Rådet for
Den Europæiske Union

Bruxelles, den 17. december 2025
(OR. en)

16960/25

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

FØLGESKRIVELSE

fra:	Martine DEPREZ, direktør, på vegne af generalsekretæren for Europa-Kommissionen
modtaget:	11. december 2025
til:	Thérèse BLANCHET, generalsekretær for Rådet for Den Europæiske Union
Komm. dok. nr.:	C(2025) 8407 final
Vedr.:	KOMMISSIONENS DELEGEREDE FORORDNING (EU) …/… af 11.12.2025 om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) 2024/2847 for så vidt angår præcisering af vilkårene og betingelserne for anvendelse af de cybersikkerhedsrelaterede grunde i forbindelse med udsættelse af formidlingen af underretninger

Hermed følger til delegationerne dokument C(2025) 8407 final.

Bilag: C(2025) 8407 final

EUROPA-
KOMMISSIONEN

Bruxelles, den 11.12.2025
C(2025) 8407 final

KOMMISSIONENS DELEGEREDE FORORDNING (EU) …/…

af 11.12.2025

om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) 2024/2847 for så vidt angår præcisering af vilkårene og betingelserne for anvendelse af de cybersikkerhedsrelaterede grunde i forbindelse med udsættelse af formidlingen af underretninger

(EØS-relevant tekst)

BEGRUNDELSE

1. BAGGRUND FOR DEN DELEGEREDE RETSAKT

I henhold til Europa-Parlamentets og Rådets forordning (EU) 2024/2847 ("forordningen om cyberrobusthed") skal fabrikanter af produkter med digitale elementer via en fælles indberetningsplatform underrette om enhver aktivt udnyttet sårbarhed eller alvorlig hændelse, der har indvirkning på sikkerheden af et produkt med digitale elementer. I henhold til nævnte forordnings artikel 16, stk. 2, kan den enhed, der håndterer IT-sikkerhedshændelser (CSIRT), og som er udpeget af medlemsstaten som koordinator og indledningsvist modtager underretningen, under ekstraordinære omstændigheder og på grundlag af begrundede cybersikkerhedsrelaterede grunde udsætte formidlingen af underretningen til CSIRT'erne i andre medlemsstater, hvor produktet med digitale elementer er blevet gjort tilgængeligt.

Nærværende delegerede retsakt har derfor til formål at supplere forordningen om cyberrobusthed ved at præcisere vilkårene og betingelserne for anvendelse af de cybersikkerhedsrelaterede grunde til at udsætte formidlingen af underretninger. Dette sker ved at fastlægge tre typer årsager til, at den CSIRT, som indledningsvist modtager underretningen, kan beslutte, at det er nødvendigt at udsætte videreformidling til andre CSIRT'er. En sådan beslutning om udsættelse kan træffes under tre omstændigheder:

- på baggrund af en vurdering af arten af de indberettede oplysninger
- hvis den CSIRT, som modtager underretningen, ikke kan sikre fortroligheden af sådanne oplysninger
- hvis den fælles indberetningsplatform er blevet kompromitteret eller midlertidigt er ude af drift.

De rapporteringsforpligtelser, der er fastsat i artikel 14 i forordning (EU) 2024/2847, finder anvendelse fra den 11. september 2026.

2. HØRINGER FORUD FOR RETSAKTENS VEDTAGELSE

CSIRT-netværket og Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) blev hørt om forskellige udkast til nærværende retsakt. En indledende drøftelse med vejledende spørgsmål fandt sted den 26. marts 2025 med mulighed for at give skriftligt input senest den 11. april 2025. Et første udkast til retsakt blev delt med CSIRT-netværket og ENISA den 16. maj 2025, og den 6. juni 2025 blev der afholdt en drøftelse med mulighed for at give skriftligt input senest den 27. juni 2025. Et andet udkast til retsakt blev delt med CSIRT-netværket og ENISA den 23. juli 2025 med mulighed for at give skriftligt input senest den 1. september 2025. Et tredje udkast til retsakt blev delt med CSIRT-netværket og ENISA den 25. september 2025, og den 9. oktober 2025 blev der afholdt en drøftelse med mulighed for at give skriftligt input senest den 27. oktober 2025.

Udkastet til retsakt blev sendt til offentlig høring fra den 16. oktober 2025 til den 13. november 2025, og der blev modtaget 34 svar fra 31 særskilte respondenter (der blev sendt feedback fire gange fra den samme respondent). Heraf kom 29,41 % fra erhvervssammenslutninger, 26,47 % fra virksomheder, 17,65 % fra EU-borgere, 14,71 % fra

offentlige myndigheder, 5,88 % fra ikkestatslige organisationer (NGO'er) og 5,88 % fra akademiske institutioner/forskningsinstitutter[1].

Den 22. oktober blev udkastet også drøftet med ekspertgruppen vedrørende cybersikkerhed for produkter med digitale elementer (E03967), hvis medlemmer omfatter medlemsstaternes myndigheder, ENISA, individuelle eksperter, der er udpeget i deres personlige egenskab, og organisationer i bred forstand (f.eks. virksomheder, sammenslutninger eller NGO'er).

3. JURIDISKE ASPEKTER AF DEN DELEGEREDE RETSAKT

Beføjelsen til at vedtage delegerede retsakter er fastsat i artikel 14, stk. 9, i forordningen om cyberrobusthed, som pålægger Kommissionen senest den 11. december 2025 at præcisere vilkårene og betingelserne for anvendelse af de cybersikkerhedsrelaterede grunde i forbindelse med udsættelse af formidlingen af underretninger.

[1] Der er i disse procentsatser ikke taget hensyn til, at den samme respondent sendte feedback fire gange.

KOMMISSIONENS DELEGEREDE FORORDNING (EU) …/…

af 11.12.2025

om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) 2024/2847 for så vidt angår præcisering af vilkårene og betingelserne for anvendelse af de cybersikkerhedsrelaterede grunde i forbindelse med udsættelse af formidlingen af underretninger

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR –

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) nr. 168/2013 og (EU) 2019/1020 og direktiv (EU) 2020/1828 (forordningen om cyberrobusthed)[2], særlig artikel 14, stk. 9, og

ud fra følgende betragtninger:

(1) Under ekstraordinære omstændigheder og navnlig efter anmodning fra fabrikanten og i lyset af følsomhedsgraden af de indberettede oplysninger og på grundlag af begrundede cybersikkerhedsrelaterede grunde kan den enhed, der håndterer IT-sikkerhedshændelser (CSIRT), og som er udpeget som koordinator og indledningsvist modtager underretning om en aktivt udnyttet sårbarhed eller en alvorlig hændelse, der har indvirkning på sikkerheden af et produkt med digitale elementer ("den CSIRT, som indledningsvist modtager underretningen"), beslutte at udsætte formidlingen af underretningen via den fælles indberetningsplatform i en periode, der er strengt nødvendig, til de CSIRT'er, der er udpeget som koordinatorer på det område, hvor den fabrikant, der har foretaget underretningen, har angivet, at produktet med digitale elementer er gjort tilgængeligt ("de relevante CSIRT'er"). Der bør derfor fastsættes vilkår og betingelser for anvendelsen af sådanne grunde. Hvis sådanne grunde gør sig gældende, kan den CSIRT, som indledningsvist modtager underretningen, udsætte formidlingen til relevante CSIRT'er i en periode, der er strengt nødvendig, men er ikke forpligtet hertil. Hvis en CSIRT, som indledningsvist modtager underretningen, beslutter at gøre sådanne grunde gældende, bør den i henhold til artikel 16, stk. 2, i forordning (EU) 2024/2847 straks underrette Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) om sin beslutning om at udsætte underretningen og om grundene hertil, samt hvornår den påtænker at videreformidle underretningen.

(2) I henhold til artikel 16, stk. 2, andet afsnit, i forordning (EU) 2024/2847 finder de vilkår og betingelser for anvendelse af de cybersikkerhedsrelaterede grunde, der er fastsat i nærværende forordning, ikke anvendelse på ENISA's adgang til de indberettede oplysninger. ENISA's adgang til de indberettede oplysninger kan kun begrænses under særlige ekstraordinære omstændigheder: når fabrikanten i sin underretning angiver, at en af de tre betingelser, der er omhandlet i artikel 16, stk. 2,

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

tredje afsnit, litra a), b) eller c), i forordning (EU) 2024/2847, er opfyldt, og derefter kun i forbindelse med den meddelelse om sårbarhed inden for 72 timer, som er omhandlet i artikel 14, stk. 2, litra b), i forordning (EU) 2024/2847. I sådanne tilfælde er de eneste oplysninger, der skal stilles til rådighed for ENISA samtidigt, oplysninger om, at en fabrikant har foretaget en underretning, generelle oplysninger om produktet med digitale elementer, oplysninger om den generelle karakter af udnyttelsen og oplysninger om, at sikkerhedsrelaterede grunde er gjort gældende.

(3) Adgang til de indberettede oplysninger gør det muligt for CSIRT'er at få et overblik over sikkerhedsmiljøet på deres område og træffe afbødende foranstaltninger, der øger det overordnede cybersikkerhedsniveau i Unionen. Yderligere begrænsninger af formidlingen af underretninger på baggrund af arten af de oplysninger, der indberettes, bør derfor kun være mulige i tilfælde, hvor de cybersikkerhedsrisici, der følger af yderligere formidling, i lyset af de indberettede oplysningers følsomhed vejer tungere end sikkerhedsfordelene for Unionen, og hvor disse risici ikke i tilstrækkelig grad kan afbødes ved at indføre begrænsninger for håndtering og yderligere deling af underretningen gennem passende protokoller, der er i brug inden for CSIRT-netværket, såsom Traffic Light Protocol (TLP) eller Permissible Actions Protocol (PAP). Dette kan f.eks. være tilfældet, hvis en fabrikant har meddelt den CSIRT, som indledningsvis modtager underretningen, at vedkommende forventer snart at træffe en afbødende foranstaltning (f.eks. en patch). Det kan også være tilfældet, når den CSIRT, som indledningsvis modtager underretningen, beslutter kun at dele dele af en underretning, og disse dele ikke desto mindre er tilstrækkelige til, at de relevante CSIRT'er kan sikre, at de kan træffe passende risikobegrænsende foranstaltninger. For at tilskynde til samarbejde om identifikation og offentliggørelse af sårbarheder mellem fabrikanter, CSIRT'er og sikkerhedsforskere kan dette desuden også være tilfældet, når CSIRT'en fungerer som betroet formidler i forbindelse med en igangværende koordineret procedure for offentliggørelse af sårbarheder som omhandlet i artikel 12, stk. 1, i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[3]. I sådanne tilfælde, når CSIRT'en beslutter at udsætte formidlingen af en underretning, og i overensstemmelse med artikel 16, stk. 6, i forordning (EU) 2024/2847 skal den pågældende CSIRT udsætte underretningen i en periode, der ikke er længere end strengt nødvendigt, og indtil de parter, som er involveret i offentliggørelsen af sårbarheder, har givet deres samtykke hertil.

(4) Oplysningerne i underretningen vil hjælpe CSIRT'erne med at udføre deres opgaver i forbindelse med risikobegrænsning og håndtering af hændelser. I sjældne tilfælde kan sådanne oplysninger imidlertid være tilstrækkelige til at muliggøre udviklingen af en udnyttelsesteknik uden større forarbejde, selv af aktører med begrænsede færdigheder og ressourcer. Hvis ondsindede aktører fik adgang til disse oplysninger, ville Unionens cybersikkerhed blive hårdt ramt i betragtning af, hvor let det er at udnytte dem. Dette kan f.eks. være tilfældet, hvis den sårbare version af et softwareprodukt kun adskiller sig marginalt fra tidligere, ikkesårbare versioner. Hvis den CSIRT, som indledningsvist modtager underretningen, i sådanne tilfælde mener, at de cybersikkerhedsrisici, der følger af videreformidling, ikke i tilstrækkelig grad kan afbødes ved at indføre begrænsninger for håndtering og yderligere deling, kan den

[3] Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333 af 27.12.2022, s. 80).

beslutte at udsætte formidlingen, indtil der foreligger en effektiv risikobegrænsende foranstaltning såsom en sikkerhedsopdatering eller brugervejledning.

(5) Hvis en relevant CSIRT ikke i tilstrækkelig grad kan beskytte de indberettede oplysninger, vil ondsindede aktører kunne få adgang til følsomme oplysninger og udnytte dem i hele det indre marked. Hvis der er alvorlige betænkeligheder med hensyn til en relevant CSIRT's evne til at sikre fortroligheden af de indberettede oplysninger, kan den CSIRT, som indledningsvist modtager underretningen, derfor beslutte at udsætte formidlingen af en underretning til kun den relevante CSIRT, indtil sådanne betænkeligheder er blevet afhjulpet. Dette kan være tilfældet i situationer, hvor en relevant CSIRT er blevet ramt af en cybersikkerhedshændelse, der påvirker dens evne til at fungere sikkert, eller hvor der er dokumentation for eller oplysninger om, at der er konstateret betydelige mangler i CSIRT'ens kapacitet, såsom alvorlige ressourcemæssige begrænsninger, der bringer dens evne til at udføre sine funktioner i fare, eller afhængighed af forældet eller sårbar software.

(6) For at forhindre ondsindede aktører i at få adgang til følsomme oplysninger, hvis den fælles indberetningsplatform, der er oprettet i henhold til artikel 16 i forordning (EU) 2024/2847, er blevet kompromitteret af en cybersikkerhedshændelse, bør den CSIRT, som indledningsvist modtager underretningen, udsætte formidlingen via den fælles indberetningsplatform, indtil platformen igen kan sikre fortroligheden af de indberettede oplysninger.

(7) I overensstemmelse med artikel 16, stk. 2, første afsnit, i forordning (EU) 2024/2847 behøver den CSIRT, som indledningsvist modtager underretningen, ikke at formidle en underretning til nogen anden relevant CSIRT, såfremt fabrikanten angiver, at produktet med digitale elementer kun gøres tilgængeligt på markedet i den medlemsstat, hvor den CSIRT, som indledningsvist modtager underretningen, er beliggende.

(8) Kommissionen har i forbindelse med udarbejdelsen af udkastet til delegeret retsakt hørt og indhentet synspunkter fra relevante interessenter og har hørt ekspertgruppen vedrørende cybersikkerhed for produkter med digitale elementer.

(9) I overensstemmelse med artikel 14, stk. 9, i forordning (EU) 2024/2847 har Kommissionen i forbindelse med udarbejdelsen af udkastet til delegeret retsakt arbejdet tæt sammen med CSIRT-netværket, der er oprettet i henhold til artikel 15 i direktiv (EU) 2022/2555, og med ENISA –

VEDTAGET DENNE FORORDNING:

Artikel 1

Genstand

I denne forordning præciseres vilkårene og betingelserne for anvendelse af de cybersikkerhedsrelaterede grunde, der er omhandlet i artikel 16, stk. 2, i forordning (EU) 2024/2847, og som gør det muligt for den CSIRT, der er udpeget som koordinator, og som indledningsvist modtager en underretning i overensstemmelse med nævnte forordnings artikel 14, stk. 1 og 3, og artikel 15, stk. 1 og 2, at udsætte formidlingen af underretningen til de CSIRT'er, der er udpeget som koordinatorer, på hvis område fabrikanten har angivet, at produktet med digitale elementer er gjort tilgængeligt.

Artikel 2

Definitioner

I denne forordning forstås ved:

1) "CSIRT, som indledningsvist modtager underretningen": den CSIRT, der er udpeget som koordinator, og som indledningsvist modtager underretningen i overensstemmelse med artikel 14, stk. 1 og 3, og artikel 15, stk. 1 og 2, i forordning (EU) 2024/2847

2) "relevant CSIRT": den CSIRT, der er udpeget som koordinator på det område, som fabrikanten har angivet, at produktet med digitale elementer er gjort tilgængeligt.

Artikel 3

Vilkår og betingelser for anvendelse af cybersikkerhedsrelaterede grunde, der følger af de indberettede oplysningers karakter

Den CSIRT, som indledningsvist modtager underretningen, kan beslutte at udsætte formidlingen af underretninger eller dele heraf til relevante CSIRT'er i en periode, der er begrænset til det strengt nødvendige, i tilfælde, hvor de cybersikkerhedsrisici, der er forbundet med formidlingen, i lyset af de indberettede oplysningers følsomhed vejer tungere end sikkerhedsfordelene herved, og disse risici ikke kan afbødes ved at indføre begrænsninger for håndtering eller yderligere deling af underretningen ved hjælp af passende protokoller såsom Traffic Light Protocol (TLP) eller Permissible Actions Protocol (PAP), og hvor mindst én af følgende betingelser er opfyldt:

a) fabrikanten har underrettet den CSIRT, som indledningsvist modtager underretningen, om, at en effektiv risikobegrænsende foranstaltning såsom en sikkerhedsopdatering eller brugervejledning forventes at blive gjort tilgængelig inden for 72 timer; hvis en effektiv risikobegrænsende foranstaltning ikke stilles til rådighed inden for denne tidsramme, formidler den CSIRT, som indledningsvist modtager underretningen, underretningen til de relevante CSIRT'er

b) oplysningerne i underretningen anses i lyset af karakteren af den indberettede aktivt udnyttede sårbarhed for at være tilstrækkelige til at skabe en udnyttelsesteknik, navnlig når sårbarheden let kan identificeres og udnyttes af aktører med begrænsede færdigheder og ressourcer; når en effektiv risikobegrænsende foranstaltning såsom en sikkerhedsopdatering eller brugervejledning er gjort tilgængelig, formidler den CSIRT, som indledningsvist modtager underretningen, underretningen til de relevante CSIRT'er

c) den CSIRT, som indledningsvist modtager underretningen, er i stand til at dele tilstrækkelige oplysninger med de relevante CSIRT'er for at sikre, at de relevante CSIRT'er kan indføre passende risikobegrænsende foranstaltninger; når en effektiv risikobegrænsende foranstaltning såsom en sikkerhedsopdatering eller brugervejledning er gjort tilgængelig, formidler den CSIRT, som indledningsvist modtager underretningen, hele underretningen til de relevante CSIRT'er

d) den CSIRT, som indledningsvist modtager underretningen om den aktivt udnyttede sårbarhed, er blevet gjort opmærksom på den som led i en koordineret offentliggørelse af sårbarheder, for hvilken den pågældende CSIRT fungerer som betroet formidler i overensstemmelse med artikel 12, stk. 1, i direktiv (EU) 2022/2555; i så fald og i overensstemmelse med artikel 16, stk. 6, i forordning (EU) 2024/2847 formidler den CSIRT, som indledningsvist modtager underretningen,

underretningen til de relevante CSIRT'er, når en udsættelse ikke længere er strengt nødvendig, og de parter, der er involveret i den koordinerede offentliggørelse af sårbarheder, har givet samtykke til offentliggørelse.

Artikel 4

Vilkår og betingelser for anvendelse af cybersikkerhedsrelaterede grunde i forbindelse med en specifik CSIRT

Den CSIRT, som indledningsvist modtager underretningen, kan beslutte at udsætte formidlingen af underretninger eller dele heraf til en specifik relevant CSIRT i en periode, der er strengt nødvendig, hvis:

a) den relevante CSIRT er blevet berørt af en cybersikkerhedshændelse, der sår tvivl om dens evne til at sikre fortroligheden af de indberettede oplysninger

b) den har tilstrækkelig grund til at antage, at den relevante CSIRT's kapacitet er utilstrækkelig til at sikre fortroligheden af de indberettede oplysninger.

I de tilfælde, der er omhandlet i litra a), første afsnit, kan den CSIRT, som indledningsvist modtager underretningen, udsætte formidlingen, indtil den relevante CSIRT har underrettet det CSIRT-netværk, der er omhandlet i artikel 15 i direktiv 2022/2555, om, at dens evne til at sikre fortroligheden af underretninger er genoprettet.

I de tilfælde, der er omhandlet i litra b), første afsnit, kan den CSIRT, som indledningsvist modtager underretningen, udsætte formidlingen til den relevante CSIRT, indtil den pågældende CSIRT har fremlagt dokumentation for, at den har afhjulpet de konstaterede mangler.

Artikel 5

Vilkår og betingelser for anvendelse af cybersikkerhedsrelaterede grunde i forbindelse med den fælles indberetningsplatform

Den CSIRT, som indledningsvist modtager underretningen, kan beslutte at udsætte formidlingen af underretninger via den fælles indberetningsplatform, der er oprettet ved artikel 16 i forordning (EU) 2024/2847, hvis ENISA i overensstemmelse med nævnte forordnings artikel 16, stk. 4, har underrettet CSIRT-netværket om, at den fælles indberetningsplatform er blevet berørt af en cybersikkerhedshændelse, der skaber tvivl om dens evne til at sikre fortroligheden af indberettede oplysninger. I sådanne tilfælde kan den CSIRT, som indledningsvist modtager underretningen, udsætte formidlingen via den fælles indberetningsplatform, indtil ENISA har underrettet CSIRT-netværket om, at platformens evne til at sikre fortroligheden af underretninger er genoprettet.

Artikel 6

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 11.12.2025.

På Kommissionens vegne
Formand
Ursula VON DER LEYEN