Ministeriet for
Samfundssikkerhed og Beredskab

KOMITÉNOTAT TIL FOLKETINGETS EUROPAUDVALG

Dato
23-09-2024

Commission implementing regulation (EU) …/… laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

KOM-dokument foreligger uden nummer (komitologiregistret).

Nyt notat.

1. Resumé

Som et led i implementeringen af NIS 2 har Europa-Kommissionen den 27. juni 2024 fremsat forslag til gennemførselsretsakt for det digitale område, som fastlægger tekniske og metodologiske krav til foranstaltninger og definerer, hvad der udgør en væsentlig hændelse, som skal indberettes til myndighederne. Formålet med gennemførselsretsakten er at specificere kravene til sikkerhedsforanstaltninger og yderligere præcisere de tilfælde, hvor en hændelse anses som væsentlig, og dermed skal indberettes til myndighederne. Gennemførselsretsakten omfatter følgende typer af enheder: DNS-tjenesteudbydere, topdomænenavnsadministratorer, udbydere af cloud-computing-tjenester, udbydere af datacentertjenester, udbydere af indholdsleveringsnetværk, udbydere af administrerede tjenester, udbydere af administrerede sikkerhedstjenester, udbydere af onlinemarkedspladser, udbydere af onlinesøgemaskiner, udbydere af platforme for sociale netværkstjenester og udbydere af tillidstjenester.

Forslaget blev senest drøftet på et møde i komiteen for cybersikkerhed den 9. september 2024 og forventes sat til afstemning den 2. oktober 2024.

Regeringen støtter det overordnede formål med forslaget.

Der skønnes at være betydelige statsfinansielle og erhvervsøkonomiske konsekvenser. Forslaget forventes endvidere at have konsekvenser for cybersikkerhedsniveauet i Danmark. Der er ikke foretaget en konsekvensvurdering af kravene i gennemførselsretsakten, men flere dele af den vurderes at kunne medføre byrder for både virksomheder og myndigheder. Dog vurderes byrderne i Kommissionens seneste reviderede forslag at stå mål med den samfundsmæssige værdi. Samtidig er flere af kravene i det reviderede forslag blevet gjort mere operationelle, hvilket vurderes at gøre det lettere at vurdere, om en hændelse er væsentlig og skal indberettes. Regeringen agter derfor at stemme for forslaget, idet der lægges afgørende vægt på, at forslagets krav ikke medfører statsfinansielle konsekvenser og administrative byrder for erhvervslivet, der ikke står mål med den sikkerheds- og samfundsmæssige værdi af indberetningerne af væsentlige hændelser. Endvidere lægges der stor vægt på, at forslagets tværgående kriterier for, hvad der udgør en væsentlig hændelse gøres klarere, er mulige for de omfattede enheder at vurdere inden for de fastsatte tidsrammer og fastsættes på et niveau, så kun hændelser af samfundsmæssig eller væsentlig økonomisk betydning indberettes til myndighederne. Regeringen er desuden positiv over for, at enhederne skal have en risikobaseret tilgang til implementeringen af de teknologiske og metodologiske krav til foranstaltninger.

2. Baggrund

Den 14. december 2022 blev der opnået enighed mellem Rådet og Europa-Parlamentet om direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148 (KOM (2020) 823 final). Forslaget (NIS 2) bygger på og ophæver direktiv (EU) 2016/1148 om sikkerhed i net- og informationssystemer (NIS-direktivet), som er den første EU-retsakt om cybersikkerhed og indeholder retlige foranstaltninger, der skal styrke det generelle cybersikkerhedsniveau i Unionen.

Som led i implementeringen af direktivet skal der vedtages en gennemførelsesretsakt med henblik på at fastsætte de tekniske og metodologiske krav til de foranstaltninger, der er omhandlet i NIS 2-direktivets artikel 21, stk. 2, og hvad der udgør en væsentlig hændelse som omhandlet i artikel 23, stk. 3. Gennemførselsretsakten angår DNS-tjenesteudbydere, topdomænenavnsadministratorer, udbydere af cloudcomputingtjenester, udbydere af datacentertjenester, udbydere af indholdsleveringsnetværk, udbydere af administrerede tjenester, udbydere af administrerede sikkerhedstjenester, udbydere af onlinemarkedspladser, udbydere af onlinesøgemaskiner, udbydere af platforme for sociale netværkstjenester og udbydere af tillidstjenester.

Forslaget behandles efter undersøgelsesproceduren i komitéen for cybersikkerhed. Undersøgelsesproceduren indebærer, at Kommissionen skal vedtage forslaget, hvis et kvalificeret flertal stemmer for. Hvis et kvalificeret flertal derimod stemmer imod, må Kommissionen ikke vedtage forslaget. Hvis der hverken er kvalificeret flertal for eller mod forslaget, kan Kommissionen enten vedtage forslaget eller fremsætte et revideret forslag.

Forslaget blev senest drøftet på et møde i komitéen den 9. september 2024, og seneste udkast er modtaget den 18. september 2024. Forslaget forventes sat til afstemning på et møde den 2. oktober 2024.

3. Formål og indhold

Gennemførselsretsakten forventes efter afstemning at blive vedtaget af Kommissionen d. 17. oktober 2024. Herefter offentliggøres den i Den Europæiske Unions Tidende, og træder i kraft 20 dage efter.

Formålet med gennemførselsretsakten er at specificere kravene til sikkerhedsforanstaltninger og yderligere præcisere de tilfælde, hvor en hændelse anses som væsentlig, og dermed skal indberettes til myndighederne. Gennemførselsretsakten omfatter følgende type af enheder: DNS-tjenesteudbydere, topdomænenavnsadministratorer, udbydere af cloud-computingtjenester, udbydere af datacentertjenester, udbydere af indholdsleveringsnetværk, udbydere af administrerede tjenester, udbydere af administrerede sikkerhedstjenester, udbydere af onlinemarkedspladser, udbydere af onlinesøgemaskiner, udbydere af platforme for sociale netværkstjenester og udbydere af tillidstjenester.

Forslaget til gennemførelsesretsakt opstiller forslag til tværgående kriterier for, hvornår en hændelse anses som væsentlig ift. de omfattede enheder.

En hændelse vil således blive defineret som væsentlig, hvis den har forårsaget eller er i stand til at forårsage:

- Et økonomisk tab for den relevante enhed, der overstiger EUR 500.000 eller 5 pct. af den relevante enheds samlede årlige omsætning i det foregående regnskabsår, alt efter hvad der er lavest.
- Uautoriseret adgang til forretningshemmeligheder.
- Betydelig skade på en fysisk persons helbred eller død.
- Ondsindet og uautoriseret adgang til netværks- og informationssystemer.

Hændelser skal ligeledes ses som væsentlige, hvis den samme hændelse sker af samme årsag to gange inden for 6 måneder, og disse hændelser tilsammen har givet eller kan give et økonomisk tab på EUR 500.000 eller 5 pct. af den relevante enheds samlede årlige omsætning i det foregående regnskabsår, alt efter hvad der er lavest.

I gennemførelsesretsaktens foreslås ligeledes særlige kriterier for, hvornår en hændelse skal anses som væsentlig for specifikke typer af enheder, herunder kvantitative kriterier for, hvor stor en del, og i hvor lang tid, en tjeneste må være utilgængelig eller have nedsat ydeevne. Tjenester må afhængigt af typen f.eks. kun være fuldstændig utilgængelige i 0-30 minutter, eller delvis utilgængelig i én time, før der er tale om en væsentlig hændelse. Der foreslås kvalitative og kvantitative kriterier for kompromittering af fortroligheden, integriteten og tilgængeligheden af data relateret til enhedens tjeneste. For datacentre og tillidstjenesteudbyder anses en hændelse ligeledes for væsentlig, hvis enhedens fysiske adgangsbegrænsning kompromitteres.

I gennemførselsretsaktens bilag foreslås uddybende tekniske og metodologiske krav til foranstaltninger for cybersikkerhedsrisikostyring, der henvises til i artikel 21, stk. 2, punkt (a) til (j), i NIS 2-direktivet.

4. Europa-Parlamentets udtalelser
Ikke relevant.

5. Nærhedsprincippet
Der er tale om gennemførelsesforanstaltninger til en allerede vedtaget retsakt. Det er derfor regeringens vurdering, at forslagene er i overensstemmelse med nærhedsprincippet.

6. Gældende dansk ret
Implementeringen af det gældende NIS-direktiv er gennemført via en række love og bekendtgørelser inden for de nuværende omfattede respektive ministerområder. Implementeringen er sket efter sektoransvarsprincippet, hvorefter de sektoransvarlige myndigheder er kompetente myndigheder i direktivets forstand og har implementeret direktivet i relevant lovgivning på deres områder. Den decentrale danske implementering har først og fremmest fokus på det eksisterende direktivs forpligtelser for "operatører af væsentlige tjenester" og "udbydere af digitale tjenester". Begge begreber forlades med NIS 2.

Gennemførelsesretsakten har i forhold til det nugældende direktiv betydning for lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester (LOV nr. 436 af 437 af 08/05/2018). Loven stiller bl.a. krav om sikkerhed og underretningspligt for topdomænenavnsadministratorer, DNS tjenesteudbyder (DNS – Domænenavnesystem), udbydere af onlinemarkedspladser, udbydere af onlinesøgemaskine og udbydere af cloud computing-tjenester.

7. Konsekvenser
<u>Lovgivningsmæssige konsekvenser</u>
En vedtagelse af forslaget vil have betydning for arbejdet med den danske implementering af NIS-2-direktivet. Dette skyldes, at der med gennemførselsretsakten fastsættes kriterier for, hvornår der for de relevante enheder (digitale tjenester) er tale om væsentlige hændelser.
Det bemærkes herudover, at selvom der er tale om kriterier, der vedrører digitale tjenester, kan de kriterier, der fastsættes med gennemførselsretsakten, potentielt have betydning for, hvordan hændelser (og foranstaltninger) for andre enheder vil blive defineret, da Kommissionen jf. NIS 2-direktivets artikel 23 stk. 11, vil kunne vedtage gennemførselsretsakter, der også gælder andre enheder. For nuværende er man ikke bekendt med, at der skulle være planlagt fremsættelse af yderligere gennemførselsretsakter.

Det bemærkes, at nærværende gennemførselsretsakt for nuværende kun vedrører de omtalte enheder og udbydere.

Økonomiske konsekvenser

Statsfinansielle konsekvenser
Gennemførelsesretsakten vurderes at have statsfinansielle konsekvenser. De statsfinansielle konsekvenser vedrører dels ministeriernes omkostninger forbundet med at implementere de specificerede krav i gennemførselsretsakten, da flere ministerier forventes at blive underlagt denne, dels at føre tilsyn med de omfattede enheders efterlevelse af gennemførelsesretsaktens bestemmelser og håndtering af hændelser. Det vurderes, at de udgiftsdrivende elementer i forslaget er relateret til tærskelværdierne for indberetningen af cybersikkerhedshændelser for de udpegede sektorer i NIS 2. Det forventes at medføre et øget behov for årsværk til NIS 2-tilsynsmyndigheden ifm. opgaver relateret til sagsbehandlingstid og håndtering indberetninger af cybersikkerhedshændelser. Disse meromkostninger skønnes at være betydelige. Det bemærkes, at skønnet for meromkostningerne er forbundet med en usikkerhed, da antallet af omfattede statslige, regionale og kommunale enheder ikke er fastlagt grundet manglende afklaring vedr. forslagets definition af begrebet "udbydere af administrerede tjenester". På den baggrund er der en risiko for, at alle statslige myndigheder, der drifter fællesoffentlige løsninger, samt kommuner og regioner, der udfører tilsvarende opgaver, vil være omfattet. Det er ligeledes ikke muligt præcist at estimere antallet af hændelsesindberetninger, som tilsynet og CSIRT'en vi skulle forholde sig til jf. afsnit om erhvervsøkonomiske konsekvenser.

Forhandling af gennemførselsretsakten har resulteret i lempelser, der medfører færre statsfinansielle konsekvenser sammenlignet med de tidligere udkast. Selvom disse nu vurderes at blive lavere, skønnes de alligevel at være betydelige som følge af gennemførselsretsaktens tekniske og metodologiske krav til enhedernes hændelsesindberetning og sikkerhedsforanstaltninger.

Det vurderes, at der bør foretages en yderlig konsekvensvurdering, når det endelige forslag er vedtaget.

Samfundsøkonomiske konsekvenser
Ikke relevant.

Erhvervsøkonomiske konsekvenser
Gennemførelsesretsakten vurderes at have betydelige erhvervsøkonomiske konsekvenser. På baggrund af input fra erhvervslivet vurderes forslaget at have mindre erhvervsøkonomiske konsekvenser for store virksomheder med en høj modenhed, mens de erhvervsøkonomiske konsekvenser for andre typer af omfattede virksomheder kan være væsentlige. Således har antallet af estimerede årlige indberetninger i svarene fra de adspurgte virksomheder et spænd fra under 10 til 1000.

Det bemærkes, at forhandling af gennemførselsretsakten har resulteret i lempelser, der også må forventes at medføre færre erhvervsmæssige konsekvenser. Der udestår imidlertid en nærmere konsekvensvurdering af forslaget i sin endelige form.

Andre konsekvenser og beskyttelsesniveauet
Forslaget forventes potentielt at medføre konsekvenser for cybersikkerhedsniveauet i Danmark, da en potentiel højere indberetningsfrekvens af cybersikkerhedshændelser kan medføre, at tilsynsmyndigheden har mindre tid til at håndtere opgaver afledt af større cybersikkerhedshændelser fra de udpegede sektorer. Dette afhænger i høj grad af, hvor mange indberetninger forslaget vil føre til, hvilket er behæftet med væsentlig usikkerhed.

En større mængde indberetninger af både samfundskritisk og ikke-samfundskritisk karakter forventes dog at have en positiv konsekvens, da det muliggør generering af data til brug for myndighedernes generelle overblik på cybersikkerhedsområdet, og dertilhørende vejledningsarbejde.

8. Høring

Sagen har været sendt i høring i EU-specialudvalget for digitalisering med frist for bemærkninger den 16. september 2024. Der er indkommet høringssvar fra Dansk standard, Teleindustrien (TI) og ingeniørforeningen (IDA).

Det bemærkes, at det for flere af høringssvarene gør sig gældende, at der henvises til en tidligere udgave af gennemførelsesretsakten og regeringens generelle holdning hertil, som blev fremlagt i SPU-høring den 16. september 2024.

Dansk Standard
Dansk Standard takker for muligheden for at bidrage med høringssvar. Vi ser den danske implementering af NIS 2-direktivet som et vigtigt område. Som Dansk Standard tidligere har fremhævet i vores høringssvar til det danske lovudkast, så vurderer vi, at standarder og standardisering spiller en central rolle i at overholde kravene i NIS 2 og den kommende danske implementering af direktivet.

Teleindustrien (TI)
Teleindustrien (TI) takker for muligheden for at bidrage til høringen om NIS 2-gennemførselsretsakt under NIS 2-direktivets artikel 21, stk. 2 og 23, stk. 3

TI kan støtte oplægget til regeringens holdning til NIS 2-gennemførselsretsakt, herunder at:

- Regeringen lægger afgørende vægt på, at forslagets krav ikke medfører statsfinansielle konsekvenser og administrative byrder for erhvervslivet, der ikke står mål med den sikkerheds- og samfundsmæssige værdi af indberetningerne af væsentlige hændelser.

- Regeringen lægger stor vægt på, at gennemførselsretsakten ikke medfører uforholdsmæssige eller unødige økonomiske byrder.

- Regeringen er positiv over for, at enhederne skal have en risikobaseret tilgang til implementeringen af de teknologiske og metodologiske krav til foranstaltninger.

- Regeringen lægger stor vægt på, at forslagets tværgående kriterier for, hvad der udgør en væsentlig hændelse gøres klarere, og er mulige for de omfattede enheder at vurdere inden for de fastsatte tidsrammer og fastsættes på et niveau, så kun hændelser af samfundsmæssig eller væsentlig økonomisk betydning indberettes til myndighederne.

- Regeringen lægger vægt på, at kravet om at indberette gentagende hændelser udgår af gennemførselsretsakten. Regeringen mener, at der er stor risiko for, at dette krav pålægger en administrativ byrde, der ikke står mål med den samfundsmæssige værdi af indberetningerne.

- Regeringen er positiv over for, at der fastlægges forskellige kriterier for indberetning af hændelser til forskellige typer enheder som fx udbydere af datacentertjenester og udbydere af onlinemarkedspladser. Imidlertid kendetegnes flere af kriterierne ved at sætte tærsklen for, hvad der skal indberettes, meget lavt. Regeringen lægger derfor stor vægt på, at tærsklerne for, hvad der skal forstås som en væsentlig hændelse, sættes højere.

IDA
Grundet den korte tidsfrist, som der er forståelse for, er der tale om ganske korte bemærkninger.

IDA er positive overfor den fremlagte kritiske holdning til forslaget, dog med følgende bemærkninger:

IDA noterer sig, at regeringen grundlæggende anerkender, at ” udviklingen i cybertruslerne sammenholdt med vores udbyggende digitale infrastruktur betyder, at cyberangreb har gode forudsætninger for at sprede sig i og på tværs af sektorer og lande.”

IDA forventer, at regeringen går ind i forhandlinger med dette som grundlag. IDA er enige i bemærkningen om, at ”hvis kriterierne sættes for lavt, eller er svære at fortolke, kan det påvirke de omfattede enheders it-sikkerhedsarbejde negativt, da det risikerer at trække fokus væk fra andre opgaver, og det kan unødigt bebyrde myndighederne med sagsbehandling af indberetninger, der ikke er vigtige”
IDA finder det meget vigtigt, at reglerne bliver så klare og gennemskuelige og dermed så lette at efterleve som muligt. IDA er også enige i, at ”Regeringen er positiv over for, at enhederne skal have en risikobaseret tilgang til implementeringen af de teknologiske og metodologiske krav til foranstaltninger.”

IDA er for så vidt også enig i, at "Regeringen lægger stor vægt på, at forslagets tværgående kriterier for, hvad der udgør en væsentlig hændelse gøres klarere, er mulige for de omfattede enheder at vurdere inden for de fastsatte tidsrammer og fastsættes på et niveau, så kun hændelser af samfundsmæssig eller væsentlig økonomisk betydning indberettes til myndighederne." NIS 2 implementeringen bliver kun effektiv, hvis der faktisk er ressourcer til at føre tilsyn og give vejledning.

Dog mener IDA, at når det handler om digitale platforme og services m.v., så er der et væsentlig hensyn at tage til private forbrugere/borgere på de forskellige platforme og digitale tjenester. Nogle typer digitale platforme/kommunikationstjenester/indholdsleveringsnetværk m.v. ligger inde med eller er formidlere af data, der forventes at være krypterede (f.eks. indenfor psykiatrien og børneområdet) eller indeholder personfølsomme data såsom kopi af pas eller kørekort og lignende. Selvom det kan være svært at opgøre de økonomiske tab, så kan det være til stor skade for den enkelte forbruger/borger, hvis sådanne følsomme data bliver hacket og lækket eller misbrugt til afpresning etc., ligesom det kan bidrage til generel utryghed, digital aversion og manglende tillid til myndigheder, hvilket i sig selv kan være et formål med større hackerangreb. Dette vil langt fra være relevant for alle de nævnte typer tjenester, platforme og services, men IDA mener, at det er et relevant kriterie at tage hensyn til.

9. Generelle forventninger til andre landes holdninger

Det forventes, at de fleste medlemsstater vil kunne støtte forslaget, da Kommissionen i det senest revurderede udkast har taget hensyn til medlemsstaternes væsentligste kritikpunkter i forhold til Kommissionens oprindelige forslag.

Der forventes således at være et kvalificeret flertal for forslaget blandt medlemsstaterne for det samlede forslag.

10. Regeringens generelle holdning

Regeringen hilser forslaget velkommen og er som udgangspunkt positiv over for, at forslaget medfører en betydelig harmonisering på tværs af EU mht. virksomheder, der leverer tjenester på det digitale område. Regeringen anerkender, at udviklingen af cybertruslen sammenholdt med vores udbyggede digitale infrastruktur betyder, at cyberangreb har gode forudsætninger for at sprede sig i og på tværs af sektorer og lande.

Regeringen lægger afgørende vægt på, at forslagets krav ikke medfører statsfinansielle konsekvenser og administrative byrder for erhvervslivet, der ikke står mål med den sikkerheds- og samfundsmæssige værdi af indberetningerne af væsentlige hændelser. Regeringen finder at, hvis kriterierne sættes for lavt eller er svære at fortolke, kan det påvirke de omfattede enheders it-sikkerhedsarbejde negativt, da det risikerer at trække fokus væk fra andre opgaver, hvilket unødigt kan bebyrde myndighederne med sagsbehandling af indberetninger, der ikke er vigtige.

Regeringen lægger stor vægt på, at gennemførselsretsakten ikke medfører uforholdsmæssige eller unødige økonomiske byrder.

Regeringen er positiv over for, at enhederne skal have en risikobaseret tilgang til implementeringen af de teknologiske og metodologiske krav til foranstaltninger.

Regeringen lægger stor vægt på, at forslagets tværgående kriterier for, hvad der udgør en væsentlig hændelse gøres klarere, er mulige for de omfattede enheder at vurdere inden for de fastsatte tidsrammer og fastsættes på et niveau, så kun hændelser af samfundsmæssig eller væsentlig økonomisk betydning indberettes til myndighederne.

Regeringen lægger vægt på, at kravet om at indberette gentagende hændelser udgår af gennemførselsretsakten. Regeringen mener, at der er stor risiko for, at dette krav pålægger en administrativ byrde, der ikke står mål med den samfundsmæssige værdi af indberetningerne, da dette vil kræve at enhederne opretholder et register over alle større og mindre hændelser. Regeringen finder, at de sektorspecifikke kriterier allerede sikrer, at hændelser med kritisk indvirkning på enheden evne til at levere deres tjenester indberettes.

Regeringen er positiv over for, at der fastlægges forskellige kriterier for indberetning af hændelser til forskellige typer enheder som f.eks. udbydere af datacentertjenester og udbydere af onlinemarkedspladser. Imidlertid er der usikkerhed forbundet med erhvervsøkonomiske og sikkerhedsmæssige konsekvenserne af de foreslåede tærskelsværdier. I lyset af disse usikkerheder lægger regeringen derfor stor vægt på, at tærsklerne for, hvad der skal forstås som en væsentlig hændelse, sættes højt.

Regeringen hilser det velkomment, at Kommissionen under forhandlingerne har imødekommet medlemsstaterne væsentlige indvendinger i forhold til Kommissionens oprindelige forslag.

Med afsæt i overstående agter regeringen på den baggrund at stemme for forslaget, idet regeringen støtter forslagets overordnet formål. Såfremt der lægges op til, at forslagets krav medfører statsfinansielle konsekvenser og administrative byrder for erhvervslivet, der ikke står mål med den sikkerheds- og samfundsmæssige værdi af indberetningerne af væsentlige hændelser, agter Danmark at stemme imod forslaget.

11. Tidligere forelæggelse for Folketingets Europaudvalg
Sagen har ikke tidligere været forelagt Folketingets Europaudvalg.

Sagen skønnes at skulle forelægges Folketingets Europaudvalg med henblik på orientering.