Europeiska unionens råd

Bryssel den 22 januari 2026
(OR. en)

5611/26
ADD 2

Interinstitutionella ärenden:
2026/0011 (COD)
2026/0012 (COD)

CYBER 29
JAI 85
DATAPROTECT 22
TELECOM 29
MI 58
IND 48
CADREFIN 26
FIN 100
BUDGET 3
CODEC 90

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	21 januari 2026
till:	Thérèse BLANCHET, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	SWD(2026) 12 final
Ärende:	ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR SAMMANFATTNING AV KONSEKVENSBEDÖMNINGSRAPPORTEN […] Följedokument till 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) och Förslag till Europaparlamentets och rådets direktiv om ändring av direktiv (EU) 2022/2555 vad gäller förenklingsåtgärder och anpassning till [förslaget till cybersäkerhetsakt 2]

För delegationerna bifogas dokument – SWD(2026) 12 final.

Bilaga: SWD(2026) 12 final

EUROPEISKA
KOMMISSIONEN

Strasbourg den 20.1.2026
SWD(2026) 12 final

ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR

SAMMANFATTNING AV KONSEKVENSBEDÖMNINGSRAPPORTEN

[…]

Följedokument till

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)

och

Förslag till Europaparlamentets och rådets direktiv om ändring av direktiv (EU) 2022/2555 vad gäller förenklingsåtgärder och anpassning till [förslaget till cybersäkerhetsakt 2]

{COM(2026) 11 final} - {SEC(2026) 11 final} - {SWD(2026) 11 final}

Sammanfattning av konsekvensbedömningen

Mål

Det främsta målet med denna konsekvensbedömning är att utvärdera om de nuvarande bestämmelserna är tillräckliga för att hantera de framväxande cybersäkerhetshoten i EU. I konsekvensbedömningen föreslås en integrerad uppsättning politiska alternativ som syftar till att stärka Europeiska unionens cybersäkerhetsbyrå (Enisa), reformera det europeiska ramverket för cybersäkerhetscertifiering och förenkla efterlevnaden av den befintliga cybersäkerhetslagstiftningen. I denna bedömning betonas vikten av att anpassa cyberstyrningen för att harmonisera den med tekniska framsteg och efterfrågan på marknaden, och samtidigt säkerställa konkurrenskraft och ta hänsyn till miljöpåverkan.

Problemformulering

Trots de befintliga insatserna står EU:s cybersäkerhetslandskap fortfarande inför betydande utmaningar i en situation med alltmer komplexa hot. Otillräcklig samordning mellan medlemsstaterna och andra aktörer på EU-nivå, ett avstannat genomförande av politiska verktyg samt rättsliga hinder och komplicerade regelverk står i vägen för en effektiv hantering av cybersäkerheten. Dessa problem leder till ökade kostnader för företag och myndigheter, större risker för cyberincidenter och inkonsekventa skyddsnivåer för medborgarna.

Skäl för EU-åtgärden

Cybersäkerhetshoten överskrider nationsgränserna, och det är därför viktigt med en enhetlig strategi så att kraftfulla åtgärder kan vidtas. Insatser på EU-nivå säkerställer ett konsekvent skydd, stärker konkurrenskraften genom att skapa lika villkor samt underlättar den fria rörligheten för digitala tjänster och produkter på den inre marknaden. Harmonisering på EU-nivå minskar också den administrativa bördan genom förenklad efterlevnad och rationaliserade förfaranden.

Politiska alternativ och rekommenderat alternativ

I denna rapport analyseras fyra insatsområden, vart och ett med en uppsättning politiska alternativ som övervägs mot bakgrund av de specifika mål som ska uppnås: 1) Enisas mandat (som även är en del av den nuvarande cybersäkerhetsakten), 2) det europeiska ramverket för cybersäkerhetscertifiering (som även är en del av den nuvarande cybersäkerhetsakten) och 3) riktade ändringar av NIS 2-direktivet i förenklingssyfte, men även i samband med Enisas mandat och det europeiska ramverket för cybersäkerhetscertifiering. Varje uppsättning alternativ är i sig insatsområden, men de är samtidigt sammankopplade och relevanta sinsemellan.

Alternativ för att ta itu med den bristande överensstämmelsen mellan EU:s policyram för cybersäkerhet och berörda parters behov i en alltmer fientlig miljö

Alternativ A.1: *förtydliga Enisas mandat och underlätta för prioritering* – Detta alternativ skulle säkerställa en tydlig och stabil ram för Enisas uppgifter genom att införliva de uppgifter som fastställs i annan lagstiftning.

Alternativ A.2: *reformera Enisas mandat* – Detta alternativ skulle leda till att cybersäkerhetsakten upphävs och ersätts, vilket innebär att byråns mandat ses över.

Alternativ A.3: *reformera Enisas mandat med ett starkt fokus på operativt stöd* – Detta alternativ skulle bygga vidare på alternativ A.2. Dessutom skulle Enisa utveckla kapacitet för att direkt stödja entiteter enligt NIS 2-direktivet när det gäller att reagera på och återhämta sig från cybersäkerhetsincidenter på en medlemsstats begäran.

Alternativ för det europeiska ramverket för cybersäkerhetscertifiering

Alternativ B.1: *förtydliga tillämpningsområdet för, inslagen i och målen med det europeiska ramverket för cybersäkerhetscertifiering samt införa en underhållsmekanism* – Genom detta alternativ skulle en ny underhållsmekanism införas för de ordningar som Enisa ska genomföra, efter det att de antagits.

Alternativ B.2: *reformera det europeiska ramverket för cybersäkerhetscertifiering genom att se över dess förfaranden samt utvidga tillämpningsområdet för att underlätta förenkling av regelefterlevnaden* – Enligt detta alternativ skulle cybersäkerhetsakten upphävas och ersättas med en ny förordning. Utöver alternativ B.1 skulle förfarandet för begäran, utveckling och antagande av ordningar ses över för att förbättra ansvarsskyldigheten och effektiviteten.

Alternativ B.3: *reformera det europeiska ramverket för cybersäkerhetscertifiering i enlighet med alternativ B.2 och införa obligatorisk certifiering för säkerhetsstatus* – Detta alternativ bygger vidare på alternativ B.2 och syftar till att ytterligare stärka ramverkets effekter genom att införa obligatorisk certifiering av väsentliga entiteter som omfattas av NIS 2-direktivet, med beaktande av särskilda riskscenarier, i stället för att enbart förlita sig på frivillig certifiering av entiteter.

Alternativ för förenkling

Alternativ C.1: *anta en strategi med icke-bindande icke-lagstiftningsinstrument, bland annat genom att använda befintliga befogenheter (anta genomförandeakter enligt artiklarna 21.5 och 23.11 i NIS 2-direktivet)* – Inom detta alternativ planeras antagandet av genomförandeakter enligt de befintliga befogenheterna i NIS 2-direktivet för att säkerställa en högre grad av harmonisering av riskhanteringsåtgärder för cybersäkerhet, tröskelvärden för incidentrapportering samt information i och formaten och förfarandena för underrättelser, tillsammans med antagandet av en uppsättning riktlinjer för ökad rättssäkerhet och ett mer harmoniserat genomförande.

Alternativ C.2: *riktade insatser – ytterligare förenkling av efterlevnaden av den relevanta unionslagstiftningen för cybersäkerhet* – Detta alternativ omfattar begränsade insatser genom ändringar av cybersäkerhetsakten och NIS 2-direktivet i syfte att förenkla särskilda aspekter av cybersäkerhetsramen, inklusive anpassningar av tillämpningsområdet, maximal

harmonisering för genomförandeakter, bevis på efterlevnad genom certifiering och antagande av den uppsättning riktlinjer som avses i alternativ C1.

Alternativ C.3: *harmonisera de cybersäkerhetsrelaterade åtgärder som fastställs i unionslagstiftningen* – Detta alternativ bygger vidare på alternativ C.2 och skulle avlägsna alla de riskhanteringsåtgärder för cybersäkerhet eller befogenheter i förhållande till dem som ingår i den sektorsspecifika lagstiftningen. I stället skulle NIS 2-ekosystemet ändras genom att kraven förenklas för alla typer av entiteter, för att på så sätt säkerställa ökad harmonisering.

Alternativ för säkerheten i IKT-leveranskedjan

Alternativ D.1: *anta en icke-bindande strategi för att hantera cybersäkerhetsrisker för IKT-leveranskedjor* – Med detta alternativ skulle inga regleringsåtgärder vidtas på EU-nivå. I stället skulle kommissionen öka antalet samordnade riskbedömningar och frivilliga verktygslådor.

Alternativ D.2: *ad hoc-regleringsåtgärder för att kodifiera 5G-verktygslådan* – Detta alternativ skulle kodifiera åtgärderna i 5G-verktygslådan. Genom alternativet skulle medlemsstaterna bli skyldiga att se till att komponenter från högriskleverantörer inte används i viktiga tillgångar i nätet.

Alternativ D.3: *utarbeta en heltäckande och övergripande ram för att hantera cybersäkerhetsrisker för IKT-leveranskedjor* – Genom detta alternativ skulle en övergripande, teknik- och sektorsneutral ram inrättas för att hantera icke-tekniska cybersäkerhetsrisker för IKT-leveranskedjor.

Efter en omfattande analys inbegriper det rekommenderade policypaketet alternativ A.2 – reformera Enisas mandat, alternativ B.2 – reformera det europeiska ramverket för cybersäkerhetscertifiering genom att se över dess förfaranden samt utvidga tillämpningsområdet för att underlätta förenkling av regelefterlevnaden, alternativ C.2 – riktade insatser – ytterligare förenkling av efterlevnaden av den relevanta unionslagstiftningen för cybersäkerhet och alternativ D.3 – utarbeta en heltäckande och övergripande ram för att hantera cybersäkerhetsrisker för IKT-leveranskedjor.

Denna kombination erbjuder ett välbalanserat svar på de konstaterade politiska utmaningarna och medför en avsevärt ökad effektivitet, ändamålsenlighet och samstämmighet i hela EU.

Huvudsaklig påverkan

Kostnads-nyttoanalys: Övergången till det föreslagna regelverket kommer att medföra kostnader både för Enisa på uppskattningsvis 161,3 miljoner EUR under fem år för fullgörandet av byråns nya uppgifter och för myndigheter i hela EU på upp till 80 miljoner EUR under fem år för tillsyn (med beaktande av relevanta kostnadsbesparingar). När det gäller företagen kan utfasningen av specifik högriskutrustning under en övergångsperiod på tre år leda till årliga kostnader på 3,4–4,3 miljarder EUR för mobilnätsoperatörer, medan investeringarna i betrodda leverantörer samtidigt kan öka med upp till 2 miljarder EUR per år. Dessutom förväntas de förenklade och minskade efterlevnadskraven främja

kostnadsbesparingar för företagen på upp till 14,6 miljarder EUR. Vidare skulle medborgarna, myndigheterna och företagen åtnjuta fördelar i form av en förbättring av EU:s övergripande cybersäkerhetsstatus och tekniska suveränitet samt av stimulerad innovation och konkurrenskraft, som till stor del väntas kompensera för de ursprungliga utgifterna på lång sikt.

Konkurrenskraft: Genom minskad marknadsfragmentering och harmoniserade bestämmelser medför de rekommenderade alternativen ökad konkurrenskraft i hela EU, vilket förser företagen med tydligare vägar till efterlevnad och innovation.

Kontroll av klimatförenlighet: Vid bedömningen beaktades varje alternativs potentiella miljöpåverkan. Särskild uppmärksamhet ägnades åt energieffektivitet, reserelaterade utsläpp och konsolidering av infrastrukturen. De rekommenderade alternativen A.2, B.2 och C.2 har begränsad miljöpåverkan, medan D.3 är miljöneutralt, med beaktande av produkters livscykel och övergångsperioder för ersättning av viktiga tillgångar. Detta är förenligt med EU:s åtagande om hållbarhet.

Digitalt som standard: Tonvikten på förenklade digitala processer visar på EU:s åtagande för en strategi enligt principen ”digitalt först”, för att säkerställa ett snabbare och mer tillförlitligt datautbyte och beslutsfattande. Alternativ D.3 skulle också kunna ha en stor inverkan på digitaliseringen, eftersom det skulle innebära ersättning av komponenter från entiteter som är etablerade i eller kontrolleras av entiteter från tredjeländer som utgör cybersäkerhetsproblem.

Förenkling och minskad administrativ börda: De rekommenderade alternativen bidrar till förenkling genom att tillämpningsområdet förtydligas och åtgärder vidtas för att effektivisera efterlevnaden och tillsynen, vilket minskar den administrativa bördan. Man har tagit hänsyn till principen ”en in och en ut” genom att säkerställa att nya skyldigheter uppvägs av minskningar på annat håll.

Slutsats

I denna konsekvensbedömning presenteras en övergripande strategi för att öka EU:s cybersäkerhet, ta itu med ineffektiv lagstiftning och rusta det digitala landskapet för framtida utmaningar. I konsekvensbedömningen rekommenderas en sammanhållen samarbetsstrategi, där politiska reformer har sin grund i de befintliga ramarna, samtidigt som man anpassar sig till den nya tekniska verkligheten. Genom dessa åtgärder strävar EU efter att säkerställa en resilient, konkurrenskraftig och hållbar digital ekonomi.