 2022/2555 che si basano sulla massima armonizzazione.
- (8) Poiché la nostra società e la nostra economia dipendono sempre di più dalle tecnologie digitali, è necessario adottare misure di mitigazione contro la minaccia quantistica. La possibilità di attacchi "*harvest now, decrypt later*" (intercettare i dati ora per deccriptarli

⁸ COM(2025) 838 final.

in futuro), che probabilmente si stanno già verificando, e i rischi futuri indotti dagli attacchi quantistici relativi alla falsificazione delle firme, la deprecazione pianificata di alcune implementazioni di algoritmi e la totale eliminazione degli attuali algoritmi crittografici a chiave pubblica, aumentano l'urgenza di avviare azioni per la migrazione alla crittografia post-quantum (PQC). Gli Stati membri dovrebbero pertanto essere tenuti ad adottare politiche per la migrazione verso la PQC nell'ambito della rispettiva strategia nazionale in materia di cibersicurezza. Tali politiche dovrebbero agevolare l'accelerazione della pianificazione strategica e la creazione di misure e strumenti di sostegno per valutare l'esposizione delle risorse crittografiche ai rischi posti dai computer quantistici. Dovrebbero inoltre contribuire alla creazione di un piano di migrazione e alla sperimentazione dell'introduzione della PQC nelle applicazioni e nelle reti digitali, promuovendo nel contempo lo sviluppo e l'adozione di soluzioni europee di PQC formalmente verificate e valutate che aderiscono ai quadri di conformità per i prodotti e i servizi. Tali politiche dovrebbero essere in linea con le tappe stabilite negli atti giuridici e nelle politiche dell'Unione, nonché con i documenti adottati dal gruppo di cooperazione NIS, in particolare la tabella di marcia per l'attuazione coordinata della transizione verso la PQC, adottata dal gruppo di cooperazione NIS nel giugno 2025, conseguendo in tal modo la migrazione verso la PQC entro il 2030 per i casi d'uso critici ed entro il 2035 per i casi d'uso di livello medio e basso.

- (9) A norma dell'articolo 21, paragrafo 2, lettera d), della direttiva (UE) 2022/2555, i soggetti essenziali e importanti devono garantire un livello adeguato di sicurezza della loro catena di approvvigionamento. Nella pratica tale obbligo ha indotto molti soggetti a richiedere ai loro fornitori informazioni approfondite tramite questionari, formati e processi eterogenei. Sebbene mirino a sostenere la dovuta diligenza e la gestione dei rischi, tali richieste possono anche creare un onere amministrativo significativo per i fornitori di soggetti essenziali e importanti, in particolare quando informazioni simili devono essere fornite ripetutamente in forme diverse. Per rendere tale onere meno gravoso e promuovere un approccio coerente, proporzionato ed efficiente alle valutazioni della sicurezza della catena di approvvigionamento, la Commissione dovrebbe elaborare orientamenti per raccomandare un livello adeguato di dettaglio, una struttura e un formato per tali richieste di informazioni. Tali orientamenti dovrebbero facilitare l'armonizzazione, ridurre inutili duplicazioni e sostenere sia i soggetti che i loro fornitori nell'adempimento efficace dei loro obblighi a norma della direttiva (UE) 2022/2555.
- (10) Gli attacchi ransomware in cui i malware criptano dati e sistemi e chiedono il pagamento di un riscatto per il rilascio rimangono una delle principali minacce per i soggetti essenziali e importanti. L'armonizzazione e il miglioramento della raccolta di dati sugli attacchi ransomware da soggetti essenziali e importanti colpiti fornirebbero informazioni ai team di risposta agli incidenti di sicurezza informatica (CSIRT) e alle autorità nazionali, consentendo loro di garantire che i futuri interventi di prevenzione dei ransomware siano adeguati ed efficaci, di aiutare i soggetti ad aumentare la loro resilienza e a prevenire attacchi futuri e di raccogliere intelligence e prove di cui le autorità di contrasto hanno bisogno per fermare e smantellare le bande criminali che si servono dei ransomware e sanzionare i loro membri. Data la natura potenzialmente sensibile delle informazioni da condividere in merito agli attacchi ransomware, in particolare se un soggetto ha pagato un riscatto e, in caso affermativo, quale importo e a chi, tali informazioni dovrebbero essere trasmesse solo ai CSIRT o, se del caso, alle autorità competenti su loro richiesta. Ai fini di tale scambio di informazioni, i soggetti essenziali e importanti sono incoraggiati a nominare una persona che funga da punto

di contatto e garantisca la riservatezza e l'affidabilità dello scambio di informazioni. Nel contesto dell'iniziativa internazionale "Counter Ransomware", l'Unione ha approvato una dichiarazione politica internazionale non vincolante in base alla quale le istituzioni competenti sotto l'autorità dei governi nazionali partecipanti non dovrebbero pagare richieste di estorsione di ransomware.

- (11) Il rispetto degli obblighi di segnalazione delle informazioni pertinenti sugli incidenti ransomware non dovrebbe comportare l'imposizione di obblighi aggiuntivi ai sensi della direttiva (UE) 2022/2555 a cui il soggetto non sarebbe stato soggetto se non avesse segnalato le informazioni. A tal fine, entro i limiti dei rispettivi ordinamenti giuridici nazionali, gli Stati membri dovrebbero far fronte ai possibili rischi derivanti da una maggiore responsabilità legata alla segnalazione di informazioni pertinenti sugli incidenti ransomware.
- (12) Data la dimensione transfrontaliera di molti soggetti essenziali e importanti in tutto il mercato interno e la necessità di garantire la coerenza e promuovere la convergenza e l'efficienza in relazione agli approcci di vigilanza, l'ENISA dovrebbe sostenere gli Stati membri nello svolgimento delle attività di assistenza reciproca relative ai soggetti essenziali e importanti che forniscono servizi in più di uno Stato membro o che forniscono servizi in uno o più Stati membri e i cui sistemi informativi e di rete sono ubicati in uno o più altri Stati membri. A tal fine gli Stati membri dovrebbero trasmettere informazioni supplementari al registro dei soggetti mantenuto dall'ENISA. Sulla base delle informazioni contenute nel registro dei soggetti essenziali e importanti, l'ENISA dovrebbe effettuare un'analisi completa dei rischi di cibersicurezza transfrontalieri relativi ai soggetti essenziali e importanti. L'analisi dovrebbe basarsi su una metodologia elaborata in collaborazione con la Commissione e il gruppo di cooperazione NIS. Tale metodologia potrebbe tenere conto della misura in cui i soggetti essenziali e importanti diffondono i propri servizi su un'ampia base transfrontaliera, dipendono da servizi transfrontalieri, sono esposti a un rischio di concentrazione della catena di approvvigionamento, possono essere identificati come fonte di rischio di concentrazione della catena di approvvigionamento, sono esposti a incidenti che potrebbero avere effetti negativi significativi sui servizi transfrontalieri o dipendono da sistemi informativi e di rete per la fornitura dei loro servizi situati in diversi Stati membri e al di fuori dell'Unione. Sulla base della relazione di analisi dei rischi, l'ENISA dovrebbe raccomandare alle pertinenti autorità competenti di istituire gruppi di esaminatori congiunti per sostenere la vigilanza dei soggetti con un livello di rischio più elevato per il buon funzionamento del mercato interno in caso di incidenti e assistere le autorità competenti, su loro richiesta, nell'esecuzione di azioni di vigilanza comuni.
- (13) Poiché l'obiettivo della presente direttiva, vale a dire semplificare l'attuazione delle misure per conseguire un livello comune elevato 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.
- (14) Il Garante europeo della protezione dei dati e il comitato europeo per la protezione dei dati sono stati consultati in conformità all'articolo 42, paragrafo 2, del regolamento

(UE) 2018/1725 del Parlamento europeo e del Consiglio⁹ e hanno espresso un parere congiunto il [data],

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

Articolo 1
Modifiche della direttiva (UE) 2022/2555

La direttiva (UE) 2022/2555 è così modificata:

(1) l'articolo 2 è così modificato:

(a) al paragrafo 2, la lettera a) è così modificata:

i) il punto iii) è sostituito dal seguente:

"iii) registri dei nomi di dominio di primo livello;"

ii) sono aggiunti i seguenti punti iv) e v):

"iv) fornitori di portafogli europei di identità digitale di cui al regolamento (UE) n. 910/2014;

v) fornitori di portafogli europei delle imprese istituiti a norma del regolamento (UE) [...]".

* Regolamento (UE) [...] [proposta di regolamento sull'istituzione dei portafogli europei delle imprese].";

(b) è aggiunto il paragrafo 3 bis seguente:

"3 bis. La presente direttiva si applica ai soggetti, indipendentemente dalle loro dimensioni, identificati come proprietari, gestori e operatori di infrastrutture strategiche a duplice uso a norma del regolamento (UE) [...]".

** Regolamento (UE) [...] [proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro di misure volte ad agevolare il trasporto di materiali, merci e personale militari in tutta l'Unione].";

(2) l'articolo 3 è così modificato:

(a) il paragrafo 1 è così modificato:

i) le lettere a) e b) sono sostituite dalle seguenti:

"a) soggetti di una tipologia elencata nell'allegato I che superano i massimali per le piccole imprese a media capitalizzazione;

b) prestatori di servizi fiduciari qualificati, fornitori di portafogli europei di identità digitale, fornitori di portafogli europei delle imprese e registri

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

dei nomi di dominio di primo livello, indipendentemente dalle loro dimensioni;"

ii) è aggiunta la seguente lettera h):

"h) soggetti identificati come proprietari, gestori e operatori di infrastrutture strategiche a duplice uso a norma del regolamento (UE) [...] [proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro di misure volte ad agevolare il trasporto di materiali, merci e personale militari in tutta l'Unione].";

(b) al paragrafo 4, il primo comma è sostituito dal seguente:

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

a) il proprio nome;

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

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

d) i dati di contatto aggiornati, compresi gli indirizzi e-mail, i numeri di telefono, l'identificativo unico e gli indirizzi digitali del portafoglio europeo delle imprese del soggetto, se del caso, e del suo rappresentante designato a norma dell'articolo 26, paragrafo 3, se del caso;

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

f) le serie di IP del soggetto.";

(3) l'articolo 5 è sostituito dal seguente:

"Articolo 5

Armonizzazione minima

Fatto salvo l'articolo 21, paragrafo 5, quinto comma, 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.";

(4) all'articolo 6

sono aggiunti i seguenti punti 42) e 43):

"42) "piccola impresa a media capitalizzazione": un'impresa quale definita nell'allegato della raccomandazione (UE) 2025/1099 della Commissione***;

43) "infrastruttura sottomarina di trasmissione dei dati": cavi sottomarini che trasmettono dati, la relativa infrastruttura e altri impianti o elementi associati alla trasmissione dei dati.

*** Raccomandazione (UE) 2025/1099 della Commissione, del 21 maggio 2025, relativa alla definizione delle piccole imprese a media capitalizzazione

- (5) all'articolo 7, paragrafo 2, è aggiunta la seguente lettera k):
- "k) la transizione verso la crittografia post-quantum, tenendo conto dei tempi di transizione e dei requisiti pertinenti stabiliti negli atti giuridici e nelle politiche dell'Unione applicabili.";
- (6) all'articolo 15, paragrafo 2, la prima frase è sostituita dalla seguente:
- "La rete di CSIRT è composta da rappresentanti dei CSIRT designati o istituiti a norma dell'articolo 10, della squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'Unione (CERT-UE) e dell'ENISA.";
- (7) l'articolo 21, paragrafo 5, è così modificato:
- (a) il secondo comma è sostituito dal seguente:
- "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. La Commissione valuta periodicamente se gli atti di esecuzione di cui al presente comma debbano essere adottati per settori o tipi di soggetti specifici per migliorare il funzionamento del mercato interno. Nel formulare tali valutazioni, la Commissione si concentra in particolare sulla natura transfrontaliera dei settori o dei tipi di soggetti e svolge un processo di consultazione aperto, trasparente e inclusivo con i pertinenti portatori di interessi e con gli Stati membri.";
- (b) è aggiunto il quinto comma seguente:
- "Quando la Commissione adotta atti di esecuzione di cui al primo e al secondo comma del presente paragrafo, gli Stati membri non impongono ulteriori requisiti tecnici, metodologici o settoriali relativi alle misure di cui all'articolo 21, paragrafo 2, della direttiva (UE) 2022/2555 ai soggetti che rientrano nell'ambito di applicazione di tali atti di esecuzione.";
- (8) all'articolo 23 sono aggiunti i paragrafi 12 e 13 seguenti:
- "12. Nell'adottare un atto di esecuzione a norma del paragrafo 11, primo comma, la Commissione vi include l'obbligo di trasmettere le seguenti informazioni relative agli attacchi ransomware a norma del paragrafo 1:
- (a) se il soggetto ha rilevato un attacco ransomware;
- (b) il vettore di attacco dell'attacco ransomware;
- (c) se sono state attuate misure di mitigazione.
13. In caso di incidente significativo causato da un attacco ransomware, gli Stati membri provvedono affinché i soggetti interessati comunichino, su richiesta del CSIRT o, se del caso, dell'autorità competente, attraverso un canale di comunicazione fornito dal CSIRT o, se del caso, dall'autorità competente:
- (a) se il soggetto ha ricevuto una richiesta di riscatto e, se del caso, da chi;
- (b) se è stato pagato un riscatto e, in caso affermativo, quale importo, tramite quale mezzo di pagamento e a quale beneficiario o destinatario,

compreso il prestatore di cripto-attività e il prestatore di servizi per le cripto-attività, se del caso.";

(9) all'articolo 24 sono aggiunti i paragrafi 4, 5 e 6 seguenti:

"4. Al fine di dimostrare la conformità all'articolo 21, gli Stati membri possono imporre ai soggetti essenziali e importanti di ottenere un certificato sulla postura di cibersicurezza nell'ambito di un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 75 del regolamento (UE) XXX/XXX**** [proposta di regolamento sulla cibersicurezza 2].

5. Se la postura di cibersicurezza di un soggetto essenziale o importante è certificata nell'ambito di un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 74 del regolamento (UE) XXX/XXX**** [proposta di regolamento sulla cibersicurezza 2] e se il certificato dimostra la conformità ai requisiti stabiliti in un atto di esecuzione adottato a norma dell'articolo 21, paragrafo 5, della presente direttiva o del diritto nazionale che recepisce l'articolo 21, paragrafi 1 e 2, della presente direttiva, le autorità competenti non sottopongono il soggetto a misure supplementari a norma dell'articolo 32, paragrafo 2, lettera b), o dell'articolo 33, paragrafo 2, lettera b), a seconda dei casi, per quanto riguarda i requisiti contemplati dal certificato.

6. Una certificazione a norma del paragrafo 4 lascia impregiudicata la responsabilità del soggetto essenziale o importante di conformarsi alla presente direttiva.

**** Regolamento (UE) XXX/XXX [proposta di regolamento sulla cibersicurezza 2].";

(10) l'articolo 26 è così modificato:

(a) al paragrafo 1, è aggiunta la lettera d) seguente:

"d) i vettori aerei, che sono considerati sotto la giurisdizione dello Stato membro la cui autorità competente per il rilascio delle licenze ha rilasciato la licenza d'esercizio al soggetto a norma del regolamento (CE) n. 1008/2008 del Parlamento europeo e del Consiglio*****, oppure, se la licenza d'esercizio o altro documento equivalente non è stato rilasciato a norma di tale regolamento, che sono considerati sotto la giurisdizione dello Stato membro in cui hanno il proprio stabilimento principale nell'Unione a norma del paragrafo 2.

***** Regolamento (CE) n. 1008/2008 del Parlamento europeo e del Consiglio, del 24 settembre 2008, recante norme comuni per la prestazione di servizi aerei nella Comunità (rifusione) (GU L 293 del 31.10.2008, pag. 3, ELI: <http://data.europa.eu/eli/reg/2008/1008/oj>).";

(b) il paragrafo 3 è sostituito dal seguente:

"3. Se un soggetto essenziale o importante 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. Qualora tale soggetto sia un soggetto di cui al paragrafo 1, lettera a), esso è considerato sotto la giurisdizione dello Stato membro in cui presta i suoi servizi. 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.";

(11) l'articolo 27 è così modificato:

(a) il paragrafo 1 è sostituito dal seguente:

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

(b) il paragrafo 2 è soppresso;

(c) i paragrafi 3, 4 e 5 sono sostituiti dai seguenti:

"3. Gli Stati membri provvedono affinché i soggetti essenziali e importanti notifichino all'autorità competente qualsiasi modifica delle informazioni trasmesse a norma dell'articolo 3, paragrafo 4, tempestivamente e, in ogni caso, entro due settimane dalla data della modifica.

4. In seguito alla ricezione delle informazioni di cui all'articolo 3, paragrafo 4, il punto di contatto unico dello Stato membro interessato le inoltra, senza indebito ritardo, all'ENISA.

5. Se opportuno, le informazioni di cui all'articolo 3, paragrafo 4, primo comma, del presente articolo sono trasmesse attraverso il meccanismo nazionale di cui all'articolo 3, paragrafo 4, quarto comma.";

(12) è inserito il seguente articolo 37 bis:

"Articolo 37 bis

Il ruolo dell'ENISA nell'assistenza reciproca

1. L'ENISA assiste gli Stati membri nello svolgimento delle attività di assistenza reciproca ai sensi dell'articolo 37 e contribuisce ad agevolare tali processi di cooperazione per i soggetti essenziali e importanti che forniscono servizi in più di uno Stato membro o che forniscono servizi in uno o più Stati membri e i cui sistemi informativi e di rete sono ubicati in uno o più altri Stati membri.

2. Ai fini di cui al paragrafo 1, l'ENISA effettua entro il ... [15 mesi dall'entrata in vigore del presente regolamento] un'analisi completa dei rischi di cibersicurezza transfrontalieri relativi ai soggetti essenziali e importanti che forniscono servizi in più di uno Stato membro o che forniscono servizi in uno o più Stati membri e i cui sistemi informativi e di rete sono ubicati in uno o più altri Stati membri. L'analisi valuta la portata delle possibili conseguenze transfrontaliere e sul mercato interno degli incidenti che interessano tali soggetti essenziali e importanti. Ai fini di tale analisi l'ENISA, in collaborazione con la Commissione e il gruppo di cooperazione,

elabora una metodologia. Sulla base dell'analisi, l'ENISA redige una relazione completa di valutazione transfrontaliera dei rischi di cibersicurezza, che è aggiornata annualmente.

3. Sulla base della relazione completa di valutazione transfrontaliera dei rischi di cibersicurezza, l'ENISA:

- (a) se del caso, raccomanda alle pertinenti autorità competenti di istituire gruppi di esaminatori congiunti a sostegno della vigilanza di soggetti specifici;
- (b) elabora orientamenti per le azioni di vigilanza comuni;
- (c) su richiesta delle autorità competenti degli Stati membri interessati, stabilisce le modalità pratiche per l'esecuzione delle azioni di vigilanza comuni;
- (d) su richiesta delle autorità competenti degli Stati membri interessati e compatibilmente con le proprie risorse, partecipa ad azioni di vigilanza comuni;
- (e) su richiesta delle autorità competenti degli Stati membri interessati, fornisce assistenza nella valutazione del livello di attuazione, da parte di un soggetto essenziale o importante, delle misure di gestione dei rischi di cibersicurezza di cui all'articolo 21.

4. Ai fini del paragrafo 3, lettera e), del presente articolo, le autorità competenti degli Stati membri interessati forniscono all'ENISA, se disponibile, un elenco delle misure di gestione dei rischi di cibersicurezza adottate dal soggetto essenziale o importante conformemente all'articolo 21, un elenco delle azioni di vigilanza o di esecuzione svolte, nonché la documentazione pertinente, compresi i dati che dimostrino l'attuazione di politiche in materia di cibersicurezza, quali i risultati di audit sulla sicurezza, che le autorità competenti hanno effettuato a norma degli articoli 32 e 33 nei confronti di tale soggetto.

5. Qualora uno Stato membro riceva l'assistenza reciproca di cui all'articolo 37, paragrafo 1, primo comma, lettera c), il punto di contatto unico informa l'ENISA dell'avvenuta assistenza reciproca. Se del caso, il punto di contatto unico indica quale incidente transfrontaliero di cui all'articolo 23, paragrafo 6, era connesso al caso di assistenza reciproca.";

- (13) gli allegati I e II sono modificati in conformità all'allegato della presente direttiva.

Articolo 2

Recepimento

1. Entro il ... [12 mesi dopo l'entrata in vigore della presente direttiva], gli Stati membri adottano e pubblicano le misure legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva. Essi ne informano immediatamente la Commissione.

Essi applicano tali disposizioni a decorrere dal ... [un giorno dopo la data di cui al primo comma].

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 3

Entrata in vigore

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

Articolo 4

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Strasburgo, il

Per il Parlamento europeo

La presidente

[...]

Per il Consiglio

Il presidente

[...]