COMMISSIONE
EUROPEA

Bruxelles, 13.9.2023
C(2023) 6068 final

COMUNICAZIONE DELLA COMMISSIONE

Orientamenti della Commissione sull'applicazione dell'articolo 4, paragrafi 1 e 2, della direttiva (UE) 2022/2555 (direttiva NIS 2)

I. Introduzione

1. A norma dell'articolo 4, paragrafo 3, della 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 (direttiva NIS 2)[1], la Commissione, entro il 17 luglio 2023, deve fornire orientamenti che chiariscano l'applicazione dell'articolo 4, paragrafi 1 e 2, della direttiva.

2. I presenti orientamenti chiariscono l'applicazione di tali disposizioni, che concernono la relazione tra la direttiva (UE) 2022/2555 e gli attuali e futuri atti giuridici settoriali dell'Unione riguardanti le misure di gestione dei rischi di cibersicurezza o gli obblighi di segnalazione degli incidenti. In appendice ai presenti orientamenti sono elencati gli atti giuridici settoriali dell'Unione che a parere della Commissione rientrano nell'ambito di applicazione dell'articolo 4 della direttiva (UE) 2022/2555. Il fatto che un atto non figuri in appendice non significa necessariamente che esso non rientri nell'ambito di applicazione di tale disposizione.

3. In applicazione dell'articolo 4, paragrafo 3, terza frase, della direttiva (UE) 2022/2555, prima di adottare i presenti orientamenti la Commissione ha tenuto conto delle osservazioni del gruppo di cooperazione NIS e dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA).

4. I presenti orientamenti non pregiudicano l'interpretazione del diritto dell'Unione da parte della Corte di giustizia dell'Unione europea.

II. Equivalenza degli obblighi di cibersicurezza degli atti giuridici settoriali dell'Unione

5. A norma dell'articolo 4, paragrafo 1, della direttiva (UE) 2022/2555, 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 suddetta direttiva, a tali soggetti non si applicano le pertinenti disposizioni della direttiva (UE) 2022/2555, comprese le disposizioni relative alla vigilanza e all'esecuzione di cui al capo VII della medesima. La stessa disposizione stabilisce altresì che, qualora gli atti giuridici settoriali dell'Unione non contemplino tutti i soggetti di un settore specifico che rientra nell'ambito di applicazione della direttiva (UE) 2022/2555, le pertinenti disposizioni della direttiva continuano ad applicarsi ai soggetti non contemplati da tali atti giuridici settoriali dell'Unione.

II.1. Obblighi di gestione dei rischi di cibersicurezza

6. A norma dell'articolo 4, paragrafo 2, lettera a), della direttiva (UE) 2022/2555, le misure di gestione dei rischi di cibersicurezza che i soggetti essenziali o importanti hanno l'obbligo di adottare ai sensi degli atti giuridici settoriali dell'Unione sono considerati di

[1] GU L 333 del 27.12.2022, pag. 80.

effetto equivalente agli obblighi stabiliti dalla direttiva (UE) 2022/2555 qualora gli effetti di tali misure siano almeno equivalenti a quelli delle misure di cui all'articolo 21, paragrafi 1 e 2, della suddetta direttiva. Nell'ambito della valutazione degli obblighi previsti da un atto giuridico settoriale dell'Unione riguardante misure di gestione dei rischi di cibersicurezza abbiano un effetto almeno equivalente a quelli delle misure di cui all'articolo 21, paragrafi 1 e 2, della direttiva (UE) 2022/2555, gli obblighi previsti da quel determinato atto giuridico settoriale dell'Unione dovrebbero corrispondere almeno agli obblighi di tali disposizioni o andare oltre, nel senso che le disposizioni settoriali potrebbero essere più granulari nel merito rispetto alle corrispondenti disposizioni della direttiva (UE) 2022/2555.

7. A norma dell'articolo 21, paragrafo 1, primo comma, della direttiva (UE) 2022/2555, gli Stati membri devono provvedere affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi. Tali misure dovrebbero essere basate sui rischi ed essere in grado di prevenire o ridurre al minimo l'impatto degli incidenti. L'articolo 21, paragrafo 1, secondo comma, della direttiva (UE) 2022/2555 specifica come deve essere valutata la proporzionalità di tali misure[2]. L'obbligo di cui all'articolo 21, paragrafo 1, della direttiva (UE) 2022/2555, che impone ai soggetti essenziali e importanti di adottare misure adeguate e proporzionate di gestione dei rischi di cibersicurezza, si riferisce a tutte le operazioni e a tutti i servizi del soggetto interessato, non solo a risorse informatiche specifiche o a servizi critici forniti dal soggetto.

8. Nell'ambito della valutazione dell'equivalenza di un atto giuridico settoriale dell'Unione alle pertinenti disposizioni della direttiva (UE) 2022/2555 in materia di gestione dei rischi di cibersicurezza, dovrebbe essere particolarmente importante determinare se gli obblighi di sicurezza imposti da tale atto giuridico comprendano misure volte a garantire la sicurezza dei sistemi informativi e di rete. La definizione di "sicurezza dei sistemi informativi e di rete" di cui all'articolo 6, punto 2, della direttiva (UE) 2022/2555, si riferisce alla capacità dei sistemi informativi 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 informativi e di rete o accessibili attraverso di essi. L'utilizzo dei termini "disponibilità", "autenticità", "integrità" e "riservatezza" nella suddetta definizione fa riferimento a tutti e quattro gli obiettivi di protezione connessi alla sicurezza dei sistemi informativi e di rete. Nell'espressione "sistemi informativi e di rete", quale definita all'articolo 6, punto 1, della direttiva (UE) 2022/2555, rientrano le reti di comunicazione elettronica[3], qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base a un programma, un'elaborazione

---

2 Cfr. anche i considerando 78, 81 e 82 del preambolo della direttiva (UE) 2022/2555.

3 Articolo 2, paragrafo 1, della 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).

automatica di dati digitali, e i dati digitali conservati, elaborati, estratti o trasmessi per mezzo di tali reti di comunicazione elettronica o dispositivi ai fini del loro funzionamento, del loro uso, della loro protezione e della loro manutenzione. Di conseguenza le misure di sicurezza previste da un atto giuridico settoriale dell'Unione dovrebbero comprendere anche gli hardware, i firmware e i software utilizzati nelle attività di un soggetto.

9. Un'altra considerazione importante nel valutare l'equivalenza di un atto giuridico settoriale dell'Unione alle prescrizioni di cui all'articolo 21, paragrafi 1 e 2, della direttiva (UE) 2022/2555, è che le misure di gestione dei rischi di cibersicurezza previste da tale atto devono basarsi su un "approccio multirischio". Poiché le minacce alla sicurezza dei sistemi informativi e di rete potrebbero avere origini diverse, qualsiasi tipo di evento può avere un impatto negativo sui sistemi informativi di rete del soggetto e determinare potenzialmente un incidente. Pertanto le misure di gestione dei rischi di cibersicurezza adottate dal soggetto devono proteggere non solo i sistemi informativi e di rete del soggetto stesso, ma anche l'ambiente fisico di tali sistemi da eventi quali sabotaggi, furti, incendi, inondazioni, problemi di telecomunicazione o interruzioni di corrente, o da qualsiasi accesso fisico non autorizzato in grado di compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi. Di conseguenza le misure di gestione dei rischi di cibersicurezza previste da un atto giuridico settoriale dell'Unione devono affrontare espressamente la sicurezza fisica e dell'ambiente dei sistemi informativi e di rete proteggendoli da guasti del sistema, errori umani, azioni malevole o fenomeni naturali[4].

10. L'articolo 21, paragrafo 2, della direttiva (UE) 2022/2555 stabilisce altresì che le misure di gestione dei rischi di cibersicurezza devono comprendere gli specifici requisiti di sicurezza elencati al paragrafo 2, lettere da a) a j), di tale disposizione. Tra i suddetti requisiti figurano misure quali politiche di analisi dei rischi e di sicurezza dei sistemi informativi, gestione degli incidenti, continuità operativa, gestione delle crisi, sicurezza della catena di approvvigionamento, politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura. A norma dell'articolo 21, paragrafo 5, secondo comma, della direttiva (UE) 2022/2555, alla Commissione è conferito il potere di adottare atti di esecuzione che stabiliscono i requisiti tecnici e metodologici, nonché, se necessario, i requisiti settoriali relativi alle misure di sicurezza di cui all'articolo 21, paragrafo 2, della direttiva. Per quanto riguarda i fornitori di servizi di sistema dei nomi di dominio ("DNS"), i registri dei nomi di dominio di primo livello ("TLD"), 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 e i prestatori di servizi fiduciari, entro il 17 ottobre 2024, la Commissione deve adottare atti di esecuzione sui requisiti tecnici e metodologici delle misure di sicurezza di cui all'articolo 21, paragrafo 2, della direttiva (UE) 2022/2555. Gli atti di esecuzione

[4] Cfr. considerando 79 del preambolo della direttiva (UE) 2022/2555.

specificano ulteriormente le condizioni e i criteri di attuazione principali stabiliti nell'atto di base, senza incidere sulla sostanza dell'atto in questione[5].

II.2. Obblighi di segnalazione

11. L'articolo 4, paragrafo 2, lettera b), della direttiva (UE) 2022/2555 stabilisce che gli obblighi di segnalazione riguardanti la notifica di incidenti significativi sono considerati di effetto equivalente agli obblighi stabiliti da tale direttiva qualora un atto giuridico settoriale dell'Unione preveda l'accesso immediato, se del caso automatico e diretto, alle notifiche degli incidenti da parte dei team di risposta agli incidenti di sicurezza informatica ("CSIRT"), delle autorità competenti o dei punti di contatto unici 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 direttiva (UE) 2022/2555.

12. Poiché gli obblighi di notifica degli incidenti significativi imposti da un atto giuridico settoriale dell'Unione devono avere un effetto almeno equivalente a quelli di cui all'articolo 23, paragrafi da 1 a 6, della direttiva (UE) 2022/2555 affinché tale atto sia applicato al posto degli obblighi di segnalazione della direttiva, gli obblighi di cui all'articolo 23, paragrafi da 1 a 6, della direttiva sono particolarmente importanti per la valutazione dell'equivalenza. L'articolo 23, paragrafi da 1 a 6, della direttiva (UE) 2022/2555 prescrive più dettagliatamente il tipo di incidenti che deve essere segnalato, i destinatari della segnalazione, le relative tempistiche e il contenuto delle informazioni. Ciò è spiegato in maggiore dettaglio nelle sottosezioni seguenti.

II.2.1. Notifica degli incidenti significativi ai CSIRT, alle autorità competenti e ai destinatari

13. La prima frase dell'articolo 23, paragrafo 1, primo comma, della direttiva (UE) 2022/2555 impone ai soggetti essenziali e importanti di notificare senza indebito ritardo al proprio CSIRT o, se opportuno, alla propria autorità competente, eventuali incidenti significativi. La seconda frase dell'articolo 23, paragrafo 1, primo comma, della direttiva (UE) 2022/2555 impone ai soggetti essenziali e importanti di notificare senza indebito ritardo ai destinatari dei loro servizi, se opportuno, gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi.

14. Mentre l'articolo 6, punto 6, della direttiva (UE) 2022/2555 fornisce una definizione molto ampia di "incidenti", ovvero tutti gli eventi che compromettono la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi, l'articolo 23, paragrafo 1, della direttiva si limita a prevedere un obbligo di segnalazione per gli incidenti significativi. Un incidente è significativo se ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato (articolo 23, paragrafo 3, lettera a)) o se si è ripercosso o è in grado di

[5] Cfr. *Criteri non vincolanti per l'applicazione degli articoli 290 e 291 del trattato sul funzionamento dell'Unione europea — 18 giugno 2019*, capo D, "Norme supplementari di integrazione dell'atto di base" (2019/C 223/01) (GU C 223 del 3.7.2019, pag. 1).

ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli (articolo 23, paragrafo 3, lettera b)).

15. Il considerando 101 del preambolo della direttiva (UE) 2022/2555 chiarisce che la segnalazione di incidenti dovrebbe basarsi su una valutazione iniziale condotta dal soggetto interessato. Detta valutazione iniziale dovrebbe tenere conto, tra l'altro, dei sistemi informativi 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.

16. A norma dell'articolo 23, paragrafo 11, secondo comma, della direttiva (UE) 2022/2555, alla Commissione è conferito il potere di adottare atti di esecuzione che specifichino ulteriormente i casi in cui un incidente debba essere considerato significativo. 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 mercati online, di motori di ricerca online e di piattaforme di servizi di social network, la Commissione deve adottare tali atti di esecuzione entro il 17 ottobre 2024. Gli atti di esecuzione specificano ulteriormente le condizioni e i criteri di attuazione principali stabiliti nell'atto di base, senza incidere sulla sostanza dell'atto in questione[6].

II.2.2. Approccio in più fasi alla segnalazione degli incidenti significativi e relative tempistiche

17. La direttiva (UE) 2022/2555 stabilisce un approccio in più fasi alla segnalazione degli incidenti significativi che comprende un preallarme, una notifica dell'incidente e una relazione finale. Questi tre elementi possono eventualmente essere integrati da relazioni intermedie e da una relazione sui progressi.

18. L'approccio in più fasi mira a 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[7].

19. Secondo l'approccio in più fasi, i soggetti essenziali e importanti devono innanzitutto trasmettere senza indebito ritardo, e comunque entro 24 ore da quando sono venuti a

[6] Cfr. *Criteri non vincolanti per l'applicazione degli articoli 290 e 291 del trattato sul funzionamento dell'Unione europea — 18 giugno 2019*, capo D, "Norme supplementari di integrazione dell'atto di base" (2019/C 223/01) (GU C 223 del 3.7.2019, pag. 1).

[7] Cfr. considerando 101 del preambolo della direttiva (UE) 2022/2555.

conoscenza dell'incidente significativo, un preallarme al CSIRT o all'autorità competente. Successivamente tali soggetti devono trasmettere senza indebito ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente. In seguito un CSIRT o un'autorità competente potrebbero richiedere una relazione intermedia. Infine deve essere trasmessa al CSIRT o all'autorità competente una relazione finale entro un mese dalla trasmissione della notifica dell'incidente, a meno che l'incidente sia ancora in corso al momento della trasmissione, nel qual caso devono essere fornite una relazione sui progressi e una relazione finale entro un mese dalla gestione dell'incidente.

20. Per la notifica dell'incidente di cui all'articolo 23, paragrafo 4, secondo comma, della direttiva (UE) 2022/2555 si applica una tempistica diversa in relazione ai prestatori di servizi fiduciari. Questi ultimi devono notificare gli incidenti significativi per la prestazione dei loro servizi fiduciari senza indebito ritardo e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo.

II.2.3. Contenuto della segnalazione obbligatoria degli incidenti significativi ai CSIRT o alle autorità competenti

21. Come regola generale, la terza frase dell'articolo 23, paragrafo 1, primo comma, della direttiva (UE) 2022/2555 impone agli Stati membri di provvedere affinché i soggetti essenziali e importanti comunichino, tra l'altro, qualunque informazione che consenta al CSIRT competente o, se opportuno, all'autorità competente di determinare l'eventuale impatto transfrontaliero dell'incidente. La suddetta prescrizione riguardante il contenuto della segnalazione obbligatoria è ulteriormente specificata all'articolo 23, paragrafo 4, della direttiva (UE) 2022/2555, che definisce l'approccio in più fasi.

22. A norma dell'articolo 23, paragrafo 4, lettera a), il preallarme deve indicare, ove opportuno, se l'incidente significativo è sospettato di essere il risultato di atti illegittimi o malevoli o se potrebbe avere (ossia se è probabile che abbia) un impatto transfrontaliero. Secondo il considerando 102 del preambolo della direttiva (UE) 2022/2555, il preallarme dovrebbe contenere soltanto le informazioni necessarie per informare il CSIRT o l'autorità competente dell'incidente significativo e consentire al soggetto interessato di chiedere assistenza, se necessario.

23. La notifica dell'incidente deve contenere, se opportuno, aggiornamenti delle informazioni trasmesse nel preallarme. Deve inoltre contenere una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione.

24. Qualora sia richiesta una relazione intermedia, essa deve contenere pertinenti aggiornamenti della situazione. La relazione finale deve comprendere una descrizione dettagliata dell'incidente, comprensiva della sua gravità e del suo impatto, il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente, le misure di mitigazione adottate e in corso e, se opportuno, l'impatto transfrontaliero dell'incidente.

II.2.4. Accesso immediato alle notifiche degli incidenti

25. L'articolo 4, paragrafo 2, lettera b), della direttiva (UE) 2022/2555 stabilisce che, per essere applicabile in relazione agli obblighi di notifica invece della direttiva, un atto giuridico settoriale dell'Unione deve fornire ai CSIRT, alle autorità competenti o ai punti di contatto unici a norma della medesima direttiva l'accesso immediato alle notifiche degli incidenti trasmesse in conformità dell'atto giuridico settoriale dell'Unione. Secondo il considerando 24 del preambolo della direttiva (UE) 2022/2555, 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.

26. L'accesso immediato può essere garantito tramite strumenti automatici e diretti che gli Stati membri dovrebbero istituire, se del caso. I meccanismi di segnalazione automatica e diretta garantiscono la condivisione sistematica e immediata delle informazioni con i CSIRT, le autorità competenti o i punti di contatto unici per quanto riguarda la gestione delle notifiche degli incidenti. Al fine di semplificare la segnalazione e di attuare il meccanismo di segnalazione automatica e diretta, gli Stati membri possono anche utilizzare un punto di accesso unico che deve essere conforme all'atto giuridico settoriale dell'Unione.

27. Ai fini della valutazione, gli obblighi previsti da un atto giuridico settoriale dell'Unione di notificare gli incidenti significativi hanno un effetto almeno equivalente a quelli di cui all'articolo 23, paragrafi da 1 a 6, della direttiva (UE) 2022/2555 se corrispondono almeno agli obblighi di cui all'articolo 23, paragrafi da 1 a 6, o sono più specifici di tali disposizioni. Gli obblighi devono fare riferimento al tipo di incidenti che devono essere segnalati a norma della direttiva (UE) 2022/2555, tenendo conto in particolare dei destinatari, dei contenuti e delle tempistiche applicabili.

III. Conseguenze dell'equivalenza

III.1. Vigilanza ed esecuzione

28. Qualora gli effetti degli obblighi previsti dagli atti giuridici settoriali dell'Unione siano almeno equivalenti a quelli degli obblighi di cui alla direttiva (UE) 2022/2555, non sono solo le pertinenti disposizioni della direttiva riguardanti l'obbligo di adottare misure di gestione dei rischi di cibersicurezza o di notificare incidenti significativi a non applicarsi, ma anche le disposizioni in materia di vigilanza ed esecuzione di cui al capo VII della direttiva (UE) 2022/2555.

29. Il considerando 25 del preambolo della direttiva (UE) 2022/2555 spiega che gli atti giuridici settoriali dell'Unione di effetto almeno equivalente potrebbero prevedere che le autorità competenti ai sensi di tali atti esercitino i loro poteri di vigilanza ed esecuzione in relazione a misure di gestione dei rischi di cibersicurezza o a obblighi di notifica con l'assistenza delle autorità competenti ai sensi della direttiva (UE) 2022/2555. Le autorità competenti interessate potrebbero stabilire modalità di cooperazione a tale scopo, comprese le procedure relative al coordinamento delle attività di vigilanza, 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. Tale meccanismo per lo scambio di informazioni pertinenti potrebbe comportare l'accesso alle informazioni relative alla cibersicurezza richieste dalle autorità competenti ai sensi della direttiva (UE) 2022/2555.

III.2. Strategia nazionale per la cibersicurezza

30. A norma dell'articolo 7, paragrafo 1, della direttiva (UE) 2022/2555, ogni Stato membro è tenuto ad adottare una strategia nazionale per la cibersicurezza. Per "strategia nazionale per la cibersicurezza" si intende 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 (cfr. articolo 6, punto 4, della direttiva (UE) 2022/2555). La strategia nazionale per la cibersicurezza deve comprendere, fra l'altro, gli obiettivi e le priorità che riguardano in particolare i settori di cui agli allegati I e II della direttiva (UE) 2022/2555. Deve comprendere inoltre un quadro di governance per la realizzazione di tali obiettivi e priorità, incluse le misure strategiche di cui all'articolo 7, paragrafo 2, della suddetta direttiva.

31. A norma dell'articolo 7, paragrafo 1, lettera c), della direttiva (UE) 2022/2555, la strategia nazionale per la cibersicurezza deve altresì comprendere 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 medesima direttiva, nonché il coordinamento e la cooperazione tra tali organismi e le autorità competenti ai sensi degli atti giuridici settoriali dell'Unione.

32. Di conseguenza l'obbligo di adottare una strategia per la cibersicurezza a norma dell'articolo 7 della direttiva (UE) 2022/2555 non riguarda gli obblighi in materia di cibersicurezza imposti ai soggetti essenziali e importanti a norma degli articoli 21 e 23 di tale direttiva né le disposizioni in materia di vigilanza ed esecuzione di cui al capo VII, come previsto dall'articolo 4, paragrafi 1 e 2, della direttiva. La pertinente disposizione dell'articolo 7 dovrebbe continuare ad applicarsi ai settori, ai sottosettori e ai tipi di soggetti per cui esistono atti giuridici settoriali dell'Unione ai sensi dell'articolo 4 della direttiva (UE) 2022/2555.

III.3. Designazione dei CSIRT

33. A norma dell'articolo 10, paragrafo 1, della direttiva (UE) 2022/2555, gli Stati membri devono designare o istituire uno o più CSIRT che si occupino almeno dei settori, dei sottosettori e dei tipi di soggetti di cui agli allegati I e II della suddetta direttiva, includendo così i settori, i sottosettori e i tipi di soggetti per cui esistono atti giuridici settoriali dell'Unione. A tal riguardo, generalmente i CSIRT svolgeranno anche i loro compiti di cui all'articolo 11, paragrafo 3, della direttiva (UE) 2022/2555, a meno che siano indicati compiti particolari negli atti giuridici settoriali dell'Unione.

III.4. Quadri nazionali di gestione delle crisi informatiche e EU-CyCLONe

34. A norma dell'articolo 9, paragrafo 1, della direttiva (UE) 2022/2555, gli Stati membri devono designare o istituire una o più autorità competenti responsabili della gestione degli incidenti e delle crisi di cibersicurezza su vasta scala. Conformemente all'articolo 6, punto 7, di tale direttiva, per "incidente di cibersicurezza su vasta scala" si intende 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. Conformemente all'articolo 9, paragrafo 4, della direttiva (UE) 2022/2555, gli Stati membri devono inoltre adottare 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. Il suddetto piano deve definire, fra l'altro, 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, nonché i pertinenti portatori di interessi del settore pubblico e privato e le infrastrutture coinvolte. Tali procedure di gestione delle crisi informatiche, nonché i portatori di interessi del settore pubblico e privato e le infrastrutture pertinenti, potrebbero comprendere procedure e portatori di interessi settoriali.

35. L'articolo 16 della direttiva (UE) 2022/2555 istituisce la rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe), il cui scopo è sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala e garantire il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione.

36. Poiché l'articolo 9 relativo ai quadri di gestione delle crisi informatiche e l'articolo 16 relativo a EU-CyCLONe non riguardano gli obblighi di cibersicurezza imposti ai soggetti a norma degli articoli 21 e 23 della direttiva (UE) 2022/2555 né la vigilanza e l'esecuzione di cui al capo VII, come previsto dall'articolo 4, paragrafi 1 e 2, della direttiva, gli articoli 9 e 16 devono essere applicati integralmente ai settori, nonostante l'esistenza di atti giuridici settoriali dell'Unione ai sensi dell'articolo 4. Gli Stati membri devono pertanto designare o istituire una o più autorità competenti responsabili della gestione degli incidenti e delle crisi di cibersicurezza su vasta scala che si verificano nei settori contemplati dagli atti giuridici settoriali dell'Unione. Inoltre i settori contemplati dagli atti giuridici settoriali dell'Unione non devono essere trascurati quando si adotta il piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala. Infine EU-CyCLONe deve svolgere i suoi compiti di cui all'articolo 16 della direttiva (UE) 2022/2555 nei settori in cui i soggetti sono soggetti ad atti giuridici settoriali dell'Unione.

III.5. Esclusione dell'applicazione dell'articolo 3, paragrafi 3 e 4, dell'articolo 20 e dell'articolo 27, paragrafi 2 e 3

37. A norma dell'articolo 3, paragrafo 3, della direttiva (UE) 2022/2555, gli Stati membri sono tenuti a definire un elenco dei soggetti essenziali e importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio rientranti nell'ambito di applicazione della direttiva. A norma dell'articolo 27, paragrafo 2, gli Stati membri devono esigere che i soggetti di cui all'articolo 27, paragrafo 1, di tale direttiva trasmettano

determinate informazioni alle autorità competenti. Poiché le suddette disposizioni hanno lo scopo di garantire una panoramica chiara dei soggetti essenziali e importanti che rientrano nell'ambito di applicazione della direttiva (UE) 2022/2555 al fine di sostenere la vigilanza di tali soggetti, ne consegue che esse non dovrebbero applicarsi ai soggetti cui si applica un atto giuridico settoriale dell'Unione per quanto riguarda gli obblighi di gestione e di segnalazione dei rischi di cibersicurezza. Ciò non impedisce agli Stati membri di includere tali soggetti nell'elenco.

A norma dell'articolo 20, paragrafo 1, della direttiva (UE) 2022/2555, gli organi di gestione dei soggetti essenziali e importanti devono approvare le misure di gestione dei rischi di cibersicurezza adottate da tali soggetti per conformarsi all'articolo 21 e sovraintendere alla sua attuazione, e possono essere ritenuti responsabili di violazione da parte dei soggetti di tale articolo. A norma dell'articolo 20, paragrafo 2, della direttiva, gli Stati membri devono provvedere 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. Poiché gli obblighi derivanti dall'articolo 20 della direttiva (UE) 2022/2555 sono intrinsecamente collegati a quelli di cui all'articolo 21 della medesima direttiva, ne consegue che l'articolo 20 non debba applicarsi nel caso in cui si applichino atti giuridici settoriali dell'Unione ai sensi dell'articolo 4 di tale direttiva con riguardo agli obblighi di gestione dei rischi di cibersicurezza.

APPENDICE: atti giuridici settoriali dell'Unione

Regolamento (UE) 2022/2554 (atto sulla resilienza operativa digitale)[1]

1. L'articolo 1, paragrafo 2, del regolamento (UE) 2022/2554 (atto sulla resilienza operativa digitale, DORA) stabilisce che, quanto alle entità finanziarie contemplate dalla direttiva (UE) 2022/2555 e dalle rispettive norme nazionali di recepimento, detto regolamento è considerato un atto giuridico settoriale dell'Unione ai sensi dell'articolo 4 della suddetta direttiva. Tale affermazione è ripresa al considerando 28 del preambolo della direttiva (UE) 2022/2555, secondo cui il DORA dovrebbe essere considerato un atto giuridico settoriale dell'Unione in relazione alla direttiva (UE) 2022/2555 per quanto riguarda i soggetti del settore finanziario. Di conseguenza, invece delle disposizioni stabilite nella direttiva (UE) 2022/2555, dovrebbero applicarsi quelle del regolamento (UE) 2022/2554 relative alla gestione dei rischi delle tecnologie dell'informazione e della comunicazione (TIC) (articolo 6 e seguenti), alla gestione degli incidenti connessi alle TIC e, in particolare, alla segnalazione dei gravi incidenti TIC (articolo 17 e seguenti), nonché ai test di resilienza operativa digitale (articolo 24 e seguenti), ai meccanismi di condivisione delle informazioni (articolo 25) e ai rischi informatici TIC derivanti da terzi (articolo 28 e seguenti). Gli Stati membri non devono pertanto applicare le disposizioni della direttiva (UE) 2022/2555 riguardanti gli obblighi di gestione e segnalazione dei rischi di cibersicurezza e la vigilanza e l'esecuzione alle entità finanziarie contemplate dal regolamento (UE) 2022/2554.

2. A tale proposito si considerano entità finanziarie le entità di cui all'articolo 2, paragrafo 1, lettere da a) a t), del regolamento (UE) 2022/2554. Tra i tipi di soggetti che rientrano nell'ambito di applicazione del regolamento (UE) 2022/2554 come entità finanziarie e nell'ambito di applicazione della direttiva (UE) 2022/2555 come soggetti essenziali o importanti figurano enti creditizi, sedi di negoziazione e controparti centrali. Poiché è importante mantenere una solida relazione e lo scambio di informazioni con il settore finanziario a norma della direttiva (UE) 2022/2555, le autorità europee di vigilanza e le autorità competenti a norma del regolamento (UE) 2022/2554 possono chiedere di partecipare alle attività del gruppo di cooperazione[2] e scambiare informazioni e cooperare con i punti di contatto unici, nonché con i CSIRT e le autorità competenti a norma della direttiva (UE) 2022/2555[3]. Le autorità competenti a norma del regolamento (UE) 2022/2554 dovrebbero inoltre trasmettere 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 a norma della direttiva (UE) 2022/2555. Tale obiettivo può essere raggiunto fornendo accesso immediato alle notifiche di incidenti e trasmettendole direttamente o attraverso un unico punto di accesso. I CSIRT dovrebbero

---

[1] 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 (GU L 333 del 27.12.2022, pag. 1).

[2] Articolo 14, paragrafo 3, della direttiva (UE) 2022/2555 e articolo 47, paragrafo 1, del regolamento (UE) 2022/2554.

[3] Cfr. considerando 28 della direttiva (UE) 2022/2555.

poter contemplare il settore finanziario nelle loro attività[4]. Gli Stati membri dovrebbero continuare a inserire il settore finanziario nelle loro strategie di cibersicurezza. Le disposizioni riguardanti i quadri nazionali di gestione delle crisi informatiche (articolo 9 della direttiva (UE) 2022/2555) e EU-CyCLONe (articolo 16 della direttiva (UE) 2022/2555), devono continuare ad applicarsi ai soggetti che rientrano nell'ambito di applicazione del regolamento (UE) 2022/2554.

[4] Ibid.