Parere congiunto 4/2026 dell'EDPB e del GEPD

sulla proposta di regolamento sulla cibersicurezza 2
e sulla proposta di modifica della direttiva NIS 2

Adottato il 18 marzo 2026

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Indice

Sintesi

Il 20 gennaio 2026 la Commissione europea ha pubblicato una proposta di regolamento relativo all'Agenzia dell'Unione europea per la cibersicurezza (ENISA), al quadro europeo di certificazione della cibersicurezza e alla sicurezza della catena di approvvigionamento delle TIC e che abroga il regolamento (UE) 2019/881 (regolamento sulla cibersicurezza 2) e una proposta di direttiva che modifica la direttiva (UE) 2022/2555 per quanto riguarda le misure di semplificazione e l'allineamento alla [proposta di regolamento sulla cibersicurezza 2]. Il 21 gennaio 2026 la Commissione ha consultato formalmente l'EDPB e il GEPD conformemente all'articolo 42, paragrafo 2, del regolamento (UE) 2018/1725.

L'EDPB e il GEPD ricordano che il rapporto tra protezione dei dati e cibersicurezza è ambivalente. Da un lato, la cibersicurezza contribuisce alla protezione dei dati personali limitando i rischi di accesso indesiderato, modifica o indisponibilità dei dati. Dall'altro, alcune misure di cibersicurezza possono interferire con i diritti e le libertà delle persone, in particolare i diritti alla vita privata e alla protezione dei dati. Pertanto, sebbene l'efficacia sia un obiettivo importante delle misure di cibersicurezza, occorre tenere conto della loro necessità e proporzionalità.

L'EDPB e il GEPD sostengono l'obiettivo generale delle proposte di rafforzare il ruolo dell'ENISA e di facilitare la diffusione della certificazione della cibersicurezza, nel rispetto delle raccomandazioni specifiche fornite nel presente parere congiunto. Accolgono inoltre con favore l'obiettivo di stabilire meccanismi e condizioni nella direttiva (UE) 2022/2555 per contribuire a facilitare la conformità ai requisiti di cibersicurezza, rendendo in tal modo la loro attuazione più coerente ed efficace, nonché l'obiettivo di affrontare ulteriormente i vari rischi per le catene di approvvigionamento delle TIC, compresi quelli di natura non tecnica. L'EDPB e il GEPD sostengono fermamente anche l'obiettivo di istituire un punto di accesso unico per la segnalazione delle violazioni dei dati personali, in quanto ridurrebbe gli oneri amministrativi per le organizzazioni senza incidere sul livello di protezione degli interessati.

L'EDPB e il GEPD accolgono inoltre con favore il fatto che la proposta di regolamento sulla cibersicurezza 2 chiarirebbe ulteriormente le modalità con cui l'ENISA fornisce sostegno ai diversi portatori di interessi e raccomandano di aggiungere anche il GEPD quale possibile soggetto richiedente la consulenza dell'ENISA. L'EDPB e il GEPD sostengono fermamente che tale consulenza farebbe seguito a una richiesta, garantendo un chiaro coordinamento e una chiara ripartizione delle responsabilità.

Per quanto riguarda la cooperazione tra l'ENISA e altri soggetti dell'Unione in generale, l'EDPB e il GEPD accolgono con favore le sinergie che tale cooperazione può apportare, in linea con i rispettivi compiti e mandati. Raccomandano di aggiungere un riferimento esplicito anche al GEPD in quanto organismo dell'Unione con cui l'ENISA coopererebbe.

L'EDPB e il GEPD ritengono che se i futuri compiti dell'ENISA quale polo di informazione richiedessero un trattamento sostanziale dei dati personali, ciò dovrebbe essere esplicitato nelle disposizioni dell'atto di base che disciplinano i rispettivi compiti, specificando anche gli elementi essenziali di qualsiasi trattamento su larga scala e le garanzie adeguate. Per contro, se l'obiettivo è consentire all'ENISA principalmente di raccogliere e trattare ulteriormente dati per lo più aggregati e non personali, anche ciò dovrebbe essere chiarito.

L'EDPB e il GEPD ricordano che, in linea di principio, solo i dettagli molto tecnici (pratici) relativi al trattamento dei dati personali dovrebbero essere decisi nell'ambito dell'autonomia amministrativa dell'organismo dell'UE interessato (in questo caso il consiglio di amministrazione di un'agenzia decentrata). L'EDPB e il GEPD raccomandano inoltre di prevedere, all'articolo 66 della proposta di regolamento sulla cibersicurezza 2, una consultazione preventiva con il GEPD prima dell'adozione di tali norme.

Per quanto riguarda il quadro europeo delle competenze in materia di cibersicurezza ("ECSF"), l'EDPB e il GEPD raccomandano ai colegislatori di modificare l'articolo 19, paragrafo 2, della proposta di regolamento sulla cibersicurezza 2 affinché l'ECSF non si limiti esclusivamente ai "professionisti della cibersicurezza", ma includa anche profili per la forza lavoro generale.

Per quanto riguarda il quadro europeo di certificazione della cibersicurezza, l'EDPB e il GEPD raccomandano di chiarire ulteriormente l'ambito di applicazione dell'articolo 80, paragrafo 1, lettera w), del regolamento sulla cibersicurezza 2 e il rapporto con la certificazione GDPR. L'EDPB e il GEPD raccomandano inoltre di imporre all'ENISA di consultarsi con l'EDPB prima di adottare un sistema di certificazione a norma dell'articolo 80, paragrafo 1, lettera w), del regolamento sulla cibersicurezza 2 per garantire la coerenza.

L'EDPB e il GEPD sottolineano la necessità di considerare non solo l'efficacia delle misure di cibersicurezza, ma anche la loro necessità e proporzionalità. L'EDPB e il GEPD raccomandano di chiarire che i sistemi di certificazione dovrebbero, nella misura del possibile, tenere conto dei controlli di sicurezza che possono contribuire a dimostrare il rispetto delle prescrizioni del GDPR, in particolare quando tali sistemi si applicano a prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti che possono essere utilizzati nell'ambito del trattamento dei dati.

Inoltre l'EDPB e il GEPD accolgono con favore la misura proposta volta a garantire un quadro per catene di approvvigionamento delle TIC affidabili e ad affrontare i rischi di natura non tecnica nei settori ad alta criticità.

Per quanto riguarda la proposta di modifica della direttiva NIS 2, l'EDPB e il GEPD accolgono con favore la designazione dei fornitori di portafogli europei di identità digitale e di portafogli europei delle imprese quali "soggetti essenziali" e sostengono pienamente l'importante obiettivo di prevenire attacchi ransomware futuri e di fermare e smantellare le organizzazioni criminali che ne sono alla base.

Il comitato europeo per la protezione dei dati e il Garante europeo della protezione dei dati

visto l'articolo 42, paragrafo 2, del regolamento (UE) 2018/1725, 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,

hanno adottato il seguente parere congiunto ("parere")

1 CONTESTO

1. Il 20 gennaio 2026 la Commissione europea ("Commissione") ha pubblicato una proposta di regolamento relativo all'Agenzia dell'Unione europea per la cibersicurezza (ENISA), al quadro europeo di certificazione della cibersicurezza e alla sicurezza della catena di approvvigionamento delle TIC e che abroga il regolamento (UE) 2019/881 (regolamento sulla cibersicurezza 2)[1] e una proposta di direttiva che modifica la direttiva (UE) 2022/2555 per quanto riguarda le misure di semplificazione e l'allineamento alla [proposta di regolamento sulla cibersicurezza 2] [2] (in appresso "proposta di regolamento sulla cibersicurezza 2", "proposta di modifica della direttiva NIS 2" e, congiuntamente, "proposte"). Il 21 gennaio 2026 la Commissione ha consultato formalmente l'EDPB e il GEPD conformemente all'articolo 42, paragrafo 2, del regolamento (UE) 2018/1725 ("EUDPR")[3].
2. La proposta di regolamento sulla cibersicurezza 2 mira a sostituire l'attuale regolamento sulla cibersicurezza[4] al fine di 1) rafforzare il ruolo dell'ENISA, prestando particolare attenzione alle esigenze dei portatori di interessi in un panorama delle minacce sempre più ostile, 2) rilanciare l'attuazione del quadro europeo di certificazione della cibersicurezza, 3) ridurre la complessità e la diversità delle politiche in materia di cibersicurezza e 4) affrontare ulteriormente i rischi per la sicurezza delle catene di approvvigionamento delle TIC[5].
3. La proposta di modifica della direttiva NIS 2 si concentra in particolare sul terzo obiettivo, introducendo chiarimenti e semplificando la conformità alle norme per i soggetti regolamentati[6].

[1] COM(2026) 11 final.
[2] COM(2026) 13 final.
[3] 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).
[4] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza") (GU L 151 del 7.6.2019, pag. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj), quale modificato dal regolamento (UE) 2025/37 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti (GU L, 2025/37, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/37/oj).
[5] Relazione, COM(2026) 11 final, pag. 1.
[6] COM(2026) 13 final.

4. L'obiettivo del presente parere congiunto è affrontare gli aspetti pertinenti delle proposte che rivestono particolare importanza per la tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali.

2 OSSERVAZIONI GENERALI

5. La proposta di regolamento sulla cibersicurezza 2 mira ad ampliare il mandato dell'ENISA e a renderla più operativa. L'EDPB e il GEPD sostengono il rafforzamento del ruolo dell'ENISA e l'obiettivo di facilitare la diffusione della certificazione della cibersicurezza, nel rispetto delle raccomandazioni specifiche fornite di seguito.

6. L'EDPB e il GEPD accolgono inoltre con favore l'obiettivo di stabilire meccanismi e condizioni nella direttiva (UE) 2022/2555[7] (in appresso "direttiva NIS 2") per contribuire a facilitare la conformità ai requisiti di cibersicurezza, rendendo in tal modo la loro attuazione più coerente ed efficace, nonché l'obiettivo di affrontare ulteriormente i vari rischi per le catene di approvvigionamento delle TIC, compresi quelli di natura non tecnica.

7. Come già affermato nel loro parere congiunto sulla proposta "omnibus digitale"[8], l'EDPB e il GEPD sostengono fermamente l'obiettivo di istituire un punto di accesso unico per la segnalazione delle violazioni dei dati personali, in quanto ciò ridurrebbe gli oneri amministrativi per le organizzazioni senza incidere sul livello di protezione degli interessati.

8. L'articolo 5, paragrafo 1, lettera f), del regolamento (UE) 2016/679 (GDPR) stabilisce la sicurezza come uno dei principi fondamentali relativi al trattamento dei dati personali. L'articolo 32 GDPR definisce ulteriormente tale obbligo, applicabile sia ai titolari che ai responsabili del trattamento, al fine di garantire un adeguato livello di sicurezza. Entrambe le disposizioni chiariscono che la sicurezza del trattamento dei dati personali è essenziale per il rispetto del diritto dell'UE in materia di protezione dei dati.

9. Il rapporto tra protezione dei dati e cibersicurezza è ambivalente. Da un lato, la cibersicurezza contribuisce alla protezione dei dati personali limitando i rischi di accesso indesiderato, modifica o indisponibilità dei dati. Dall'altro, alcune misure di cibersicurezza possono interferire con i diritti e le libertà delle persone, in particolare i diritti alla vita privata e alla protezione dei dati[9].

10. L'EDPB e il GEPD ricordano che il considerando 49 GDPR riconosce che le misure di cibersicurezza che comportano il trattamento di dati personali costituiscono un legittimo interesse del titolare del trattamento interessato, sottolineando nel contempo che le misure dovrebbero essere strettamente necessarie e proporzionate per garantire la sicurezza delle reti e dell'informazione. Pertanto le misure di cibersicurezza dovrebbero non solo essere guidate da considerazioni di efficacia, ma anche valutare se il loro impatto sui diritti fondamentali resti limitato a quanto necessario e proporzionato.

[7] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).
[8] Parere congiunto 2/2026 dell'EDPB e del GEPD sulla proposta di regolamento per quanto riguarda la semplificazione del quadro legislativo nel settore digitale (omnibus digitale), adottato il 10 febbraio 2026.
[9] Cfr. parere del GEPD 5/2021 sulla strategia in materia di cibersicurezza e sulla direttiva NIS 2.0, 11 marzo 2021, punti 10-11, parere del GEPD 7/2022 sulla proposta di regolamento sulla sicurezza delle informazioni nelle istituzioni, negli organi e negli organismi dell'Unione, 17 maggio 2022, punti 9-10, e parere del GEPD 2/2024 sulla proposta di regolamento che modifica il regolamento sulla cibersicurezza per quanto riguarda i servizi di sicurezza gestiti, 10 gennaio 2024, punto 5.

3 SOSTEGNO DELL'ENISA ALL'ATTUAZIONE DELLE POLITICHE E DELLA NORMATIVA DELL'UNIONE E ALLA COOPERAZIONE CON ALTRI SOGGETTI DELL'UNIONE

11. A norma dell'articolo 5, paragrafo 1, della proposta di regolamento sulla cibersicurezza 2, l'ENISA contribuisce all'attuazione delle politiche e della normativa dell'Unione in una serie di settori, fornendo sostegno ai diversi portatori di interessi elencati in tale articolo.

12. Tra questi settori, in linea con l'articolo 5, paragrafo 1, lettera h), della proposta di regolamento sulla cibersicurezza 2, l'ENISA fornirebbe, su richiesta del comitato europeo per la protezione dei dati, consulenza sull'attuazione di aspetti specifici relativi alla cibersicurezza delle politiche e del diritto dell'Unione in materia di protezione dei dati e della vita privata. L'EDPB e il GEPD osservano che l'articolo 5, paragrafo 1, lettera h), della proposta di regolamento sulla cibersicurezza 2 non è una disposizione completamente nuova. L'articolo 5, paragrafo 5, lettera c), dell'attuale regolamento sulla cibersicurezza già prevede che l'ENISA possa sostenere "gli Stati membri nell'attuazione di aspetti specifici relativi alla cibersicurezza della politica e del diritto dell'Unione in materia di protezione dei dati e vita privata, anche fornendo su richiesta un parere al comitato europeo per la protezione dei dati".

13. L'EDPB e il GEPD accolgono con favore il fatto che la proposta di regolamento sulla cibersicurezza 2 fornirebbe ulteriori chiarimenti sulle modalità di cooperazione, mantenendo nel contempo gli elementi fondamentali dell'articolo 5, paragrafo 5, lettera c), del regolamento sulla cibersicurezza. Il nuovo articolo 5, paragrafo 1, lettera h), chiarirebbe che l'EDPB, in quanto organismo dell'Unione, ha il diritto di chiedere direttamente la consulenza dell'ENISA (senza che ciò sia collegato all'attuazione da parte degli Stati membri di aspetti specifici relativi alla cibersicurezza della politica e del diritto dell'Unione in materia di protezione dei dati e vita privata).

14. Allo stesso tempo l'EDPB e il GEPD raccomandano di aggiungere anche il GEPD come possibile soggetto richiedente all'articolo 5, paragrafo 1, lettera h), del regolamento sulla cibersicurezza 2, in considerazione del suo ruolo di autorità di controllo per il trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione europea. Consentire sia all'EDPB che al GEPD di avvalersi della competenza tecnica dell'ENISA nel settore della cibersicurezza può contribuire a garantire che i loro orientamenti e le loro decisioni nel settore della protezione dei dati si basino sulle conoscenze più avanzate in materia di cibersicurezza. Vi potrebbero essere diversi temi per i quali la consulenza e la cooperazione potrebbero essere vantaggiose, tra cui le norme e le pratiche operative in materia di cibersicurezza, nonché l'uso delle tecnologie di rafforzamento della tutela della vita privata (PET) nel contesto della cibersicurezza.

15. L'EDPB e il GEPD sostengono fermamente che la consulenza di cui all'articolo 5, paragrafo 1, lettera h), del regolamento sulla cibersicurezza 2 sia fornita solo previa richiesta dell'EDPB o, come qui proposto, del GEPD. Prevedendo che l'ENISA agisca solo su richiesta dell'EDPB o del GEPD, l'articolo 5, paragrafo 1, lettera h), garantirebbe un chiaro coordinamento e una chiara ripartizione delle responsabilità[10].

[10] Contemplando il coinvolgimento dell'ENISA su richiesta delle autorità di controllo, si mantiene un processo consultivo strutturato, in cui l'ENISA fornisce competenze tecniche, mentre dette autorità mantengono il pieno controllo sulle decisioni relative alla protezione dei dati. Si garantisce inoltre che qualsiasi intervento dell'ENISA sia coordinato e che l'EDPB o il GEPD assumano un ruolo guida e determinino la linea d'azione appropriata. Il rispetto dei ruoli stabiliti promuove la coerenza, evita la frammentazione normativa e rafforza la responsabilità degli organismi di protezione dei dati nel loro ruolo di controllo.

16. L'EDPB e il GEPD osservano che l'articolo 5, paragrafo 1, lettera h), della proposta di regolamento sulla cibersicurezza 2 sembra costituire una manifestazione specifica dell'obbligo più generale di cooperazione sancito dall'articolo 68 della medesima proposta, che disciplina la cooperazione dell'ENISA con altri soggetti dell'Unione. A norma dell'articolo 68, l'ENISA coopera su questioni relative alla cibersicurezza con altri organismi dell'UE, tra cui il comitato europeo per la protezione dei dati, per garantire coerenza, creare sinergie e affrontare questioni di interesse comune. Tale cooperazione può essere assicurata tramite lo scambio di know-how e migliori pratiche; la fornitura di consulenza e l'emanazione di orientamenti su questioni relative alla cibersicurezza; e la definizione di disposizioni pratiche per l'esecuzione di compiti specifici, previa consultazione della Commissione.

17. L'EDPB e il GEPD accolgono con favore la cooperazione e le sinergie tra l'ENISA e altri soggetti dell'Unione, in linea con i rispettivi compiti e mandati. In questo contesto, per motivi di chiarezza giuridica, l'EDPB e il GEPD raccomandano di modificare l'articolo 68 della proposta di regolamento sulla cibersicurezza 2 aggiungendo un riferimento esplicito anche al GEPD in quanto organismo dell'Unione con cui l'ENISA coopererebbe[11].

4 COOPERAZIONE OPERATIVA, CONOSCENZA SITUAZIONALE CONDIVISA IN MATERIA DI CIBERSICUREZZA E PROTEZIONE DEI DATI PERSONALI

18. Ai sensi degli articoli 10 e 11 della proposta di regolamento sulla cibersicurezza 2, che costituirebbero un ulteriore sviluppo dell'attuale articolo 7 del regolamento sulla cibersicurezza, l'ENISA amplierebbe il suo ruolo di polo centrale per la cooperazione operativa, compreso il trattamento di quantità sostanziali di informazioni di intelligence sulle minacce[12]. Pertanto si potrebbe dedurre che le informazioni trattate dall'ENISA nell'ambito del suo ruolo possono includere dati personali, quali indirizzi IP, credenziali e registri degli utenti, scambi finanziari o dettagli di account compromessi.

19. A seguito dei chiarimenti forniti dalla Commissione europea[13], l'EDPB e il GEPD ritengono che nessun trattamento su larga scala di dati personali da parte dell'ENISA debba intendersi quale prescritto e autorizzato dal regolamento sulla cibersicurezza 2[14].

[11] L'EDPB e il GEPD ritengono che l'articolo 7, paragrafo 2, dell'attuale regolamento sulla cibersicurezza, che impone all'ENISA di cooperare a livello operativo e di stabilire sinergie con le istituzioni, gli organi e gli organismi dell'Unione, tra cui le autorità di vigilanza che si occupano della tutela della vita privata e della protezione dei dati personali, al fine di affrontare questioni di interesse comune, già si estenda al GEPD.

[12] Cfr. COM(2026) 11 final, scheda finanziaria e digitale legislativa, pag. 21: "I nuovi elementi/compiti previsti nella proposta apporteranno un valore aggiunto ai portatori di interessi europei, che trarranno vantaggio dal ruolo svolto dall'ENISA in quanto polo d'informazione che contribuisce alla condivisione delle informazioni e fornisce notifiche di allerta ai soggetti pertinenti" e pag. 101: "Negli ultimi anni l'ENISA è diventata un polo di informazione, presso il quale sono disponibili informazioni provenienti da diverse fonti. In tal senso, molti dei compiti dell'ENISA sono associati al riutilizzo e al riciclo delle informazioni per scopi legati a diverse analisi".

[13] Forniti nell'ambito di una riunione ad hoc del sottogruppo di esperti tecnologici dell'EDPB tenutasi il 27 febbraio 2026.

[14] La Commissione ha chiarito che l'ENISA non ha alcun mandato per effettuare analisi operative degli incidenti e non ha accesso ai dati relativi agli incidenti stessi. Piuttosto, i dati trattati saranno aggregati. Le allerte dei CSIRT nazionali non includeranno di norma dati personali operativi, bensì piuttosto dati amministrativi come le informazioni di contatto. Nella stessa ottica, anche le imprese che si iscrivono per ricevere allerte precoci potrebbero fornire le loro informazioni di contatto. Secondo la Commissione europea, nel caso raro in cui le informazioni aggregate su minacce o incidenti fornite all'ENISA contengano indirizzi IP, l'ENISA non avrebbe alcuna necessità operativa e di conseguenza alcuna possibilità giuridica e fattuale di indagare sull'abbonato che si cela dietro un indirizzo IP. La Commissione europea chiarisce inoltre che l'helpdesk di cui all'articolo 13 ha carattere consultivo e fornisce, ad esempio, informazioni sull'autorità competente dello Stato membro da contattare.

Pur prendendo atto del fatto che l'ENISA raccoglierebbe e tratterebbe ulteriormente dati per lo più non personali e aggregati, l'EDPB e il GEPD ricordano tuttavia che se i futuri compiti dell'ENISA in quanto polo di informazione richiedessero un trattamento sostanziale dei dati personali, ciò dovrebbe essere esplicitato nelle disposizioni dell'atto di base che disciplinano i rispettivi compiti, specificando anche gli elementi essenziali di qualsiasi trattamento su larga scala e le garanzie adeguate. Per contro, se l'obiettivo è consentire all'ENISA di raccogliere e trattare ulteriormente dati per lo più non personali e aggregati, anche ciò dovrebbe essere chiarito, almeno mediante un considerando.

20. L'EDPB e il GEPD osservano che l'ENISA continuerebbe a trattare i dati personali per finalità amministrative[15]. L'articolo 66, paragrafo 1, della proposta di regolamento sulla cibersicurezza 2, analogamente all'attuale regolamento sulla cibersicurezza[16], contiene un riferimento generale alla legislazione applicabile in materia di protezione dei dati, ossia l'EUDPR, senza fornire ulteriori norme specifiche.

21. In modo analogo, l'articolo 66, paragrafo 2, della proposta di regolamento sulla cibersicurezza 2 riprende l'attuale articolo 41, paragrafo 2, del regolamento sulla cibersicurezza, che prevede la possibilità per il consiglio di amministrazione dell'ENISA di adottare "misure aggiuntive necessarie per l'applicazione del regolamento (UE) 2018/1725" da parte dell'Agenzia[17], senza l'obbligo per il consiglio di amministrazione di intraprendere alcuna azione specifica. La disposizione di cui all'articolo 66, paragrafo 2, della proposta di regolamento sulla cibersicurezza 2 non specifica l'ambito di applicazione e il tipo di tali misure aggiuntive di protezione dei dati, né la procedura applicabile per la loro adozione. Inoltre non chiarisce il ruolo del GEPD in questo processo[18].

22. L'EDPB e il GEPD ritengono che, se il consiglio di amministrazione dell'ENISA procede all'applicazione dell'articolo 66, paragrafo 2, della proposta di regolamento sulla cibersicurezza 2, le sue decisioni dovrebbero fornire ulteriori dettagli sul modo in cui l'ENISA effettua il trattamento dei dati personali.

23. L'EDPB e il GEPD ricordano che, in linea di principio, solo i dettagli molto tecnici (pratici) relativi al trattamento dei dati personali dovrebbero essere decisi nell'ambito dell'autonomia amministrativa dell'organismo dell'UE interessato, ossia, in questo caso, il consiglio di amministrazione di un'agenzia decentrata. Ciò perché autorizzare le ingerenze nei diritti fondamentali dovrebbe essere una questione meglio riservata alla competenza del legislatore e, al massimo, della Commissione mediante atti di esecuzione o atti delegati[19]. Pertanto ciò che si intende esattamente con la seconda frase del progetto di articolo 66, paragrafo 2, per "misure aggiuntive necessarie per l'applicazione del regolamento (UE) 2018/1725 da parte dell'ENISA", dovrebbe essere chiarito esplicitamente nella disposizione attuativa del regolamento.

---

[15] Ad esempio, nel processo di esame delle domande per ottenere l'autorizzazione come fornitore di attestati nell'ambito del sistema europeo di attestazione delle competenze individuali in materia di cibersicurezza (articolo 22), durante la procedura di ricorso contro le decisioni adottate (articoli 36 e seguenti), nel trattamento dei reclami delle persone fisiche o giuridiche in relazione alla certificazione o alle dichiarazioni UE di conformità (articolo 88, paragrafo 6, lettera h)) o in relazione alle certificazioni di cibersicurezza (articolo 96).

[16] Cfr. articolo 41, paragrafo 1, del regolamento (UE) 2019/881.

[17] Il 21 novembre 2019 il consiglio di amministrazione dell'ENISA ha adottato, a norma dell'articolo 25 EUDPR, la decisione sulle norme interne relative alle limitazioni di determinati diritti degli interessati in relazione al trattamento dei dati personali nell'ambito del funzionamento dell'ENISA.

[18] Ad esempio, l'articolo 18 bis, paragrafo 5, del regolamento (UE) 2016/794 (regolamento Europol) prevede che il consiglio di amministrazione di Europol, su proposta del direttore esecutivo e **previa consultazione del GEPD**, specifichi le condizioni relative alla fornitura e al trattamento di dati personali [...] (grassetto aggiunto).

[19] Cfr. gli orientamenti del GEPD per i colegislatori sugli elementi chiave delle proposte legislative, disponibili all'indirizzo https://www.edps.europa.eu/system/files/2025-05/EDPS_Publication_Guidance_for_co-legislators_EN.pdf, punto 76.

24. Tuttavia se si ritiene necessario che il consiglio di amministrazione adotti misure che vadano oltre le modalità tecniche (pratiche) di trattamento già previste dalla legislazione o dagli atti delegati o di esecuzione, oltre a definirne più chiaramente l'ambito di applicazione, le misure che devono essere adottate dal consiglio di amministrazione dovrebbero essere chiare e precise e la loro applicazione dovrebbe essere prevedibile per le persone interessate. Ciò significa anche dare un'adeguata pubblicità a tali norme. Queste dovrebbero inoltre prevedere le garanzie necessarie per assicurare il rispetto dei principi e delle garanzie fondamentali in materia di protezione dei dati, quali la limitazione delle finalità, la limitazione della conservazione, la protezione dei dati fin dalla progettazione e per impostazione predefinita. Inoltre, come importante garanzia supplementare in tali casi, l'EDPB e il GEPD raccomandano che l'articolo 66 della proposta di regolamento sulla cibersicurezza 2 preveda una consultazione preventiva con il GEPD prima dell'adozione di tali norme[20].

5 PUNTO DI ACCESSO UNICO PER LA SEGNALAZIONE DI INCIDENTI (ARTICOLO 15 DEL REGOLAMENTO SULLA CIBERSICUREZZA 2)

25. A norma dell'articolo 15 della proposta di regolamento sulla cibersicurezza 2, l'ENISA deve istituire, fornire, gestire, mantenere e aggiornare, se necessario, tra l'altro, la piattaforma unica di segnalazione istituita a norma dell'articolo 16, paragrafo 1, del regolamento (UE) 2024/2847 e il punto di accesso unico per la segnalazione degli incidenti istituito a norma dell'articolo 23 bis della direttiva (UE) 2022/2555. Tali strumenti mirano a semplificare i diversi obblighi di segnalazione relativi alla cibersicurezza[21].

26. Come già affermato nel loro parere congiunto sulla proposta "omnibus digitale"[22], l'EDPB e il GEPD sostengono fermamente l'obiettivo di istituire un punto di accesso unico per la segnalazione delle violazioni dei dati personali, in quanto ciò ridurrebbe gli oneri amministrativi per le organizzazioni senza incidere sul livello di protezione degli interessati. Nella sua dichiarazione di Helsinki[23], l'EDPB aveva già sottolineato il proprio sostegno a un'eventuale soluzione di segnalazione europea inter-normativa, in quanto ciò contribuirebbe a facilitare la conformità al GDPR. L'EDPB e il GEPD ricordano inoltre l'importanza di garantire la sicurezza delle notifiche presentate e trasmesse attraverso il punto di accesso unico, in quanto le notifiche di violazione dei dati spesso comprendono informazioni sensibili[24].

[20] Analogamente a quanto previsto dall'articolo 18 bis, paragrafo 5, del regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI (regolamento Europol) (GU L 135 del 24.5.2016, pag. 53).
[21] Cfr. articolo 16, paragrafo 1, del regolamento (UE) 2024/2847 e COM(2025) 837 final, pag. 9.
[22] Parere congiunto 2/2026 dell'EDPB e del GEPD sulla proposta di regolamento per quanto riguarda la semplificazione del quadro legislativo nel settore digitale (omnibus digitale), adottato il 10 febbraio 2026.
[23] EDPB, Dichiarazione di Helsinki sul rafforzamento della chiarezza, del sostegno e dell'impegno - Un approccio all'innovazione e alla competitività basato sui diritti fondamentali, adottata il 2 luglio 2025.
[24] Cfr. capitolo 8.3. del parere congiunto 2/2026 dell'EDPB e del GEPD sulla proposta di regolamento per quanto riguarda la semplificazione del quadro legislativo nel settore digitale (omnibus digitale), adottato il 10 febbraio 2026.

6 QUADRO EUROPEO DELLE COMPETENZE IN MATERIA DI CIBERSICUREZZA ("ECSF") (ARTICOLO 19 DEL REGOLAMENTO SULLA CIBERSICUREZZA 2)

27. L'articolo 19 della proposta di regolamento sulla cibersicurezza 2 imporrebbe all'ENISA di sviluppare e rendere pubblicamente disponibile un quadro europeo delle competenze in materia di cibersicurezza ("ECSF"). L'ECSF contribuirebbe a garantire che i professionisti della cibersicurezza, i datori di lavoro, gli erogatori di istruzione e le autorità pubbliche di tutti gli Stati membri abbiano un'interpretazione condivisa delle competenze specifiche richieste per i posti di lavoro nel settore della cibersicurezza. Il quadro sosterrebbe profili professionali chiari, requisiti di qualifica trasparenti e un migliore allineamento tra l'istruzione e le esigenze del mercato del lavoro. L'ENISA utilizzerebbe l'ECSF come base per fornire formazione, in particolare per sostenere l'attuazione della legislazione dell'UE in materia di cibersicurezza, la cooperazione operativa tra gli Stati membri e le attività di sensibilizzazione. Ciò significa che l'ECSF fungerebbe da base per programmi strutturati di formazione in materia di cibersicurezza, in particolare per le autorità pubbliche e i soggetti disciplinati dalla normativa dell'UE in materia di cibersicurezza.

28. L'EDPB e il GEPD accolgono con favore l'obiettivo di potenziare la forza lavoro nel settore della cibersicurezza dell'UE e sottolineano che rendere le competenze più trasferibili e riconoscibili a livello transfrontaliero è importante per il funzionamento del mercato unico digitale.

29. Allo stesso tempo rilevano che i profili definiti all'articolo 19, paragrafo 2, della proposta di regolamento sulla cibersicurezza 2 sono attualmente limitati ai professionisti della cibersicurezza. La proposta non prevede un profilo delle competenze necessarie per i cittadini, i funzionari pubblici o i membri non specializzati della forza lavoro. Come riconosciuto nel considerando 21 della proposta di regolamento sulla cibersicurezza 2, l'alfabetizzazione digitale è essenziale per l'emancipazione di cittadini resilienti; tuttavia quasi la metà della popolazione adulta non dispone delle competenze digitali di base, nonostante oltre il 90 % dei posti di lavoro le richieda. Pertanto l'ECSF dovrebbe includere il profilo "cibersicurezza per i generalisti", che contempli le competenze minime che ogni residente dell'UE in età lavorativa dovrebbe possedere per interagire in modo sicuro all'interno del mercato unico digitale, proteggendo non solo sé stesso, ma anche la sua organizzazione e altri soggetti, in particolare per quanto riguarda il phishing assistito dall'IA, i deepfake, l'usurpazione di identità e gli attacchi di ingegneria sociale. Tale profilo potrebbe essere utilizzato da organizzazioni pubbliche o private per la formazione del loro personale al fine di ridurre al minimo i rischi derivanti dal fattore umano, riducendo così il rischio complessivo di violazioni dei dati.

30. L'EDPB e il GEPD osservano che il considerando 45 della proposta distingue esplicitamente l'ECSF dal quadro europeo delle competenze digitali (DigComp 3.0), chiarendo che quest'ultimo riguarda la vita quotidiana, la partecipazione alla società, il lavoro e l'apprendimento e può essere utilizzato sia dagli adulti che dai bambini[25], mentre l'ECSF si rivolge a un pubblico specializzato, offrendo un quadro semplice che individua i ruoli attinenti alla cibersicurezza e i compiti, le conoscenze e le competenze associati necessari per svolgerli.

31. L'EDPB e il GEPD sostengono tutte le iniziative menzionate, siano esse attuate dall'ENISA o, nel caso del DigComp, dal Centro comune di ricerca (JRC) della Commissione europea, in quanto ridurrebbero il rischio di violazioni dei dati, purché diffuse in modo sufficiente. Invitano pertanto tutte le parti coinvolte a esaminare modalità per aumentare l'impatto dei quadri.

32. Allo stesso tempo l'EDPB e il GEPD ritengono che il DigComp non possa sostituire un sistema di cibersicurezza specifico per i generalisti[26] e raccomandano ai colegislatori di modificare l'articolo 19, paragrafo 2, della proposta di regolamento sulla cibersicurezza 2 affinché l'ECSF non si limiti esclusivamente ai "professionisti della cibersicurezza", ma includa anche profili per la forza lavoro in generale o per i cittadini. Ciò dovrebbe essere accompagnato da una corrispondente modifica al considerando 45.

33. L'EDPB e il GEPD ritengono inoltre che i profili professionali dell'ECSF dovrebbero integrare un modulo sulla necessità di garantire la conformità delle misure di cibersicurezza al diritto dell'UE in materia di protezione dei dati, in particolare per quanto riguarda l'attuazione pratica del principio della protezione dei dati fin dalla progettazione e per impostazione predefinita (articolo 25 GDPR), e invitano il colegislatore ad aggiungere un considerando a tal fine.

7 QUADRO EUROPEO DI CERTIFICAZIONE DELLA CIBERSICUREZZA (TITOLO III)

[25] L'EDPB e il GEPD ricordano inoltre che tra il 2022 e il 2024 la Commissione europea ha esaminato lo sviluppo di un certificato europeo delle competenze digitali (EDSC), basato sul DigComp. Il certificato aiuterebbe le persone a ottenere rapidamente e facilmente il riconoscimento delle loro competenze digitali da parte dei datori di lavoro, degli erogatori di istruzione e di altri soggetti. L'iniziativa era intesa a offrire un marchio di qualità per la certificazione delle competenze digitali in tutta Europa. A seguito di uno studio di fattibilità (cfr. CENTENO, C., COSGROVE, J., CACHIA, R., MORA, T., DI LEGGE, A., VIVARELLI, S., BULIAN, G., MOYES PRELLEZO, N., PIÑA DE SANTISTEBAN, P., SCHULZ, C., HÜSING, T., CUARTAS-ACOSTA, A. e TROIA, S., *European Digital Skills Certificate (EDSC) Feasibility Study*, Ufficio delle pubblicazioni dell'Unione europea, Lussemburgo, 2024, doi:10.2760/958195, JRC138344, https://publications.jrc.ec.europa.eu/repository/handle/JRC138344) e di un progetto pilota con diversi paesi dell'UE, la Commissione europea ha concluso che tale marchio di qualità non apporterebbe un valore aggiunto sufficiente ai cittadini europei. In ogni caso, il DigComp, pubblicato per la prima volta nel 2013, esiste ancora (COSGROVE, J. e CACHIA, R., *DigComp 3.0: European Digital Competence Framework - Fifth Edition*, Ufficio delle pubblicazioni dell'Unione europea, Lussemburgo, 2025, https://data.europa.eu/doi/10.2760/0001149, JRC144121). Descrive ciò che è necessario per avere competenze digitali nella società odierna e sostiene lo sviluppo delle competenze digitali tra le persone di tutte le età. Copre un'ampia gamma di livelli di competenze, da quelle di base a quelle altamente avanzate. Diverse competenze nel DigComp fanno esplicito riferimento alla cibersicurezza, tra cui "4.1 Protezione dei dispositivi", "4.2 Protezione dei dati personali e della vita privata" e persino "4.4 Protezione dell'ambiente (prevenzione della fuga di dati dalle apparecchiature fuori uso)". Anche altri settori riguardano le competenze pertinenti, tra cui le competenze fondamentali per difendersi dall'ingegneria sociale (settore 1), per ridurre i rischi di minacce interne e impedire la divulgazione accidentale di informazioni (settore 2) e per migliorare la velocità di rilevamento degli incidenti (settore 5).

[26] Nel DigComp, il contenuto di sicurezza è distribuito in 21 competenze, non fornisce modelli espliciti di minaccia, non rende operativi i rischi per la sicurezza a livello organizzativo e non effettua una mappatura diretta degli obblighi di conformità. Sebbene l'ECSF, nella sua forma attuale, si applichi alle competenze dei professionisti della cibersicurezza, manca un quadro strutturato a livello dell'UE per i dipendenti non addetti alla cibersicurezza. L'EDPB e il GEPD ricordano che la maggior parte delle violazioni deriva dal phishing, dall'ingegneria sociale, dall'uso improprio delle credenziali, dalla configurazione errata e dall'uso del "sistema informatico ombra" (*shadow IT*). Trattasi di comportamenti generalisti. Un quadro di cibersicurezza generalista potrebbe rendere espliciti i rischi, fornire aspettative basate sui ruoli (ad esempio per le risorse umane e finanziarie) e sostenere risultati misurabili.

34. L'articolo 71 e l'articolo 80, paragrafo 1, lettera w), della proposta di regolamento sulla cibersicurezza 2 disciplinano l'ambito di applicazione della certificazione della cibersicurezza. L'articolo 80, paragrafo 1, lettera w), aggiunge, quale obiettivo di sicurezza dei sistemi europei di certificazione della cibersicurezza, "provvedere affinché il soggetto sia in grado di garantire la sicurezza del trattamento dei dati personali".

35. L'EDPB e il GEPD osservano che la formulazione dell'articolo 80, paragrafo 1, lettera w), della proposta di regolamento sulla cibersicurezza 2 è molto vicina alle prescrizioni dettate dal GDPR in materia di sicurezza del trattamento[27]. In tal senso, l'ambito di applicazione del nuovo sistema di certificazione potrebbe essere interpretato come comprendente le prescrizioni di cui al GDPR. L'ambito di applicazione giuridico e operativo non è però del tutto chiaro, in quanto l'articolo in questione non rimanda alle disposizioni del GDPR (ad esempio l'articolo 5, paragrafo 1, lettera f), gli articoli 32 e 25 GDPR) ed è inserito in un elenco di "obiettivi di sicurezza" (articolo 80, paragrafo 1, prima frase).

36. L'EDPB e il GEPD ricordano che la sicurezza ai sensi del GDPR riguarda i rischi per i diritti e le libertà fondamentali delle persone fisiche. Sebbene la definizione giuridica di cibersicurezza ai sensi del diritto dell'Unione includa ampiamente la protezione degli utenti e di altre persone[28], l'ambito di applicazione delle misure di cibersicurezza comprende generalmente rischi di tutti i tipi per l'organizzazione interessata. Vi è comunque l'opportunità di creare sinergie in modo che la valutazione dei rischi possa integrare la protezione dei diritti e delle libertà delle persone.

37. L'EDPB e il GEPD ricordano inoltre che il GDPR dispone di un proprio meccanismo di certificazione (articoli da 42 a 43 GDPR) e ritengono che la certificazione della cibersicurezza sia distinta dalla certificazione della protezione dei dati a norma dell'articolo 42 GDPR.

38. Ciò detto, l'EDPB e il GEPD sono dell'avviso che possano esistere sinergie tra la certificazione della cibersicurezza e la certificazione della protezione dei dati. Ad esempio, la certificazione prevista dal regolamento sulla cibersicurezza 2 potrebbe essere utilizzata come prova del fatto che alcune prescrizioni di una certificazione a norma del GDPR sono soddisfatte per quanto riguarda la cibersicurezza. L'EDPB e il GEPD osservano tuttavia che l'articolo 80, paragrafo 1, lettera w), della proposta di regolamento sulla cibersicurezza 2 non definisce chiaramente il rapporto con la certificazione di cui agli articoli 42 e 43 GDPR. Nell'interesse della certezza del diritto, l'EDPB e il GEPD raccomandano di chiarire ulteriormente l'ambito di applicazione dell'articolo 80, paragrafo 1, lettera w), del regolamento sulla cibersicurezza 2 e il rapporto con la certificazione a norma del GDPR. L'EDPB e il GEPD raccomandano inoltre di imporre all'ENISA di consultarsi con l'EDPB prima di adottare un sistema di certificazione a norma dell'articolo 80, paragrafo 1, lettera w), del regolamento sulla cibersicurezza 2, al fine di garantire la coerenza.

[27] Cfr. articolo 5, paragrafo 1, lettera f), e articolo 32 GDPR.

[28] Cfr. articolo 2, punto 1), della proposta di regolamento sulla cibersicurezza 2, che è una disposizione preesistente e recita: ""cibersicurezza": l'insieme delle attività necessarie per proteggere i sistemi informativi e di rete, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche".

39. L'EDPB e il GEPD sottolineano la necessità di considerare non solo l'efficacia delle misure di cibersicurezza, ma anche la loro necessità e proporzionalità. Alcuni controlli di cibersicurezza pongono rischi specifici per la protezione dei dati. Ciò può verificarsi con il monitoraggio e la registrazione, l'ispezione approfondita dei pacchetti o l'analisi del comportamento degli utenti. Un sistema di certificazione ben concepito per la sicurezza del trattamento potrebbe includere controlli volti a garantire che le misure di sicurezza possano essere attuate in modo conforme alle norme in materia di protezione dei dati (ad esempio, alcuni aspetti dovrebbero essere configurabili, tra cui, ad esempio, la granularità dei dati registrati a fini di sicurezza, in quanto ciò può consentire o agevolare il rispetto da parte del titolare del trattamento dei principi di sicurezza e minimizzazione dei dati di cui al GDPR; in modo analogo, i periodi di conservazione dovrebbero essere configurabili in modo che il titolare del trattamento possa decidere, nell'ambito del trattamento interessato, per quanto tempo i dati personali debbano essere conservati prima di essere cancellati o anonimizzati utilizzando tecniche certificate).

40. L'EDPB e il GEPD raccomandano pertanto di specificare in un considerando che i sistemi di certificazione dovrebbero, nella misura del possibile, essere progettati, attuati e mantenuti in modo da tenere conto dei controlli di sicurezza che possono contribuire a dimostrare il rispetto delle prescrizioni del GDPR, laddove i sistemi si applicano a prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti che possono essere utilizzati nell'ambito del trattamento di dati. Va inoltre osservato che alcuni controlli possono essere fattori abilitanti per la tutela della vita privata e la protezione dei dati fin dalla progettazione e per impostazione predefinita.

8 QUADRO PER CATENE DI APPROVVIGIONAMENTO DELLE TIC AFFIDABILI (TITOLO IV)

41. La proposta di regolamento sulla cibersicurezza 2 aggiunge misure per la sicurezza delle catene di approvvigionamento delle TIC, affrontando in particolare i rischi di natura non tecnica quali i fattori geopolitici, giuridici, di proprietà, di dipendenza e di interferenza strategica che incidono sulle catene di approvvigionamento delle TIC nei settori ad alta criticità e in altri settori critici. Sebbene mirino principalmente ad affrontare rischi che non sono direttamente connessi alla protezione dei dati, tali misure per la sicurezza delle catene di approvvigionamento possono anche avere un impatto positivo sulla protezione dei diritti fondamentali limitando le ingerenze straniere nei dati degli interessati dell'UE attraverso attività quali lo spionaggio e la sorveglianza.

42. L'EDPB e il GEPD accolgono con favore la misura proposta volta a garantire un quadro per catene di approvvigionamento delle TIC affidabili e ad affrontare i rischi di natura non tecnica in settori ad alta criticità.

9 ULTERIORI SOGGETTI ESSENZIALI AI SENSI DELLA PROPOSTA DI MODIFICA DELLA DIRETTIVA NIS 2

43. La proposta di modifica della direttiva NIS 2 include i fornitori di portafogli europei di identità digitale e di portafogli europei delle imprese quali "soggetti essenziali", indipendentemente dalle loro dimensioni. I soggetti classificati come "essenziali" sono tenuti a rispettare tutti gli obblighi di gestione dei rischi di cibersicurezza previsti dalla direttiva NIS 2 e ad attuare le misure di sicurezza di cui all'articolo 21 della medesima direttiva, tra cui politiche di analisi dei rischi e di sicurezza, gestione degli incidenti, continuità operativa e gestione delle crisi, sicurezza della catena di approvvigionamento, gestione delle vulnerabilità, politiche in materia di crittografia e cifratura, controllo dell'accesso e gestione degli attivi.

44. L'EDPB e il GEPD accolgono con favore la designazione dei fornitori di portafogli europei di identità digitale e di portafogli europei delle imprese quali "soggetti essenziali". L'EDPB e il GEPD ritengono che i portafogli di identità digitale siano una componente fondamentale dell'infrastruttura digitale dell'UE e che quindi gli incidenti che li riguardano possano avere un ampio impatto transfrontaliero. Detti portafogli sono alla base dell'identificazione, dell'autenticazione e dello scambio di attestati elettronici in sicurezza. Per l'economia digitale, i portafogli delle imprese sono tanto critici quanto i portafogli europei di identità digitale. Pertanto entrambi i tipi di fornitori di portafogli sono trattati in modo analogo ai prestatori di servizi fiduciari, già designati quali "soggetti essenziali" ai sensi della direttiva NIS 2, e ad altri operatori di infrastrutture altamente critiche.

10 RACCOLTA DI DATI SUGLI ATTACCHI RANSOMWARE

45. A norma dell'articolo 5, paragrafo 8, della proposta di modifica della direttiva NIS 2, che propone di aggiungere i nuovi paragrafi 12 e 13 all'articolo 23 della direttiva NIS 2, in caso di attacco ransomware, ai soggetti interessati può essere chiesto di trasmettere determinate informazioni relative a tali incidenti ai team di risposta agli incidenti di sicurezza informatica (CSIRT), compreso se un soggetto ha pagato un riscatto e, in caso affermativo, quale importo e a chi (prestatori di cripto-attività e di servizi per le cripto-attività) e l'identità della persona che funge da punto di contatto.

46. A norma dell'articolo 23, paragrafo 11, della direttiva NIS 2, alla Commissione è conferito il potere di adottare atti di esecuzione che specifichino ulteriormente il tipo di informazioni, il relativo formato e la procedura degli obblighi di segnalazione. L'ambito di applicazione di tale atto di esecuzione sarebbe esteso per includere anche i nuovi obblighi di segnalazione in caso di attacchi ransomware.

47. L'EDPB e il GEPD sostengono pienamente l'importante obiettivo di prevenire attacchi ransomware futuri e di fermare e smantellare le organizzazioni criminali che ne sono alla base. L'EDPB e il GEPD osservano che le informazioni da condividere in merito agli attacchi ransomware potrebbero essere di natura potenzialmente sensibile, come spiegato ulteriormente dalla Commissione al considerando 10 della proposta di modifica della direttiva NIS 2. Inoltre tali segnalazioni possono comportare il trattamento di dati personali. L'EDPB e il GEPD accolgono con favore l'approccio a più livelli adottato nei paragrafi 12 e 13, secondo il quale le informazioni più sensibili di cui al paragrafo 13 saranno comunicate solo su richiesta.

48. Nel contempo, in considerazione della natura sensibile dei dati segnalati e in linea con i principi di necessità e proporzionalità, nel caso in cui la segnalazione di attacchi ransomware comporti il trattamento di dati personali, l'EDPB e il GEPD raccomandano di specificare nell'atto di esecuzione a norma dell'articolo 23, paragrafo 11, della direttiva NIS 2 le garanzie applicabili in materia di protezione dei dati. A tale riguardo, ricordano inoltre l'obbligo per la Commissione, a norma dell'articolo 42, paragrafo 1, EUDPR, di consultare il GEPD sui progetti di atti delegati e di esecuzione qualora essi incidano sulla tutela dei diritti e delle libertà delle persone in relazione al trattamento dei dati personali.