Europeiska unionens råd

Bryssel den 22 maj 2026
(OR. en)

9399/26

Interinstitutionella ärenden:
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

NOT

från:	Rådets generalsekretariat
till:	Ständiga representanternas kommitté (Coreper)/rådet
Ärende:	Förslag till Europaparlamentets och rådets förordning om Europeiska unionens cybersäkerhetsbyrå (Enisa), om det europeiska ramverket för cybersäkerhetscertifiering och om säkerhet i IKT-leveranskedjan samt om upphävande av förordning (EU) 2019/881 (cybersäkerhetsakt 2) Förslag till Europaparlamentets och rådets direktiv om ändring av direktiv (EU) 2022/2555 vad gäller förenklingsåtgärder och anpassning till [förslaget till cybersäkerhetsakt] – Lägesrapport

Ordförandeskapet har utarbetat en lägesrapport om förslaget till Europaparlamentets och rådets förordning om Europeiska unionens cybersäkerhetsbyrå (Enisa), om det europeiska ramverket för cybersäkerhetscertifiering och om säkerhet i IKT-leveranskedjan och om upphävande av förordning (EU) 2019/881 (cybersäkerhetsakt 2), i syfte att rapportera om det arbete som hittills gjorts av rådets förberedande organ och om läget i behandlingen av förslaget.

INLEDNING

1. Den 20 januari 2026 föreslog kommissionen ett nytt cybersäkerhetspaket för att stärka EU:s resiliens och förmågor på cybersäkerhetsområdet. Paketet består av en **förordning** om Europeiska unionens cybersäkerhetsbyrå (Enisa), det europeiska ramverket för cybersäkerhetscertifiering och säkerhet i IKT-leveranskedjan och om upphävande av förordning (EU) 2019/881 (cybersäkerhetsakten). Denna förordning (*cybersäkerhetsakt 2*) kompletteras av ett **direktiv** om ändring av direktiv (EU) 2022/2555 (NIS 2-direktivet) vad gäller förenklingsåtgärder och anpassning till [förslaget till cybersäkerhetsakt].

2. Innan förslaget lades fram uppmanades kommissionen i rådets slutsatser om Enisa av den 6 december 2024[1] att undersöka och ytterligare stärka Enisas roll när det gäller att stödja operativt samarbete på EU-nivå och mellan medlemsstaterna vad gäller att öka cyberresiliensen, med beaktande av medlemsstaternas befogenheter på detta område. Kommissionen uppmanades också att säkerställa att Enisas mandat att stödja medlemsstaterna var fokuserat och tydligt definierat, med konkreta strategiska mål och prioriterade uppgifter, utöver en mer exakt fördelning av uppgifter och befogenheter i förhållande till andra aktörer. Rådet uppmanade även kommissionen att utnyttja möjligheten med utvärderingen av cybersäkerhetsakten för att hitta sätt att ha en smidigare, riskbaserad samt mer transparent och snabbare strategi för utvecklingen av EU:s ordningar för cybersäkerhetscertifiering. I sina slutsatser[2] av den 21 maj 2024 om framtidens cybersäkerhet betonade rådet dessutom sitt åtagande att säkerställa säkra IKT-leveranskedjor och pekade på betydelsen av icke-tekniska riskfaktorer, inbegripet otillbörlig påverkan från tredjestater på leverantörer av varor och tjänster. Slutligen underströks i rådets slutsatser[3] av den 17 oktober 2022 om säkerheten i IKT-leveranskedjan behovet av att stärka IKT-leveranskedjornas motståndskraft och säkerhet, med tanke på effekterna av geopolitiska spänningar och beroenden av IKT-produkter och IKT-tjänster.

---

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

3. Syftet med förslaget till förordning, som grundar sig på artikel 114 i EUF-fördraget, är att stärka unionens ramverk för cybersäkerhet. Det stärker Europeiska unionens cybersäkerhetsbyrås (Enisa) roll och uppgifter för att hjälpa medlemsstaterna och unionens enheter att uppnå en hög nivå av cybersäkerhet, resiliens och förtroende för unionen. Det syftar till att göra det europeiska ramverket för cybersäkerhetscertifiering mer ändamålsenligt och effektivt så att ordningarna kan utvecklas och genomföras snabbare. Genom förslaget inrättas också en unionsram för säkerhet i tillförlitliga IKT-leveranskedjor, som tar itu med icke-tekniska riskfaktorer och beroenden som påverkar säkerheten för kritisk IKT-infrastruktur och kritiska IKT-tjänster. Ramen åtföljs av riktade förenklingsåtgärder i samband med genomförandet av NIS 2-direktivet[4], som syftar till att förenkla efterlevnadskraven, minska onödiga administrativa bördor och öka den rättsliga klarheten.

4. Färdplanen Ett Europa, en marknad[5], som undertecknades i anslutning till stats- och regeringschefernas informella möte på Cypern den 24 april 2026, inbegriper detta förslag som en av prioriteringarna.

5. Europaparlamentet utsåg Gregorová Markéta (Verts/ALE) till föredragande i utskottet för industrifrågor, forskning och energi, som är det utskott som är ansvarigt.

6. Europeiska ekonomiska och sociala kommittén avgav ett yttrande om förslaget[6] den 29 april 2026.

---

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

7. En allmän presentation av cybersäkerhetspaketet ägde rum vid ett möte i den övergripande arbetsgruppen för cyberfrågor den 26 januari 2026 och vid ett möte i Coreper den 28 januari 2026.

8. Den övergripande arbetsgruppen för cyberfrågor började diskutera förslaget den 2 februari 2026 med en detaljerad föredragning av kommissionen. Vid föredragningen presenterade kommissionen också resultaten i utvärderingsrapporten, finansieringsöversikten och konsekvensbedömningen.

9. Den övergripande arbetsgruppen för cyberfrågor inledde genomgången av förslaget till förordning den 23 februari 2026.

10. Medlemsstaterna välkomnade förslaget och stödde i allmänhet dess övergripande mål, särskilt förstärkningen av Enisas stöd till medlemsstaternas operativa samarbete och effektivisering av certifieringsramverket. Diskussionerna visade dock också att flera aspekter av förslaget kräver ytterligare behandling. Delegationerna begärde ytterligare förtydliganden om Enisas utökade operativa roll och uppgifter, såsom utfärdande av tidiga varningar, inrättande av en hjälpcentral för utpressningsärenden och Enisas roll i nätverket för enheter för hantering av it-säkerhetsincidenter. Flera delegationer ifrågasatte resurskonsekvenserna för medlemsstaterna i samband med det föreslagna bidraget från två utstationerade nationella experter per medlemsstat till stöd för Enisas uppgifter. Styrelsens omröstningsregler kräver också ytterligare diskussioner. Delegationerna betonade behovet av större tydlighet och precision när det gäller definitioner och begrepp som används i hela förslaget. Sammansättningen av Enisas budget, särskilt uttaget av avgifter, behövde också förtydligas ytterligare.

11. De nya bestämmelserna för att göra certifieringsprocessen mer ändamålsenlig och effektiv välkomnades i allmänhet, även om ett allmänt behov konstaterades av ett ökat deltagande från medlemsstaternas sida under hela certifieringsprocessen. Certifieringens frivilliga karaktär välkomnades generellt. Delegationerna ifrågasatte dock några av de föreslagna tidsfristerna enligt certifieringsramverket.

12. Diskussionerna om ramen för den tillförlitliga IKT-leveranskedjan belyste flera farhågor bland medlemsstaterna. Delegationerna efterlyste ytterligare förtydliganden om metoden och förfarandena för identifiering av centrala IKT-tillgångar och högriskleverantörer samt om de föreslagna åtgärdernas omfattning och eventuella effekter. Delegationerna betonade vikten av att säkerställa en lämplig nivå av deltagande från medlemsstaternas sida.

13. Flera delegationer lämnade in granskningsreservationer mot olika delar av förslaget, särskilt när det gäller styrningsaspekter, användningen av genomförandeakter och den föreslagna mekanismen för identifiering av högriskleverantörer och säkerheten i IKT-leveranskedjan.

14. Efter diskussionerna i den övergripande arbetsgruppen uppmanades medlemsstaterna att lämna skriftliga synpunkter på bestämmelserna i avdelning I om allmänna bestämmelser och avdelning II om Enisa. 23 medlemsstater lämnade in bidrag. Senare uppmanades medlemsstaterna också att lämna skriftliga synpunkter på avdelning III om det europeiska ramverket för cybersäkerhetscertifiering. Tjugo medlemsstater tog chansen att uttrycka sina ståndpunkter skriftligen.

15. På grundval av dessa skriftliga bidrag från medlemsstaterna och arbetet i den övergripande arbetsgruppen för cyberfrågor kommer ordförandeskapet att utarbeta en kompromisstext om avdelningarna II (Enisa) och III (det europeiska ramverket för cybersäkerhetscertifiering) som kommer att läggas fram vid mötet i den övergripande arbetsgruppen för cyberfrågor i början av juni 2026.

16. Flera medlemsstater bad rådets juridiska avdelning att utreda huruvida den rättsliga grunden är lämplig.

17. Ordförandeskapet kommer att inleda genomgången av förenklingsåtgärderna i NIS 2-direktivet i slutet av maj 2026.

18. Under Cypern ordförandeskap kommer arbetsgruppen att ha hållit sammanlagt 15 möten om förslaget till cybersäkerhetsakt 2.

19. Med utgångspunkt i de framsteg som gjorts under Cyperns ordförandeskap planerar det tillträdande irländska ordförandeskapet att fortsätta arbetet med det här viktiga ärendet.

20. Mot bakgrund av det ovanstående uppmanas Coreper och rådet att notera de framsteg som har gjorts vid behandlingen av förslaget till förordning.