Rådet for
Den Europæiske Union

Bruxelles, den 22. maj 2026
(OR. en)

9399/26

Interinstitutionel sag:
2026/0011(COD)
2026/0012(COD)

LIMITE

CYBER 229
JAI 606
DATAPROTECT 161
TELECOM 239
MI 489
IND 342
CADREFIN 220
FIN 697
BUDGET 19
CSC 316
CODEC 937

NOTE

fra:	Generalsekretariatet for Rådet
til:	De Faste Repræsentanters Komité/Rådet
Vedr.:	Forslag til Europa-Parlamentets og Rådets forordning om Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), den europæiske ramme for cybersikkerhedscertificering og sikkerhed i IKT-forsyningskæden og om ophævelse af forordning (EU) 2019/881 (forordningen om cybersikkerhed 2) Forslag til Europa-Parlamentets og Rådets direktiv om ændring af direktiv (EU) 2022/2555 for så vidt angår forenklingsforanstaltninger og tilpasning til [forslaget til forordning om cybersikkerhed] – Situationsrapport

Formandskabet har udarbejdet en situationsrapport om forslaget til Europa-Parlamentets og Rådets forordning om Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), den europæiske ramme for cybersikkerhedscertificering og sikkerhed i IKT-forsyningskæden og om ophævelse af forordning (EU) 2019/991 (forordningen om cybersikkerhed 2) med henblik på at aflægge rapport om det arbejde, der hidtil er udført af Rådets forberedende organer, og om status for behandlingen af forslaget.

INDLEDNING

1. 20. januar 2026 foreslog Kommissionen en ny cybersikkerhedspakke for at styrke EU's modstandsdygtighed og kapacitet inden for cybersikkerhed. Pakken består af en **forordning** om Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), den europæiske ramme for cybersikkerhedscertificering og sikkerhed i forsyningskæden for informations- og kommunikationsteknologi (IKT) og ophæver forordning (EU) 2019/881 (forordningen om cybersikkerhed). Denne forordning ("forordningen om cybersikkerhed 2") suppleres af et **direktiv** om ændring af direktiv (EU) 2022/2555 (NIS 2-direktivet) for så vidt angår forenklingsforanstaltninger og tilpasning til [forslaget til forordningen om cybersikkerhed].

2. Forud for forslaget opfordrede Rådet i sine konklusioner om ENISA af 6. december 2024[1] Kommissionen til at undersøge og yderligere styrke ENISA's rolle med hensyn til at støtte operationelt samarbejde på EU-plan og blandt medlemsstaterne med henblik på at øge cyberrobustheden under hensyntagen til medlemsstaternes kompetencer på dette område. Kommissionen blev også opfordret til at sikre, at ENISA's mandat til at støtte medlemsstaterne var fokuseret og klart defineret med konkrete strategiske mål og prioriterede opgaver ud over en mere præcis fordeling af opgaver og kompetencer med hensyn til andre aktører. Rådet opfordrede derfor også indtrængende Kommissionen til at benytte evalueringen af forordningen om cybersikkerhed til at finde en mere lempelig, risikobaseret og mere gennemsigtig og hurtigere tilgang til udviklingen af EU's ordninger for cybersikkerhedscertificering. Desuden understregede Rådet i sine konklusioner[2] af 21. maj 2024 om fremtiden for cybersikkerhed sit tilsagn om at sikre IKT-forsyningskæder og fremhævede relevansen af ikketekniske risikofaktorer, herunder tredjelandes utilbørlige indflydelse på leverandører og udbydere. Endelig understregede Rådet i sine konklusioner[3] af 17. oktober 2022 om sikkerhed i IKT-forsyningskæden behovet for at styrke IKT-forsyningskædernes modstandsdygtighed og sikkerhed i betragtning af indvirkningen af geopolitiske spændinger og afhængighed af IKT-produkter og -tjenester.

---

1 16527/24.
2 10133/24.
3 13664/22.

3. Formålet med forslaget til forordning, som er baseret på artikel 114 i TEUF, er at styrke Unionens ramme for cybersikkerhed. Det styrker Den Europæiske Unions Agentur for Cybersikkerheds (ENISA's) rolle og opgaver med hensyn til at støtte medlemsstaterne og EU-enhederne i at opnå et højt niveau af cybersikkerhed, modstandsdygtighed og tillid til Unionen. Dets formål er at gøre den europæiske ramme for cybersikkerhedscertificering mere effektiv og virkningsfuld for at muliggøre en hurtigere udvikling og gennemførelse af ordningen. Forslaget fastlægger også en EU-ramme for pålidelig sikkerhed i IKT-forsyningskæden, der tager højde for ikketekniske risikofaktorer og afhængighedsforhold, der påvirker sikkerheden i kritisk IKT-infrastruktur og kritiske IKT-tjenester. Det er ledsaget af målrettede forenklingsforanstaltninger i forbindelse med gennemførelsen af NIS 2-direktivet[4], der har til formål at forenkle overensstemmelseskravene, mindske unødvendige administrative byrder og øge den juridiske klarhed.

4. I køreplanen "Et Europa, ét marked"[5], der blev undertegnet i tilknytning til det uformelle møde mellem stats- og regeringscheferne, der blev afholdt i Cypern den 24. april 2026, indgår dette forslag som et af de prioriterede mål.

5. Europa-Parlamentet udpegede Gregorová Markéta (Verts/ALE) til ordfører i det kompetente udvalg, ITRE.

6. Den 29. april 2026 afgav Det Europæiske Økonomiske og Sociale Udvalg sin udtalelse om forslaget[6].

---

4 EUT L 333 af 27.12.2022, s. 80.
5 8473/26.
6 8980/26.

STATUS FOR ARBEJDET I RÅDETS FORBEREDENDE ORGANER

7. En generel præsentation af cybersikkerhedspakken fandt sted på et møde i Den Horisontale Gruppe vedrørende Cyberspørgsmål (Cybergruppen) den 26. januar 2026 og på et møde i De Faste Repræsentanters Komité den 28. januar 2026.

8. Cybergruppen begyndte at drøfte forslaget den 2. februar 2026 med en nærmere redegørelse fra Kommissionen. Under denne redegørelse fremlagde Kommissionen også resultaterne af evalueringsrapporten, finansieringsoversigten og konsekvensanalysen.

9. Cybergruppen påbegyndte gennemgangen af den foreslåede forordning den 23. februar 2026.

10. Medlemsstaterne hilste forslaget velkommen og støttede generelt dets overordnede mål, navnlig styrkelsen af ENISA's støtte til medlemsstaternes operationelle samarbejde og strømlining af certificeringsrammen. Drøftelserne viste imidlertid også, at flere af forslagets aspekter vil kræve yderligere behandling. Delegationerne anmodede om yderligere præciseringer vedrørende ENISA's øgede operationelle rolle og opgaver såsom udstedelse af tidlige varslinger, oprettelse af en ransomware-helpdesk og ENISA's rolle i CSIRT-netværket. Flere delegationer satte spørgsmålstegn ved de ressourcemæssige konsekvenser for medlemsstaterne i forbindelse med det foreslåede bidrag fra to udstationerede nationale eksperter pr. medlemsstat til støtte for ENISA's opgaver. Bestyrelsens afstemningsregler kræver også yderligere drøftelser. Delegationerne understregede behovet for større klarhed og præcision med hensyn til de definitioner og begreber, der anvendes i hele forslaget. Sammensætningen af ENISA's budget, navnlig opkrævningen af gebyrer, krævede også yderligere præciseringer.

11. De nye bestemmelser, der skal gøre certificeringsprocessen mere effektiv, blev generelt hilst velkommen, selv om der blev konstateret et generelt behov for større deltagelse fra medlemsstaternes side i hele certificeringsprocessen. Certificeringens frivillige karakter blev generelt hilst velkommen. Delegationerne satte imidlertid spørgsmålstegn ved nogle af de foreslåede frister i certificeringsrammen.

12. Drøftelserne om rammen for en pålidelig IKT-forsyningskæde fremhævede flere betænkeligheder blandt medlemsstaterne. Delegationerne opfordrede til yderligere præciseringer af metoden og procedurerne til identifikation af centrale IKT-aktiver og højrisikoleverandører samt af anvendelsesområdet for og den mulige virkning af de foreslåede foranstaltninger. Delegationerne understregede betydningen af at sikre en passende grad af inddragelse af medlemsstaterne.

13. Flere delegationer tog undersøgelsesforbehold med hensyn til forskellige dele af forslaget, navnlig vedrørende forvaltningsaspekter, anvendelsen af gennemførelsesretsakter og den foreslåede mekanisme til identifikation af højrisikoleverandører og sikkerhed i IKT-forsyningskæden.

14. Efter drøftelserne i Cybergruppen blev medlemsstaterne opfordret til at fremsætte skriftlige bemærkninger til bestemmelserne vedrørende afsnit I om almindelige bestemmelser og afsnit II om ENISA. 23 medlemsstater indsendte bidrag. Senere blev medlemsstaterne også opfordret til at fremsætte skriftlige bemærkninger til afsnit III om den europæiske ramme for cybersikkerhedscertificering. 20 medlemsstater benyttede sig af muligheden for at fremlægge deres holdninger skriftligt.

15. På grundlag af disse skriftlige bidrag fra medlemsstaterne og arbejdet i Cybergruppen vil formandskabet udarbejde en kompromistekst om afsnit II (ENISA) og III (den europæiske ramme for cybersikkerhedscertificering), som vil blive forelagt på Cybergruppens møde i begyndelsen af juni 2026.

16. Flere medlemsstater anmodede Rådets Juridiske Tjeneste om at undersøge, om retsgrundlaget er hensigtsmæssigt.

17. Formandskabet vil indlede gennemgangen af forenklingsforanstaltningerne i NIS 2-direktivet ved udgangen af maj 2026.

18. Cybergruppen vil alt i alt have afholdt 15 møder om forslaget til forordning om cybersikkerhed 2 under Cyperns formandskab.

19. På baggrund af fremskridtene under Cyperns formandskab planlægger det kommende irske formandskab at fortsætte arbejdet med denne vigtige sag.

20. I lyset af ovenstående opfordres de Faste Repræsentanters Komité og Rådet til at notere sig de fremskridt, der er gjort under gennemgangen af forslaget til forordning.