



Council of the
European Union

Brussels, 3 April 2023

6532/23

**Interinstitutional File:
2020/0359 (COD)**

**JUR 124
CYBER 37
TELECOM 42
CSC 80
CSCI 26
DATAPROTECT 45
JAI 177
MI 120
CODEC 206**

LEGISLATIVE ACTS AND OTHER INSTRUMENTS: CORRIGENDUM/RECTIFICATIF

Subject: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
(Official Journal of the European Union L 333 of 27 December 2022)

LANGUAGES concerned: **IT, NL**

PROCEDURE APPLICABLE (according to Council document R/2521/75):

— Procedure 2(b) (obvious errors in a number of language versions)

This text has also been transmitted to the European Parliament.

TIME LIMIT for the observations by Member States: 8 days

**OBSERVATIONS to be notified to: dql.rectificatifs@consilium.europa.eu
(DQL RECTIFICATIFS (JUR 7), Directorate Quality of Legislation, Legal Service)**

RETTIFICA

della 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)

(Gazzetta ufficiale dell'Unione europea L 333 del 27 dicembre 2022)

1. Pagina 80, considerando 3, prima frase:

anziché:

"(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. (...)"

leggasi:

"(3) I sistemi informativi 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. (...)".

2. Pagina 80, considerando 3, terza frase:

anziché:

"(...) 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. (...)"

leggasi:

"(...) 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 informativi e di rete. (...)".

3. Pagina 81, considerando 4, terza frase:

anziché:

"(...) Tali disparità comportano costi aggiuntivi e creano difficoltà per le entità che offrono beni o servizi transfrontalieri. (...)"

leggasi:

"(...) Tali disparità comportano costi aggiuntivi e creano difficoltà per i soggetti che offrono beni o servizi transfrontalieri. (...)".

4. Pagina 81, considerando 4:

anziché:

"(...) Gli obblighi di cibersecurity 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 cibersecurity in uno Stato membro abbia ripercussioni sul livello di cibersecurity di altri Stati membri, in particolare in considerazione dell'intensità degli scambi transfrontalieri. (...)"

leggasi:

"(...) I requisiti in materia di cibersecurity 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 dei requisiti in materia di cibersecurity in uno Stato membro abbia ripercussioni sul livello di cibersecurity di altri Stati membri, in particolare in considerazione dell'intensità degli scambi transfrontalieri. (...)".

5. Pagina 86, considerando 31:

anziché:

"(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 cibersecurity 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."

leggasi:

"(31) I soggetti appartenenti al settore delle infrastrutture digitali sono essenzialmente basati su sistemi informativi 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 cibersecurity 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."

6. Pagina 87, considerando 35, terza frase:

anziché:

"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. (...)"

leggasi:

"Al fine di gestire tutti i rischi posti alla sicurezza dei sistemi informativi e di rete, la presente direttiva dovrebbe pertanto applicarsi ai fornitori di servizi di data center che non sono servizi di cloud computing. (...)"

7. Pagina 87, considerando 36, seconda frase:

anziché:

"(36) (...) 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 cibersecurity globale del mercato interno. (...)"

leggasi:

"(36) (...) Tali soggetti possono pertanto essere attori importanti nelle catene del valore, il che rende la sicurezza dei loro sistemi informativi e di rete parte integrante della cibersecurity globale del mercato interno. (...)".

8. Pagina 88, considerando 39:

anziché:

"(39) Al fine di agevolare la cooperazione e la comunicazione transfrontaliera 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."

leggasi:

"(39) Al fine di agevolare la cooperazione e la comunicazione transfrontaliera 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 informativi e di rete e la cooperazione transfrontaliera a livello dell'Unione."

9. Pagina 89, considerando 43:

anziché:

"(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"

leggasi:

"(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 informativi 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".

10. Pagina 91, considerando 58, prima frase:

anziché:

"(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. (...)"

leggasi:

"(58) Poiché lo sfruttamento delle vulnerabilità nei sistemi informativi 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. (...)"

11. Pagina 95, considerando 77:

anziché:

"(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 cibersecurity adeguate ai rischi esistenti."

leggasi:

"(77) La responsabilità di garantire la sicurezza dei sistemi informativi 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 cibersecurity adeguate ai rischi esistenti."

12. Pagina 95, considerando 78:

anziché:

"(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."

leggasi:

"(78) Le misure di gestione dei rischi dovrebbero tenere conto del grado di dipendenza del soggetto essenziale o importante dai sistemi informativi 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 informativi 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 informativo e di rete."

13. Pagina 95, considerando 79:

anziché:

"(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."

leggasi:

"(79) Poiché le minacce alla sicurezza dei sistemi informativi 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 informativi 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 informativi 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 informativi 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."

14. Pagina 95, considerando 81:

anziché:

"(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."

leggasi:

"(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 informativo 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".

15. Pagina 96, considerando 83:

anziché:

"(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"

leggasi:

"(83) I soggetti essenziali e importanti dovrebbero garantire la sicurezza dei sistemi informativi e di rete che utilizzano nelle loro attività. Si tratta in particolare di sistemi informativi 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 informativi e di rete o che la esternalizzino".

16. Pagina 96, considerando 85:

anziché:

"(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. (...)"

leggasi:

"(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 informativi e di rete di un soggetto sfruttando le vulnerabilità che interessano prodotti e servizi di terzi. (...)"

17. Pagina 96, considerando 89, ultima frase:

anziché:

"(89) (...) Inoltre, tali soggetti dovrebbero valutare le loro capacità di cibersecurity e, se del caso, perseguire l'integrazione di tecnologie per il rafforzamento della cibersecurity quali l'intelligenza artificiale o i sistemi di apprendimento automatico, per migliorare le loro capacità e la sicurezza dei sistemi informatici e di rete."

leggasi:

"(89) (...) Inoltre, tali soggetti dovrebbero valutare le loro capacità di cibersecurity e, se del caso, perseguire l'integrazione di tecnologie per il rafforzamento della cibersecurity quali l'intelligenza artificiale o i sistemi di apprendimento automatico, per migliorare le loro capacità e la sicurezza dei sistemi informativi e di rete."

18. Pagina 97, considerando 92, prima frase:

anziché:

"(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. (...)"

leggasi:

"(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 informativi 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. (...)"

19. Pagina 98, considerando 96, terza e quarta frase:

anziché:

"(96) (...) 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. (...)"

leggasi:

"(96) (...) 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 informativi e di rete. I fornitori di servizi di comunicazione interpersonale indipendenti dal numero dovrebbero garantire un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti. (...)".

20. Pagina 99, considerando 101, terza frase:

anziché:

"(101) (...) 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. (...)"

leggasi:

"(101) (...) 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. (...)".

21. Pagina 102, considerando 114, terza frase:

anziché:

"(114) (...) 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(...)"

leggasi:

"(114) (...) 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 informativi 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(...)"

22. Pagina 103, considerando 117, prima frase:

anziché:

"(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. (...)"

leggasi:

"(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 soggetti, sulla base delle informazioni ricevute dagli Stati membri, se del caso attraverso i meccanismi nazionali istituiti per la loro registrazione. (...)".

23. Pagina 104, considerando 121, prima frase:

anziché:

"(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. (...)"

leggasi:

"(121) Il trattamento dei dati personali, nella misura necessaria e proporzionata al fine di garantire la sicurezza dei sistemi informativi 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. (...)"

24. Pagina 106, considerando 135:

anziché:

"(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."

leggasi:

"(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 un sistema informativo e di rete sul territorio di tale Stato membro."

25. Pagina 108, articolo 1, titolo:

anziché:

"Oggetto e ambito di applicazione"

leggasi:

"Oggetto".

26. Pagina 108, articolo 1, paragrafo 2, lettera a):

anziché:

"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);"

leggasi:

"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 cibersicurezza (punti di contatto unici) e team di risposta agli incidenti di sicurezza informatica (CSIRT);".

27. Pagina 110, articolo 3, paragrafo 4, parte introduttiva:

anziché:

"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:"

leggasi:

"4. 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:".

28. Pagina 111, articolo 3, paragrafo 4, ultimo comma:

anziché:

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

leggasi:

"Gli Stati membri possono istituire meccanismi nazionali che consentano ai soggetti di registrarsi".

29. Pagina 111, articolo 3, paragrafo 5, primo comma, lettera a):

anziché:

"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"

leggasi:

"a) alla Commissione e al gruppo di cooperazione, 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".

30. Pagina 111, articolo 6, punto 1):

anziché:

"1) «sistema informatico e di rete»:"

leggasi:

"1) «sistema informativo e di rete»:".

31. Pagina 112, articolo 6, punto 2):

anziché:

"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;"

leggasi:

"2) «sicurezza dei sistemi informativi e di rete»: la 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;"

32. Pagina 112, articolo 6, punto 5):

anziché:

"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;"

leggasi:

"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 informativi e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato;"

33. Pagina 112, articolo 6, punto 6):

anziché:

"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;"

leggasi:

"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 informativi e di rete o accessibili attraverso di essi;"

34. Pagina 112, articolo 6, punto 11):

anziché:

"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;"

leggasi:

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

35. Pagina 114, articolo 6, punto 39):

anziché:

"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;"

leggasi:

"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 informativo e di rete, tramite assistenza o amministrazione attiva effettuata nei locali dei clienti o a distanza;"

36. Pagina 115, articolo 7, paragrafo 1, lettera h):

anziché:

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

leggasi:

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

37. Pagina 115, articolo 7, paragrafo 2, lettera d):

anziché:

"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;"

leggasi:

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

38. Pagina 118, articolo 11, paragrafo 3, lettera a):

anziché:

"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;"

leggasi:

"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 informativi e di rete;"

39. Pagina 119, articolo 11, paragrafo 3, lettera e):

anziché:

"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;"

leggasi:

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

40. Pagina 119, articolo 11, paragrafo 3, secondo comma:

anziché:

"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."

leggasi:

"I CSIRT possono effettuare una scansione proattiva e non intrusiva dei sistemi informativi e di rete accessibili al pubblico di soggetti essenziali e importanti. Tale scansione è effettuata per individuare sistemi informativi 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."

41. Pagina 120, articolo 12, paragrafo 2, primo comma, seconda frase:

anziché:

"2. (...) 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. (...):"

leggasi:

"2. (...). A tal fine l'ENISA istituisce e gestisce i sistemi informativi, 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 informativi e di rete, di divulgare e registrare, su base volontaria, le vulnerabilità pubblicamente note presenti nei prodotti TIC o nei servizi TIC. (...):".

42. Pagina 120, articolo 12, paragrafo 2, primo comma, lettera c):

anziché:

"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."

leggasi:

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

43. Pagina 120, articolo 13, paragrafo 3:

anziché:

"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."

leggasi:

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

44. Pagina 121, articolo 14, paragrafo 4, lettera j):

anziché:

"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;"

leggasi:

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

45. Pagina 122, articolo 14, paragrafo 4, lettera m):

anziché:

"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";

leggasi:

"m) effettuare scambi di opinioni sulla politica in materia di azioni intraprese a seguito di incidenti e crisi di cibersicurezza su vasta scala sulla base delle lezioni apprese dalla rete di CSIRT e da EU-CyCLONE";

46. Pagina 124, articolo 16, paragrafo 3, lettera a):

anziché:

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

leggasi:

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

47. Pagina 124, articolo 16, paragrafo 3, lettera c):

anziché:

"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;"

leggasi:

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

48. Pagina 125, articolo 18, paragrafo 1, primo comma:

anziché:

"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:"

leggasi:

"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 da dispositivo automatico e comprende gli aspetti seguenti:"

49. Pagina 127, articolo 21, paragrafo 1, primo comma:

anziché:

"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."

leggasi:

"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 informativi 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."

50. Pagina 127, articolo 21, paragrafo 1, secondo comma:

anziché:

"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."

leggasi:

"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 informativi 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."

51. Pagina 127, articolo 21, paragrafo 2, parte introduttiva:

anziché:

"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:"

leggasi:

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

52. Pagina 127, articolo 21, paragrafo 2, lettera a):

anziché:

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

leggasi:

"a) politiche di analisi dei rischi e di sicurezza dei sistemi informativi;"

53. Pagina 127, articolo 21, paragrafo 2, lettera e):

anziché:

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

leggasi:

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

54. Pagina 129, articolo 23, paragrafo 4, lettera d), punto iii):

anziché:

"iii) le misure di attenuazione adottate e in corso;"

leggasi:

"iii) le misure di mitigazione adottate e in corso;"

55. Pagina 129, articolo 23, paragrafo 5, prima frase:

anziché:

"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."

leggasi:

"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 mitigazione."

56. Pagina 130, articolo 23, paragrafo 10:

anziché:

"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."

leggasi:

"10. I CSIRT 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."

57. Pagina 131, articolo 25, paragrafo 1:

anziché:

"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."

leggasi:

"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 informativi e di rete."

58. Pagina 132, articolo 26, paragrafo 5:

anziché:

"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."

leggasi:

"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 informativo e di rete nel loro territorio."

59. Pagina 132, articolo 27, paragrafo 3:

anziché:

"3. Gli Stati membri provvedono affinché i soggetti di cui al paragrafo 1 notificchino 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."

leggasi:

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

60. Pagina 133, articolo 29, paragrafo 1, lettera b):

anziché:

"b) aumenta il livello di cibersecurity, 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."

leggasi:

"b) aumenta il livello di cibersecurity, 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 mitigazione o fasi di risposta e recupero, oppure promuovendo la ricerca collaborativa sulle minacce informatiche tra soggetti pubblici e privati."

61. Pagina 136, articolo 32, paragrafo 4, lettera g):

anziché:

"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;"

leggasi:

"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 21 e 23;"

62. Pagina 140, articolo 37, paragrafo 1, primo comma:

anziché:

"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:"

leggasi:

"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 informativi 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:"

63. Pagina 140, articolo 37, paragrafo 2:

anziché:

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

leggasi:

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

RECTIFICATIE

**van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022
betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie,
tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot
intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn)**

(Publicatieblad van de Europese Unie L 333 van 27 december 2022)

Bladzijde 108, artikel 2, lid 2, punt a), iii):

in plaats van:

“iii) registers voor topleveldomeinnamen en verleners van domeinnaamregistratiediensten;”,

lezen:

“iii) registers voor topleveldomeinnamen en aanbieders van domeinnaamsysteemdiensten;”.
