Regeringskansliet
Faktapromemoria 2020/21:FPM72

Direktiv om resiliens inom kritiska enheter

2020/21:FPM72

Justitiedepartementet

2021-01-20

Dokumentbeteckning

COM (2020) 829
Förslag till Europaparlamentets och rådets direktiv om resiliens inom kritiska enheter

Sammanfattning

Kommissionens förslag den 16 december 2020 till ett direktiv om resiliens inom kritiska enheter återspeglar prioriteringarna i kommissionens strategi för EU:s säkerhetsunion 2020–2025, som pekar på behovet av förbättrad resiliens inom kritiska enheter. Förslaget syftar till att bättre återspegla både nuvarande och förväntade framtida risker, det alltmer täta och ömsesidiga beroendet mellan olika sektorer samt beroendet mellan fysisk och digital infrastruktur. Det föreslagna direktivet är tänkt att ersätta den nuvarande EU-regleringen om europeisk kritisk infrastruktur från 2008.

Förslaget syftar till att skapa ett ramverk som ska ge stöd till medlemsstaterna avseende säkerställande av kritiska enheters förmåga att förebygga, motstå och hantera störningar eller avbrott i verksamheten. Detta ska gälla oavsett om störningen eller avbrottet har föranletts av t.ex. naturolyckor, terroristattacker, pandemier eller andra allvarliga händelser. Förslaget avser följande sektorer: *energi, transporter, bankverksamhet, infrastruktur för finansiella marknader, hälso- och sjukvård, dricksvattenförsörjning, avlopp, digital infrastruktur, offentliga tjänster och rymden*. Enligt förslaget ska medlemsstaterna bl.a. ta fram en strategi för säkerställande av resiliensen inom kritiska enheter samt att ansvariga för kritiska enheter ska göra riskbedömningar, vidta åtgärder för att stärka sin resiliens och rapportera störningar och avbrott till nationella myndigheter.

Regeringen välkomnar en revidering av den nuvarande EU-regleringen om europeisk kritisk infrastruktur. Att stärka robustheten för kritiska enheter är av yttersta vikt såväl på medlemsstatsnivå som på EU-nivå. En viktig utgångspunkt är dock att medlemsstaternas ansvar för att skydda den nationella säkerheten säkerställs.

Förslaget

1.1 Ärendets bakgrund

Förslaget återspeglar prioriteringarna i kommissionens strategi för EU:s säkerhetsunion 2020–2025 och som pekar på behovet av förbättrad resiliens inom kritiska enheter. Arbetet ska bättre återspegla både nuvarande och förväntade framtida risker, det alltmer täta och ömsesidiga beroendet mellan olika sektorer samt beroendet mellan fysisk och digital infrastruktur. Det föreslagna direktivet är tänkt att ersätta direktivet om europeisk kritisk infrastruktur (ECI-direktivet) från 2008.

I juni 2004 beslutade rådet om ett program för skydd av kritisk infrastruktur (European Programme for Critical Infrastructure Protection - EPCIP). Initiativet hade sin grund i de behov som identifierats efter terrorhandlingarna i Madrid år 2004. Inom ramen för EPCIP betonades att särskilt fokus skulle ägnas åt gränsöverskridande infrastruktur, dvs. infrastruktur vars bortfall får stora samhällskonsekvenser för två eller fler medlemsstater. EPCIP benämner sådan infrastruktur som europeisk kritisk infrastruktur.

I november 2005 publicerade kommissionen en grönbok om ett europeiskt program för skydd av kritisk infrastruktur.

Den 12 december 2006 presenterade kommissionen sitt förslag till direktiv för skydd av europeisk kritisk infrastruktur (KOM [2006] 787).

Den 31 oktober 2008 presenterades ett förslag till rådets beslut om inrättande av nätverket för varningar om hot mot kritisk infrastruktur (CIWIN) vilket resulterade i ett direktiv samma år. Direktivet granskades 2012 och utvärderades 2019 (SWD (2019) 308 final).

Det nu aktuella förslaget till direktiv presenterades av kommissionen den 16 december 2020.

Förslaget utgör en del i ett paket av åtgärder som syftar till att ytterligare förbättra resiliensen både i den digitala och fysiska infrastrukturen hos den offentliga och privata sektorn, behöriga myndigheter och unionen i dess helhet. I paketet ingår även en ny cybersäkerhetsstrategi, EU:s strategi för

cybersäkerhet för ett digitalt decenium (The EU's Cybersecurity Strategy for the Digital Decade) och Förslag till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam nivå på cybersäkerhet i hela unionen (KOM (2020) 823) (Directive on measures for a high common level of cybersecurity across the UnionNIS2). Detta går i linje med kommissionens prioriteringar att skapa ett Europa rustat för den digitala tidsåldern (Europe fit for the digital age) som ska se till att den digitala omställningen fungerar för alla människor och företag.

1.2 Förslagets innehåll

Förslaget syftar till att skapa ett ramverk som ska ge stöd till medlemsstaterna avseende säkerställande av kritiska enheters förmåga att förebygga, motstå och hantera störningar eller avbrott i verksamheten. Detta ska gälla oavsett om störningen eller avbrottet har föranletts av t.ex. naturolyckor, terroristattacker, pandemier eller andra allvarliga händelser. Förslaget avser följande sektorer: *energi, transporter, bankverksamhet, infrastruktur för finansiella marknader, hälso- och sjukvård, dricksvattenförsörjning, avlopp, digital infrastruktur, offentliga tjänster och rymden*.

I förslaget anges att

- medlemsstaterna ska ta fram en strategi för säkerställande av resiliensen inom kritiska enheter,
- ansvariga för kritiska enheter ska göra riskbedömningar, vidta åtgärder för att stärka sin resiliens och rapportera störningar och avbrott till nationella myndigheter,
- kritiska enheter som tillhandahåller tjänster till eller i minst en tredjedel av medlemsstaterna ska bli föremål för översyn och rådgivning från kommissionen,
- kommissionen kommer att erbjuda risköversikter, metodstöd och övningar för att kunna testa resiliensen i kritiska enheter,
- gränsöverskridande samarbete avseende implementering av direktivet kommer att faciliteras genom en expertgrupp (Critical Entities Resilience Group).

Direktivet förväntas förbättra resiliensen inom kritiska enheter med tillhörande verksamhet, och stärka motståndskraften att hantera risker och störningar. Stärkt resiliens inom kritiska enheter kommer enligt förslaget att bidra till en bättre fungerande inre marknad. Det föreslagna direktivet ska inte tillämpas på områden som regleras av förslaget till Förslag till

Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam nivå på cybersäkerhet i hela unionen (KOM (2020) 823).

1.3 Gällande svenska regler och förslagets effekt på dessa

Förslaget kan komma att påverka närliggande svenska regler inom flera områden, som exempelvis säkerhetsskyddslagstiftningen och lagstiftning om krisberedskap och civilt försvar. Svenska regler avseende resiliens inom kritiska enheter inom olika sektorer kan alltså komma att påverkas. Det kan t.ex. gälla regler för arbetet med riskbedömningar, risk- och sårbarhetsanalyser, förmågeanalyser samt rapportering av störningar och incidenter. Det är dock svårt att i nuläget förutse hur det föreslagna direktivet kommer att påverka svenska regler.

1.4 Budgetära konsekvenser / Konsekvensanalys

Det föreslagna direktivet har konsekvenser för unionens budget. De totala ekonomiska medlen som behövs för att stödja genomförandet av förslaget uppskattas av kommissionen till 42,9 miljoner euro för perioden 2021--2027, varav 5,1 miljoner euro är administrativa utgifter.

2 Ståndpunkter

2.1 Preliminär svensk ståndpunkt

Regeringen välkomnar en revidering av den nuvarande EU-regleringen om europeisk kritisk infrastruktur. Att organisationer och verksamheter som inryms i begreppen kritiska enheter, kritisk infrastruktur och samhällsviktiga verksamhet är robusta och arbetar med att stärka sin motståndskraft är av yttersta vikt Det gäller såväl för de enskilda medlemsstaterna som på EU-nivå. En viktig utgångspunkt är dock att medlemsstaternas ansvar för att skydda nationell säkerhet säkerställs. Direktivet ska inte hindra att medlemsstaterna vidtar de åtgärder som de anser nödvändiga för att skydda den nationella säkerheten. Regeringen anser att det vidare är viktigt att tillvarata erfarenheter från andra processer inom EU som har bäring på direktivet. Regeringen välkomnar därför det tvärsektoriella upplägget i direktivet som kan ge värdefulla synergivinster inom fler områden. Regeringen anser även att viktiga lärdomar kan dras av arbetet inom Nato:s partnerskap för fred som avser grundläggande förmågor inom civil verksamhet (seven baseline requirements).

Regeringen avser i kommande förhandlingar av detta förslag betona vikten av att medlemsstaternas ansvar för att skydda nationell säkerhet säkerställs. Direktivet ska inte hindra att medlemsstaterna vidtar de åtgärder som de anser nödvändiga för att skydda den nationella säkerheten. Regeringen avser att framhålla att det bör vara tydligt hur medlemsstaternas rapportering till kommissionen ska användas samt att den ska ge ett mervärde till arbetet med att stärka resiliensen inom EU. Regeringen anser att rapporteringen ska vara ändamålsenlig och ligga på en aggregerad nivå. Förslagen behöver bevakas och närmare analyseras inför de kommande förhandlingarna.

Vidare är det viktigt att i kommande förhandlingar framhålla vikten av enhetliga begrepp och definitioner inom detta område, i syfte att öka tydligheten i kommande arbete på såväl EU-nivå som nationell nivå.

Det är viktigt att Sverige verkar konstruktivt för att medel används så effektivt som möjligt på de utgifter som ingår i uppgörelsen om EU:s långtidsbudget 2021–2027. Tillkommande uppgifter ska som huvudregel finansieras genom omprioritering av medel inom området eller från andra områden. Riksdagen har vid Sveriges EU-inträde beslutat om principer om neutralitet för statens budget vilket innebär att när ett beslut på EU-nivå föranleder en ökning av den svenska EU-avgiften ska ökningen finansieras genom en utgiftsminskning på det utgiftsområde till vilket EU-åtgärden kan hänföras.

2.2 Medlemsstaternas ståndpunkter

Vid tiden för framtagandet av denna faktapromemoria har några förhandlingar ännu inte inletts i berörd rådsarbetsgrupp.

2.3 Institutionernas ståndpunkter

Europaparlamentets ståndpunkt är ännu inte känd.

2.4 Remissinstansernas ståndpunkter

Förslaget har inte remitterats.

3 Förslagets förutsättningar

3.1 Rättslig grund och beslutsförfarande

Kommissionen har som rättslig grund angett artikel 114 i Fördraget om europeiska unionens funktionssätt (EUF).

Beslut fattas enligt ordinarie lagstiftningsförfarande, dvs. Europaparlamentet och rådet fattar beslut gemensamt.

3.2 Subsidiaritets- och proportionalitetsprincipen

Kommissionen anser att subsidiaritetsprincipen är tillämplig eftersom förslaget inte avser ett område där gemenskapen är ensam behörig. De menar vidare att målen för förslaget inte i tillräcklig utsträckning uppnås av de enskilda medlemsstaterna. De åtgärder som förslaget omfattar bör därför vidtas på gemenskapsnivå men att det är varje enskild medlemsstats uppgift att skydda den kritiska enheter inom statens territorium. Regeringen delar i huvudsak denna bedömning.

Enligt kommissionen är förslaget förenligt med proportionalitetsprincipen då det inte går utöver vad som är nödvändigt för att uppnå målen för ett samarbete mellan medlemsstaterna på området skydd av kritiska enheter. Regeringen delar i huvudsak bedömningarna i förslaget.

4 Övrigt

4.1 Fortsatt behandling av ärendet

Förslaget kommer att börja förhandlas i rådet tidigt under våren 2021, mest troligt i rådsarbetsgruppen för civilskyddsfrågor (PROCIV).

4.2 Fackuttryck/termer

1. ”Kritiska enheter”: en enhet inom offentlig eller privat verksamhet som har identifierats som sådan av en medlemsstat som tillhandahåller en eller flera oundgängliga tjänster, där utförandet av tjänsten är beroende av en medlemsstats kritiska infrastruktur och där

en incident skulle ha en betydande negativ påverkan på samhällsviktig verksamhet som utförs inom olika sektorer.

2. ”Resiliens”: förmågan att förhindra, motstå och återhämta sig från en störning eller ett avbrott i verksamheten.

3. ”Incident”: en händelse som innebär en oönskad och oplanerad störning eller ett avbrott i verksamhet som kan påverka säkerheten och den kritiska entitetens förmåga att bedriva sin verksamhet.

4. ”Infrastruktur”: en tillgång, ett system eller en del därav, som är nödvändigt för att leverera en samhällsviktig tjänst.

5. ”Samhällsviktig tjänst”: en tjänst som är nödvändig för att upprätthålla livsviktiga och nödvändiga samhälleliga funktioner eller ekonomiska verksamheter.

6. ”Risk”: varje omständighet eller händelse som kan ha en potentiell negativ inverkan på motståndskraften hos kritiska enheter.

7. ”Riskbedömning”: en metod för att bestämma riskens art och omfattning genom att analysera potentiella hot och risker och utvärdera befintliga sårbarheter som kan störa eller orsaka avbrott i den kritiska entitetens verksamhet.