impl | Implementeringsrådet

2025-08-25
Komm2025/ 00057

Implementeringsrådet
KN 2024:04

Försvarsdepartementet,
Enheten för cyber- och hybridfrågor (ECH)

Justitiedepartementet,
Grundlagsenheten (Ju L6)

Kopia KN NIM

Underlag till svensk ståndpunkt inför kommande EU-förhandling – förslag till digitala paketet

Implementeringsrådets bidrag till svensk ståndpunkt framgår i sin helhet i avsnitt 5. Rådets förslag i sammandrag är:

- Förtydliga och klargör överlapp, motsägelser och terminologin mellan EU-rättsakter inom cybersäkerhet, digitalisering och artificiell intelligens.
- Inför mer enhetliga och förenliga kriterier och krav för inrapportering av incidenter.
- Låt CSA-certifieringen vara giltig för överlappande krav.
- Säkerställ att cybersäkerhetsregleringar inte hindrar dataöverföring eller motarbetar globala dataflöden.

1. Implementeringsrådets uppgift

Implementeringsrådet har i uppgift att bistå regeringen i arbetet med att stärka svenska företags konkurrenskraft genom att undvika implementering över miniminivån och motverka omotiverade regelbördor samt minska administrativa kostnader och andra fullgörandekostnader vid genomförande av EU:s regelverk i svensk rätt. Implementeringsrådets arbete ska utgå ifrån ett företagsperspektiv.

Implementeringsrådet ska lämna underlag och rekommendationer till regeringen, dels som bidrag till svenska ståndpunkter i förhandlingar, dels

om hur EU-rättsakter kan genomföras i svensk rätt på ett sätt som inte är mer långtgående ur ett företagsperspektiv än vad rättsakterna kräver.

Implementeringsrådets arbete har sin utgångspunkt i problembeskrivningar som förmedlats till rådet, främst från branschorganisationer och deras medlemsföretag. Under arbetet med underlagen tas också kontakter med andra som är insatta i respektive sakområde, till exempel myndigheter. Mot bakgrund av den information och kunskap som inhämtats och inom ramen för den aktuella rättsaktens övergripande syfte gör rådet en sammanvägd och självständig bedömning av hur företagsperspektivet kan tillgodoses på ett ändamålsenligt sätt i varje enskilt fall.

I framtagandet av detta yttrande har rådet främst använt sig av underlag som inkommit genom samtal med sakkunniga/näringslivsexperter från Svenskt Näringsliv, Teknikföretagen, SOFF, Almega, TechSverige, Svensk Bankförening, Visita, Transportföretagen, Livsmedelsföretagen, Svensk Handel och Ikem. Implementeringsrådet har därutöver tagit del av skriftliga förslag och sammanställningar från Digital Europe och Orgalim.

Berörda EU-rättsakter

EU-kommissionen har aviserat att ett förslag kallat det digitala paketet (omnibus) ska komma i slutet av 2025. Det är vid författandet av detta yttrande inte fullt ut känt vad som kommer att inkluderas i det digitala paketet från kommissionen. Det finns bland annat information om att revideringar av cybersäkerhetsakten (CSA) kommer att ingå. Tidigare har det diskuterats att även förändringarna av dataskyddsförordningen (GDPR) skulle ingå i detta omnibuspaket. Det har dock förändrats och planeras nu läggas fram separat i början av år 2026 (meddelades vid stakeholderdialog den 15 juli av DG Justice). Detta yttrande ämnar således inte täcka företagens fulla perspektiv och kommande medskick angående revideringar av GDPR.

Mål och syfte med EU-rättsakterna

Revideringar av cybersäkerhetsakten
Planerade revideringar av CSA syftar till att förenkla, säkerställa synergier mellan initiativ som gäller förbättring av unionens beredskap samt att minska den administrativa bördan och effektivisera genomförande för företagen. Målet är att effektivisera cybersäkerhetsåtgärder, stärka

cybermotståndskraften och uppnå en hög gemensam nivå av cybersäkerhet i hela EU.

Revideringarna kommer främst omfatta: Europeiska unionens byrå för säkerhets (ENISA:s) mandat, att utveckla det gemensamma certifieringsramverket för cybersäkerhet (ECCF) för ökad resiliens samt att ta itu med utmaningar relaterade till säkerheten i IKT-leveranskedjan. Revideringarna har initierats av ENISA mot bakgrund av den skyndsamma utvecklingen inom cybersäkerhet, bland annat vad gäller komplexitet och antal attacker. Det har även tillkommit flertalet andra närliggande rättsakter efter införandet av CSA, vilket har påverkat ENISA:s roll och uppdrag.

Införandet av CSA för cirka sex år sedan (år 2019) innebar bland annat att ett gemensamt certifieringsramverk för IKT-produkter och -processer etablerades, European Cybersecurity Certification Framework (ECCF). Det infördes i syfte att bland annat skydda industrier, medborgare och kritisk infrastruktur från interna och externa hot. Det finns bland annat behov av att förbättra certifieringsramverket samt förtydliga roller och ansvar hos olika aktörer genom processen för att stärka säkerheten genom värdekedjan.

Planerade ändringar av dataskyddsförordningen syftar till att förenkla lagstiftningen som trädde i kraft år 2018. Det är ännu inte känt i vilken omfattning dataskyddsförordningen kommer att öppnas upp för revidering.

Införandet av dataskyddsförordningen innebar hårdare krav på hantering av personuppgifter med syftet att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Förordningen omfattar samtliga företag med hantering av personuppgifter.

I Omnibus IV ges förslag om ändring av artikel 30 i GDPR (register över behandling)[1], förändringar som rådet inte kommer beröra närmare i detta yttrande.

2. Var i processen befinner sig förslagen?

Förslaget om det digitala paketet har aviserats i kommissionens arbetsprogram för 2025. Revideringar av cybersäkerhetsakten har varit ute

[1] I nuläget behöver företag med färre än 250 anställda inte föra register över alla personuppgiftsbehandlingar, så länge behandlingen inte innebär särskilda risker. Kommissionen föreslår att detta undantag även ska omfatta företag med upp till 750 anställda, förutsatt att behandlingen inte är av sådan art att den innebär "hög risk" för de registrerade.

för samråd mellan 11 april och 20 juni 2025. Ändringar som är aktuella inom dataskyddförordningen har diskuterats i möte mellan kommissionen och branschledare, branschgrupper och civilsamhällesorganisationer i mitten av juli 2025 och det planeras ett särskilt möte om detta i september.

Formellt förslag från kommissionen om det digitala paketet planeras under Q4 2025, förmodligen i december. Inget skriftligt förslag från kommissionen föreligger ännu. Tillgänglig information framgår bland annat av kommissionens samrådsdokument vad gäller cybersäkerhetsakten.

Trots detta tidiga skede och det relativt begränsade underlaget som finns om förändringarna i det digitala paketet bedömer Implementeringsrådet att det är av vikt att inkomma med ett yttrande. Det utifrån att förslaget bland annat har konsekvenser för en bredd av företagare och att det från berörda branschorganisationer framkommit flertalet synpunkter och medskick samt alternativa förslag. Yttrandet kan utgöra underlag för bilaterala kontakter med kommissionen, inskick i pågående samrådsprocess eller annat påverkansarbete i tidigt skede.

3. Ansvarigt departement

Försvarsdepartementet ansvarar för revideringar av cybersäkerhetsakten medan Justitiedepartementet ansvarar för dataskyddsförordningen, vilka omfattas i detta yttrande. I det slutliga förslaget till digitala paketet (omnibusen) kommer även Finansdepartementet vara ansvarig för berörda akter.

Problembeskrivning ur ett svenskt företagsperspektiv

Regleringar inom digitalisering, cybersäkerhet och automatisering har skett med en hög intensitet vilket medfört att lagstiftningarna samlat upplevs snåriga och inte anpassade till varandra.

Flertalet av vidtalade branschorganisationer ställer sig övergripande neutrala eller positiva till föreslagna revideringar av cybersäkerhetsakten. Bland annat nämns det vara välkommet att ENISA får ett utvidgat mandat och ansvar.

När det gäller dataskyddsförordningen, finns det farhågor bland annat förknippat med om hela förordningen öppnas upp för revidering. Nödvändiga förändringar och korrigeringar bedöms kunna ske utan att

öppna upp hela förordningen. Näringslivet vill fortsatt ha kvar grundprinciperna i GDPR men det finns behov av regelförenkling när det kommer till administrativa bördor där kraven anses oproportionerliga och alltför betungande.

Nedan sammanfattas de huvudsakliga problemområden som fångats upp kopplat till EU-rättsakterna.

Överlappande EU-rättsakter inom det digitala området medför utökade rapporteringskrav

Den snabba utvecklingen och regleringen av digitalisering, cybersäkerhet och artificiell intelligens har gett upphov till överlappningar mellan EU-rättsakter vilket bland annat medfört utökade rapporteringskrav för företagen och i vissa fall dubbelrapporteringar av liknande information till olika myndigheter. Kriterierna för inrapportering av incidenter skiljer sig även åt (tröskelvärden, tidslinjer och rapporteringsmallar) i nuläget och företagen förväntas rapportera in incidenter enligt bland annat GDPR, Network and Information Systems Directive 2 (NIS2), The Digital Operational Resilience Act (DORA) och cyberresiliensförordningen (CRA). Det finns även skillnader i definitionen av ”risk” mellan NIS2, GDPR och cyberresiliensakten.

Det försvårar för företagen att leva upp till kraven i lagstiftningen då det är utmanande och tar tid från produktion/kärnverksamhet att sätta sig in regelverken, de olika rapporteringskriterierna och mallarna samt att rapporteringen sker i olika system. Det gäller i synnerhet de mindre företagen där resurser och kompetenser är mer begränsade.

Exempelvis beskrivs upphovsrättslagen, AI-förordningen samt GDPR relatera och delvis överlappa varandra. Detsamma gäller för plattformsdirektivet, NIS2-direktivet och AI-förordningen som i vissa fall kan ses som komplementära[2]. Det finns behov av att förtydliga förhållandet mellan dessa i syfte att underlätta för företagens regelefterlevnad. Den lag med högst krav bör då utgöra utgångspunkt för harmonisering.

[2] De tre regelverken syftar till att skydda grundläggande rättigheter. NIS2-direktivet fokuserar på säkerhet och integritet, plattformsdirektivet på likabehandling och arbetsvillkor, och AI-förordningen på att säkerställa att AI-system inte skadar hälsa, säkerhet eller demokrati. NIS2-direktivet och AI-förordningen har gemensamma beröringspunkter i frågor om säkerhet och riskhantering, medan plattformsdirektivet och AI-förordningen delar fokus på transparens och skydd av grundläggande rättigheter.

Inom finanssektorn lyfts exemplet om hur CRA och DORA överlappar varandra och det saknas en tydlig hierarki mellan dessa. De båda syftar till att förbättra cybersäkerheten men från olika perspektiv, CRA med horisontella regler för digitala produkter medan DORA omfattar en resiliensram specifik för finanssektorn.

Det finns fler exempel på överlappande lagstiftningar inom området än ovan nämnda[3].

Inkonsekvent terminologi mellan akter, förordningar och direktiv skapar onödig komplexitet och är administrativt krävande

Det råder en terminologiförvirring mellan flertalet regleringar inom det digitala området där lika eller snarlika termer och begrepp definieras olika. Detta leder till utmaningar i att tolka, förstå och efterleva regleringarna för företagen och blir administrativt krävande.

Exempelvis har CSA en definition av "IKT-produkt" och i CRA definieras "produkt med digitala element". Dessa är exempel från övergripande lagstiftning, därtill finns definitionerna av produkter i sektorsspecifika regler som tillkommer. Alla dessa lagar har krav för att produkter ska få släppas ut på EU-marknaden och de tillämpas samtidigt.

Ett annat exempel är de inkonsekventa definitionerna av "väsentlig ändring" i AI-förordningen, CRA och maskinförordningen (MR). Det finns även flertalet definitioner av ”risk” mellan bland annat NIS2, CRA, AI-förordningen och General Product Safety Regulation (GPSR).

Den parallella förekomsten av frivillig certifiering tredjepartsbedömningar av överensstämmelse och egenkontroll skapar förvirring

CSA fungerar för närvarande isolerad från nyligen antagna cyberlagstiftningar, inklusive NIS2-direktivet och CRA. Företag, särskilt de mindre, står inför osäkerhet om hur frivilliga CSA-certifieringssystem interagerar med nya cybersäkerhets- och riskhanteringskrav enligt CRA och NIS2. Den parallella förekomsten av frivillig certifiering enligt CSA, tredjepartsbedömningar av överensstämmelse samt egenkontroll skapar

[3] Business Europe paper – simplification of the digital rulebook (17 juli 2025).

förvirring. Vidare påtalas det av flertalet branschföreträdare/företag att det är av vikt att fortsatt ha CSA-certifieringen primärt som valbar utifrån att det bland annat medger lägre trösklar för marknadstillträde, medför lägre kostnader samt främjar innovation.

Det finns även farhågor om att CRA som för närvarande inte kräver obligatorisk certifiering för någon produktkategori kan komma att förändras i framtida delegerade akter och att det då införs som en skyldighet. För närvarande följer CRA den nya lagstiftningsramen (NLF), som gör det möjligt att använda proportionella bedömningar av risk och cybersäkerhetsaspekter, inklusive egenkontroll för lågriskprodukter.

GDPR kan försvåra informationsöverföring och begränsar internationell dataöverföring

Artikel 10 i dataskyddsförordningen (behandling av personuppgifter som rör fällande domar i brottmål och överträdelser) försvårar i nuläget informationsdelning mellan företag och andra organisationer när de utsätts för exempelvis cybersäkerhetshot. Branschen uttrycker att det är främst den svenska tolkningen av begreppet ”personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott eller därmed sammanhängande säkerhetsåtgärder” som försvårar. Flertalet andra EU-länder har intagit en annan tolkning som inte medför förhinder av informationsdelningen på samma sätt.

Det finns även farhågor kring att GDPR begränsar dataöverföringen globalt (till tredjeland) och således möjligheten att använda och utveckla exempelvis molntjänster. Svenska och finska företag är bland de ledande i att använda molntjänster och det beskrivs vara en viktig del i att utveckla teknikbranschen framgent. Vikten av globala molntjänster och annan digital infrastruktur beskrivs i regeringens strategi för cybersäkerhet Sverige i en digital värld (december 2024).

Motsägelser mellan GDPR och bland annat dataförordningen försvårar och kan hämma innovationskraft hos företagen

Branschen uttrycker även att det finns motsägelser mellan s.k. dataförordningens[4] krav på att tillgängliggöra stora mängder data (inklusive

[4] Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen)

personuppgifter) och dataskyddsförordningens förebyggande förbud mot utlämnande av personuppgifter. Även om det anges att GDPR har företräde vid konflikt mellan de två förordningarna, beskrivs det komplexa samspelet mellan bestämmelserna skapa betydande osäkerheter för företag på teknisk och avtalsmässig nivå. Företagens innovations- och konkurrenskraft kan hämmas när de behöver ägna tid och kraft för att förstå och reda ut motsägelser i lagstiftningarna. Problematiken påtalas bli särskilt tydlig vid personal and non personal data (data som innehåller både personuppgifter och annan data).

Farhågor om att revideringar i GDPR kommer medföra ytterligare komplexitet och administration, samtidigt som lagstiftningen idag upplevs vara svårtolkad

Flertalet företag, i synnerhet mindre företag, upplever fortfarande att det är svårt att tolka GDPR och förstå huruvida de efterlever lagstiftningen eller inte. Dessa utmaningar avspeglar sig bland annat i uppföljningar av efterlevnadsgraden av GDPR bland svenska företag, som visar att ca 37% av småföretag klarar kraven och ca 48% av de större företagen (där flertalet har en så kallad Data Protection Officer).[5] Det kan indikera ett behov av ytterligare vägledning och rådgivning.

4. Implementeringsrådets analys

Berörda branscher och företag

Det digitala paketet och revideringar av CSA och GDPR bedöms slå brett branschmässigt och inkludera såväl större som mindre svenska företag. Det exakta antalet företag som kommer att beröras av revideringarna har varit svårt att uppskatta, då det bland annat finns begränsat med tillgängliga uppgifter om hur många som behandlar personuppgifter och/eller berörs av ändringarna i cybersäkerhetsakten.

Mikro- samt små- och medelstora företag kommer särskilt att påverkas utifrån deras begränsade resurser och kapacitet att sätta sig in i och ställa om utifrån ny lagstiftning. Men även de större företagen påverkas då de innehar en mer omfattande systemstruktur och i flera fall verkar på en global marknad med nationella olikheter i lagstiftningar.

[5] Enligt undersökningar från Entreprenörskapsforum och Integritetsskyddsmyndigheten, IMY.

Konsekvenser för svenska företag

Administrativa kostnader och andra fullgörandekostnader

Inkonsekvent terminologi mellan akter, förordningar och direktiv skapar bland annat onödig komplexitet och det tar tid för företagen att tränga igenom lagstiftningen och veta om de verkligen förstått den korrekt.

Den parallella förekomsten av frivillig certifiering (CSA), tredjepartsbedömningar av överensstämmelse och egenkontroller skapar förvirring och administration för företagen. Det medför även en osäkerhet för företagen om huruvida de uppfyller krav och är dessutom administrativt betungande.

Det finns farhågor att en total omförhandling av GDPR skulle medföra kostnader istället för att minska den administrativa bördan. Det på grund av att det bland annat blir svårt att orientera sig och förstå hur företagen ska ställa om i praktiken för att efterleva lagstiftningen, framför allt för de mindre företagen.

I och med att det inte finns ett färdigt förslag från kommissionen ännu om det digitala paketet är det svårt för företagen att uppskatta omfattningen av kostnaderna som förslagen kommer att medföra. Men exempel på kostnader som skulle kunna uppstå för företagen i samband med implementering av det digitala paketet är:

- Kostnader för konsulthjälp och/eller juristkostnader för att tolka regler och hur företaget ska ställa om för regelefterlevnad.
- Administrativa kostnader i form av exempelvis inläsning, kontakter med ansvariga myndigheter, rapportering till tillsynsmyndigheter, framtagande av nya policys med mera när förändringarna sker.
- Administrativa kostnader för överlappande/fördubblade rapporteringskrav och att sätta sig in i de olika rapporteringsstrukturerna.
- Kostnader för eventuella inköp av nya/uppdaterade systemstöd.

Det finns även delar av branscher där affärsmöjligheter skapas till följd av regelförändringarna, så som IT-konsulter och exempelvis rådgivande konsulttjänster inom GDPR.

Övriga konsekvenser och påverkan på det svenska näringslivets konkurrenskraft

Om de reviderade regleringarna inom det digitala paketet blir för omfattande och krångliga, finns risk att företag avstår från att starta och skala upp affärer eftersom regelbördan blir en tröskel.

Otydliga och betungande regler i GDPR kan göra att företag (av rädsla för att göra fel, på grund av osäkerheter kring vad som är tillåtet eller otillåtet, eller på grund av de höga administrativa kostnaderna som följer), avstår från att utveckla nya digitala produkter och tjänster, särskilt sådana som stöds av AI.

Otydliga och betungade regler i GDPR kan göra att företag, på grund av osäkerheter kring vad som är tillåtet eller otillåtet eller på grund av de höga administrativa kostnaderna som följer, avstår från att utveckla och ta fram nya effektiva och innovativa produkter och tjänster med hjälp av AI. Regleringar i GDPR samt AI-förordningen kan leda till att investeringar i AI och teknisk utveckling inte sker i Europa, en tendens som redan setts inom exempelvis läkemedelsbranschen. Tillgången till stora och kvalitativa datamängder är central för att företagen ska vara en del av denna utveckling.

Det finns även risk att investerarviljan avtar i svenska företag om exempelvis upphovsrätten och skyddet av algoritmer och annan skyddsvärd information avtar som konsekvens av krav på ökad transparens i regelverken.

5. Implementeringsrådets underlag till svensk ståndpunkt i påverkansarbete och inför kommande EU-förhandlingar om det digitala paketet

Förtydliga och klargör överlappning, motsägelser och terminologin mellan EU-rättsakter inom cybersäkerhet, digitalisering och artificiell intelligens

- Använd standardiserade termer och begrepp i EU-regleringarna och gör det obligatoriskt att korsreferera definitioner vid utarbetande av ny lagstiftning. Se även över och anpassa den befintliga lagstiftningen på området.

- Termer och definitioner för produkter, uppkopplade produkter och omfattande ändring behöver få samma lydelse och förklaring i CSA,

GPSR, PLD, maskinförordningen, dataförordningen, CRA med flera regleringar.

- Förtydliga och minska överlappningar mellan EU-rättsakter inom det digitala området. Nedan är exempel på förtydliganden som lyfts av näringslivet:

  - Artikel 5 GDPR[6] principer för behandling av personuppgifter. Anpassa principerna om ändamålsbegränsning och uppgiftsminimering för att möjliggöra träning av AI-system på stora datamängder. Det finns ett behov av att tydliggöra att det är tillåtet att "behandla" uppgifter i syfte att göra dem anonyma och hur den typen av data får användas.

  - Artikel 10 GDPR (behandling av personuppgifter som rör fällande domar i brottmål och överträdelser) har tolkats i Sverige som att den hindrar möjligheten att dela information om cyberhot (till exempel IP-adresser som förekommer i hotaktiviteter). Det vore önskvärt med vägledning från EU-nivå om hur denna artikel ska tolkas.

  - Artikel 22 GDPR[7]. Det finns ett behov av att förtydliga hur automatiserat beslutsfattande ska tillämpas på AI-system och när den mänskliga inblandningen är tillräcklig enligt krav i lagstiftningen.

Inför mer enhetliga och förenliga kriterier och krav för inrapportering av incidenter

- Inför förenliga tröskelvärden, tidslinjer och kriterier för inrapportering av incidenter för att minska den administrativa bördan och öka regelefterlevnad.

[6] Handlar om att uppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska inte anses vara oförenlig med de ursprungliga ändamålen (ändamålsbegränsning).

[7] Handlar om att den registrerade ska ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne.

impl | Implementeringsrådet

- Anpassa tidslinjerna för rapportering av incidenter till GDPR:s tidslinje/timmar modell för att möjliggöra en grundlig inledande bedömning före anmälan.

- Skapa en enda, harmoniserad rapporteringsmall som gäller enligt NIS2, CRA, GDPR och andra relaterade rättsakter.

- Incidentrapporteringen behöver förenklas i takt med att nya cybersäkerhetsregler implementeras. Detta kan uppnås genom att utarbeta tydliga och stegvisa regler för rapportering av incidenter och en enda kontaktpunkt.

Låt CSA-certifieringen vara giltig för överlappande krav

- Låt CSA-certifiering, när den erhållits frivilligt och när den uppfyller relevanta juridiska skyldigheter, vara giltig för överlappande krav i CRA och NIS2. Det i syfte att undvika onödig upprepning av bedömningar eller revisioner.

- Behåll proportionalitetsprincipen vid genomförandet av CRA genom ett upprätthållande av NLF och se till att lågriskprodukter fortsätter att omfattas av möjlighet till egenkontroll, utan att utvidga certifieringskraven utöver vad som är absolut nödvändigt.

Säkerställ att cybersäkerhetsregleringar inte hindrar dataöverföring eller motarbetar globala dataflöden

- Effektivisera och förtydliga kraven i GDPR, dataförordningen och dataförvaltningsakten för att öka rättssäkerheten kring internationella dataflöden.

Kontaktperson i detta ärende är utredningssekreterare Veronica Götherström eller Lena Nordqvist (förnamn.efternamn@regeringskansliet.se)

Beslutad av Implementeringsrådet den 25 augusti 2025.