Consiglio dell'Unione europea

Bruxelles, 17 dicembre 2025
(OR. en)

16960/25

CYBER 389
JAI 1924
DATAPROTECT 345
TELECOM 485
MI 1075
CSC 693
CSCI 284
DELACT 198

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	11 dicembre 2025
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	C(2025) 8407 final
Oggetto:	REGOLAMENTO DELEGATO (UE) …/... DELLA COMMISSIONE del 11.12.2025 che integra il regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio specificando i termini e le condizioni per l'applicazione dei motivi connessi alla cibersicurezza relativamente al ritardo nella diffusione delle notifiche

Si trasmette in allegato, per le delegazioni, il documento C(2025) 8407 final.

All.: C(2025) 8407 final

COMMISSIONE
EUROPEA

Bruxelles, 11.12.2025
C(2025) 8407 final

REGOLAMENTO DELEGATO (UE) …/... DELLA COMMISSIONE

del 11.12.2025

che integra il regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio specificando i termini e le condizioni per l'applicazione dei motivi connessi alla cibersicurezza relativamente al ritardo nella diffusione delle notifiche

(Testo rilevante ai fini del SEE)

RELAZIONE

1. CONTESTO DELL'ATTO DELEGATO

Il regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio ("regolamento sulla ciberresilienza") impone ai fabbricanti di prodotti con elementi digitali di notificare, mediante una piattaforma unica di segnalazione, qualsiasi vulnerabilità attivamente sfruttata o incidente grave che abbia un impatto sulla sicurezza di uno di tali prodotti. A norma dell'articolo 16, paragrafo 2, di tale regolamento, in circostanze eccezionali e per motivi connessi alla cibersicurezza il team di risposta agli incidenti di sicurezza informatica (CSIRT) designato dallo Stato membro come coordinatore che riceve per primo la notifica può ritardarne la diffusione ai CSIRT degli altri Stati membri in cui il prodotto con elementi digitali è stato messo a disposizione.

Il presente atto delegato è pertanto inteso a integrare il regolamento sulla ciberresilienza specificando i termini e le condizioni per l'applicazione di motivi connessi alla cibersicurezza allo scopo di ritardare la diffusione delle notifiche. A tal fine individua tre motivi per cui il CSIRT che ha ricevuto per primo la notifica può decidere che sia necessario ritardare l'ulteriore diffusione ad altri CSIRT. Tale decisione può essere adottata in tre circostanze:

- alla luce di una valutazione della natura delle informazioni notificate;
- se il CSIRT che riceve la notifica non è in grado di garantire la riservatezza di tali informazioni;
- se la piattaforma unica di segnalazione è stata compromessa o è temporaneamente non operativa.

È previsto che gli obblighi di segnalazione di cui all'articolo 14 del regolamento (UE) 2024/2847 si applichino a decorrere dall'11 settembre 2026.

2. CONSULTAZIONI PRECEDENTI L'ADOZIONE DELL'ATTO

La rete di CSIRT e l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) sono state consultate in merito a diversi progetti del presente atto. Il 26 marzo 2025 si è tenuta una discussione preliminare con quesiti orientativi, con l'opportunità di presentare contributi scritti entro l'11 aprile 2025. Un primo progetto del presente atto è stato condiviso con la rete di CSIRT e con l'ENISA il 16 maggio 2025 e il 6 giugno 2025 si è tenuta una discussione, con l'opportunità di presentare contributi scritti entro il 27 giugno 2025. Un secondo progetto del presente atto è stato condiviso con la rete di CSIRT e con l'ENISA il 23 luglio 2025, con l'opportunità di presentare contributi scritti entro il 1º settembre 2025. Un terzo progetto del presente atto è stato condiviso con la rete di CSIRT e con l'ENISA il 25 settembre 2025 e il 9 ottobre 2025 si è tenuta una discussione, con l'opportunità di presentare contributi scritti entro il 27 ottobre 2025.

Il progetto di atto è stato oggetto di una consultazione pubblica svoltasi tra il 16 ottobre 2025 e il 13 novembre 2025, nell'ambito della quale sono state ricevute 34 risposte inviate da 31 singoli rispondenti (tenendo conto del fatto che lo stesso rispondente ha fornito riscontri inviando quattro risposte distinte). Di queste, il 29,41 % proveniva da associazioni d'imprese, il 26,47 % da società/imprese, il 17,65 % da cittadini dell'UE, il 14,71 % da autorità

pubbliche, il 5,88 % da organizzazioni non governative (ONG) e il 5,88 % da istituti accademici/di ricerca[1].

Il 22 ottobre il progetto è stato inoltre discusso con il gruppo di esperti sulla cibersicurezza dei prodotti con elementi digitali (E03967), di cui fanno parte, tra l'altro, le autorità degli Stati membri, l'ENISA, singoli esperti nominati a titolo personale e organizzazioni in senso lato (ad es. società, associazioni ed ONG).

3. ELEMENTI GIURIDICI DELL'ATTO DELEGATO

Il potere di adottare atti delegati è previsto dall'articolo 14, paragrafo 9, del regolamento sulla ciberresilienza, che impone alla Commissione di specificare i termini e le condizioni per l'applicazione dei motivi connessi alla cibersicurezza relativamente al ritardo nella diffusione delle notifiche entro l'11 dicembre 2025.

[1] Queste percentuali non tengono conto del fatto che lo stesso rispondente ha fornito riscontri inviando quattro risposte distinte.

REGOLAMENTO DELEGATO (UE) …/... DELLA COMMISSIONE

del 11.12.2025

che integra il regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio specificando i termini e le condizioni per l'applicazione dei motivi connessi alla cibersicurezza relativamente al ritardo nella diffusione delle notifiche

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza)[2], in particolare l'articolo 14, paragrafo 9,

considerando quanto segue:

(1) In circostanze eccezionali e, in particolare, su richiesta del fabbricante e alla luce del grado di sensibilità delle informazioni notificate, per motivi giustificati connessi alla cibersicurezza, il team di risposta agli incidenti di sicurezza informatica (CSIRT) designato come coordinatore che ha ricevuto per primo la notifica di una vulnerabilità attivamente sfruttata o di un incidente grave che abbia un impatto sulla sicurezza di un prodotto con elementi digitali ("CSIRT che ha ricevuto per primo la notifica") può decidere di ritardare per un periodo di tempo strettamente necessario la diffusione di tale notifica mediante la piattaforma unica di segnalazione ai CSIRT designati come coordinatori sul cui territorio il fabbricante che ha trasmesso la notifica ha indicato che il prodotto con elementi digitali è stato messo a disposizione ("CSIRT pertinenti"). È pertanto necessario stabilire i termini e le condizioni per l'applicazione di tali motivi. Qualora si applichino tali motivi, il CSIRT che ha ricevuto per primo la notifica può ritardare la diffusione ai CSIRT pertinenti per un periodo di tempo strettamente necessario, ma non è tenuto a farlo. A norma dell'articolo 16, paragrafo 2, del regolamento (UE) 2024/2847, se decide di applicare tali motivi il CSIRT che ha ricevuto per primo la notifica deve informare immediatamente l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) della decisione di ritardarne la diffusione e delle ragioni alla base di tale decisione, e indicare quando intende diffondere ulteriormente la notifica.

(2) Conformemente all'articolo 16, paragrafo 2, secondo comma, del regolamento (UE) 2024/2847, i termini e le condizioni per l'applicazione dei motivi connessi alla cibersicurezza stabiliti nel presente regolamento non si applicano all'accesso dell'ENISA alle informazioni notificate. L'accesso dell'ENISA alle informazioni notificate può essere limitato solo in circostanze particolarmente eccezionali: se nella sua notifica il fabbricante indica che è soddisfatta una delle tre condizioni di cui all'articolo 16, paragrafo 2, terzo comma, lettere a), b) o c), del regolamento (UE)

[2] GU L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

2024/2847, e solo in relazione alla notifica delle vulnerabilità entro 72 ore di cui all'articolo 14, paragrafo 2, lettera b), del medesimo regolamento. In tali casi, le uniche informazioni che devono essere rese simultaneamente disponibili all'ENISA sono l'avvenuta notifica da parte del fabbricante, le informazioni generali sul prodotto con elementi digitali, le informazioni sulla natura generale dello sfruttamento e l'informazione che sono stati sollevati motivi di sicurezza.

(3) L'accesso alle informazioni notificate consente ai CSIRT di disporre di una panoramica dell'ambiente di sicurezza sul loro territorio e di attuare misure di attenuazione, aumentando il livello generale di cibersicurezza nell'Unione. L'applicazione di ulteriori restrizioni alla diffusione delle notifiche alla luce della natura delle informazioni notificate dovrebbe pertanto essere possibile solo nei casi in cui, considerata la sensibilità delle informazioni notificate, i rischi di cibersicurezza derivanti dall'ulteriore diffusione superino i benefici in termini di sicurezza per l'Unione, e tali rischi non possano essere adeguatamente attenuati applicando restrizioni al trattamento e all'ulteriore condivisione della notifica attraverso protocolli adeguati in uso all'interno della rete di CSIRT, quali il protocollo del semaforo (*Traffic Light Protocol*, TLP) o il protocollo delle azioni consentite (*Permissible Actions Protocol*, PAP). Ciò potrebbe verificarsi ad esempio nel caso in cui un fabbricante abbia informato il CSIRT che ha ricevuto per primo la notifica di prevedere di fornire a breve una misura di attenuazione (ad esempio una patch). Ciò potrebbe altresì verificarsi nel caso in cui il CSIRT che ha ricevuto per primo la notifica decida di condividere solo parti della notifica, e tali parti siano comunque sufficienti affinché i CSIRT pertinenti siano in grado di adottare adeguate misure di attenuazione dei rischi. Inoltre, al fine di incoraggiare la cooperazione in materia di identificazione e divulgazione delle vulnerabilità tra fabbricanti, CSIRT e ricercatori nel settore della sicurezza, ciò potrebbe verificarsi anche nel caso in cui il CSIRT agisca da intermediario di fiducia in una procedura in corso di divulgazione coordinata delle vulnerabilità, di cui all'articolo 12, paragrafo 1, della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[3]. In tal caso, se decide di ritardare la diffusione di una notifica, e conformemente all'articolo 16, paragrafo 6, del regolamento (UE) 2024/2847, tale CSIRT può ritardare tale diffusione per un periodo non superiore a quello strettamente necessario e fino a quando non sia stato dato il consenso alla divulgazione dalle parti coinvolte nella divulgazione coordinata delle vulnerabilità.

(4) Le informazioni contenute nella notifica aiuteranno i CSIRT a svolgere i loro compiti nel contesto dell'attenuazione dei rischi e della gestione degli incidenti. In rari casi, tuttavia, tali informazioni potrebbero essere sufficienti per consentire la creazione di una tecnica di sfruttamento senza ulteriori ricerche, anche da parte di soggetti con competenze e risorse limitate. Se soggetti malintenzionati dovessero accedere a tali informazioni, la cibersicurezza dell'Unione ne risentirebbe pesantemente, data la facilità di sfruttamento. Ciò potrebbe verificarsi, ad esempio, se la versione vulnerabile di un software differisce solo marginalmente dalle versioni precedenti non vulnerabili. In tali casi, se ritiene che i rischi per la cibersicurezza derivanti dall'ulteriore diffusione non possano essere adeguatamente attenuati applicando restrizioni al trattamento e all'ulteriore condivisione, il CSIRT che ha ricevuto per primo la notifica può decidere

[3] 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) (GU L 333 del 27.12.2022, pag. 80).

di ritardare la diffusione fino a quando non sarà disponibile una misura efficace di attenuazione dei rischi, come un aggiornamento di sicurezza o orientamenti per gli utilizzatori.

(5) Se un CSIRT pertinente non è in grado di proteggere adeguatamente le informazioni notificate, soggetti malintenzionati potrebbero accedere alle informazioni sensibili e mettere in atto sfruttamenti in tutto il mercato unico. Pertanto, qualora sussistano gravi preoccupazioni in merito alla capacità di un CSIRT pertinente di garantire la riservatezza delle informazioni notificate, il CSIRT che ha ricevuto per primo la notifica può decidere di ritardarne la diffusione solo a tale CSIRT pertinente fino a quando tali preoccupazioni non siano state affrontate. Ciò potrebbe succedere in situazioni in cui un CSIRT pertinente è stato vittima di un incidente di cibersicurezza che incide sulla sua capacità di operare in modo sicuro, o in cui vi sono prove o informazioni relative all'individuazione di carenze significative nelle capacità del CSIRT, quali gravi vincoli in termini di risorse che compromettono la sua capacità di svolgere le sue funzioni o il ricorso a software obsoleti o vulnerabili.

(6) Per impedire ai soggetti malintenzionati di accedere a informazioni sensibili, qualora la piattaforma unica di segnalazione istituita a norma dell'articolo 16 del regolamento (UE) 2024/2847 sia stata compromessa da un incidente di cibersicurezza, il CSIRT che ha ricevuto per primo la notifica dovrebbe ritardarne la diffusione attraverso la piattaforma unica di segnalazione fino a quando non sia stata ripristinata la capacità della piattaforma di garantire la riservatezza delle informazioni notificate.

(7) Conformemente all'articolo 16, paragrafo 2, primo comma, del regolamento (UE) 2024/2847, il CSIRT che ha ricevuto per primo la notifica non è tenuto a diffondere una notifica a nessun altro CSIRT pertinente se il fabbricante indica che il prodotto con elementi digitali è messo a disposizione solo sul mercato dello Stato membro del CSIRT che ha ricevuto per primo la notifica.

(8) Nella preparazione del progetto di atto delegato la Commissione ha consultato i portatori di interessi pertinenti e chiesto il loro parere e ha consultato il gruppo di esperti sulla cibersicurezza dei prodotti con elementi digitali.

(9) Conformemente all'articolo 14, paragrafo 9, del regolamento (UE) 2024/2847, nella preparazione del progetto di atto delegato la Commissione ha collaborato strettamente con la rete di CSIRT istituita a norma dell'articolo 15 della direttiva (UE) 2022/2555 e con l'ENISA,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Oggetto

Il presente regolamento specifica i termini e le condizioni per l'applicazione dei motivi connessi alla cibersicurezza di cui all'articolo 16, paragrafo 2, del regolamento (UE) 2024/2847 che consentono al CSIRT designato come coordinatore che ha ricevuto per primo una notifica a norma dell'articolo 14, paragrafi 1 e 3, nonché dell'articolo 15, paragrafi 1 e 2, di tale regolamento di ritardare la diffusione della notifica ai CSIRT designati come coordinatori sul cui territorio il fabbricante ha indicato che il prodotto con elementi digitali è stato messo a disposizione.

Articolo 2

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

(1) "CSIRT che ha ricevuto per primo la notifica": il CSIRT designato come coordinatore che ha ricevuto per primo la notifica a norma dell'articolo 14, paragrafi 1 e 3, e dell'articolo 15, paragrafi 1 e 2, del regolamento (UE) 2024/2847;

(2) "CSIRT pertinente": il CSIRT designato come coordinatore sul cui territorio il fabbricante ha indicato che il prodotto con elementi digitali è stato messo a disposizione.

Articolo 3

Termini e condizioni per l'applicazione dei motivi connessi alla cibersicurezza derivanti dalla natura delle informazioni comunicate

Il CSIRT che ha ricevuto per primo la notifica può decidere di ritardare, per un periodo di tempo limitato allo stretto necessario, la diffusione delle notifiche o di parti di esse ai CSIRT pertinenti nei casi in cui, alla luce della sensibilità delle informazioni notificate, i rischi di cibersicurezza posti dalla diffusione siano superiori ai benefici in termini di sicurezza e tali rischi non possano essere attenuati applicando restrizioni al trattamento o all'ulteriore condivisione della notifica attraverso protocolli adeguati, quali il protocollo del semaforo (*Traffic Light Protocol*, TLP) o il protocollo delle azioni consentite (*Permissible Actions Protocol*, PAP), e qualora sia soddisfatta almeno una delle condizioni seguenti:

(a) il fabbricante ha informato il CSIRT che ha ricevuto per primo la notifica che entro 72 ore è prevista la messa a disposizione di una misura efficace di attenuazione dei rischi, come un aggiornamento di sicurezza o orientamenti per gli utilizzatori; se entro tale termine non è messa a disposizione una misura efficace di attenuazione dei rischi, il CSIRT che ha ricevuto per primo la notifica la diffonde ai CSIRT pertinenti;

(b) le informazioni comprese nella notifica sono ritenute sufficienti, alla luce della natura della vulnerabilità attivamente sfruttata notificata, per creare una tecnica di sfruttamento, in particolare quando la vulnerabilità può essere facilmente individuata e sfruttata da soggetti con competenze e risorse limitate; una volta disponibile una misura efficace di attenuazione dei rischi, come un aggiornamento di sicurezza o orientamenti per gli utilizzatori, il CSIRT che ha ricevuto per primo la notifica la diffonde ai CSIRT pertinenti;

(c) il CSIRT che ha ricevuto per primo la notifica è in grado di condividere con i CSIRT pertinenti informazioni sufficienti a garantire che questi ultimi possano mettere in atto adeguate misure di attenuazione dei rischi; una volta disponibile una misura efficace di attenuazione dei rischi, come un aggiornamento di sicurezza o orientamenti per gli utilizzatori, il CSIRT che ha ricevuto per primo la notifica diffonde la notifica completa ai CSIRT pertinenti;

(d) il CSIRT che ha ricevuto per primo la notifica della vulnerabilità attivamente sfruttata ne è stato informato nell'ambito di una divulgazione coordinata delle vulnerabilità per la quale tale CSIRT agisce in qualità di intermediario di fiducia a norma dell'articolo 12, paragrafo 1, della direttiva (UE) 2022/2555; in tal caso, e conformemente all'articolo 16, paragrafo 6, del regolamento (UE) 2024/2847, il CSIRT che ha ricevuto per primo la notifica la diffonde ai CSIRT pertinenti quando ritardarne la diffusione non è più strettamente necessario ed è stato dato il consenso

alla divulgazione dalle parti coinvolte nella divulgazione coordinata delle vulnerabilità.

Articolo 4

Termini e condizioni per l'applicazione dei motivi connessi alla cibersicurezza in relazione a uno specifico CSIRT

Il CSIRT che ha ricevuto per primo la notifica può decidere di ritardare per un periodo di tempo strettamente necessario la diffusione delle notifiche o di parti di esse a uno specifico CSIRT pertinente nei casi in cui:

(a) il CSIRT pertinente è stato interessato da un incidente di cibersicurezza che ha messo in dubbio la sua capacità di garantire la riservatezza delle informazioni notificate;

(b) ha motivi sufficienti di ritenere che le capacità del CSIRT pertinente siano inadeguate a garantire la riservatezza delle informazioni notificate.

Nei casi di cui al primo comma, lettera a), il CSIRT che ha ricevuto per primo la notifica può ritardare la diffusione fino a quando il CSIRT pertinente non abbia informato la rete di CSIRT di cui all'articolo 15 della direttiva 2022/2555 del ripristino della sua capacità di garantire la riservatezza delle notifiche.

Nei casi di cui al primo comma, lettera b), il CSIRT che ha ricevuto per primo la notifica può ritardare la diffusione al CSIRT pertinente fino a quando quest'ultimo non abbia fornito prove di aver affrontato le carenze individuate.

Articolo 5

Termini e condizioni per l'applicazione dei motivi connessi alla cibersicurezza in relazione alla piattaforma unica di segnalazione

Il CSIRT che ha ricevuto per primo la notifica può decidere di ritardare la diffusione delle notifiche attraverso la piattaforma unica di segnalazione istituita dall'articolo 16 del regolamento (UE) 2024/2847 qualora l'ENISA abbia informato la rete di CSIRT, a norma dell'articolo 16, paragrafo 4, di tale regolamento, che la piattaforma unica di segnalazione è stata interessata da un incidente di cibersicurezza che mette in dubbio la sua capacità di garantire la riservatezza delle informazioni notificate. In tali casi il CSIRT che ha ricevuto per primo la notifica può ritardare la diffusione attraverso la piattaforma unica di segnalazione fino a quando l'ENISA non abbia informato la rete di CSIRT che è stata ripristinata la capacità della piattaforma di garantire la riservatezza delle notifiche.

Articolo 6

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

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 11.12.2025

Per la Commissione
La presidente
Ursula VON DER LEYEN