EUROPEISKA
KOMMISSIONEN

Bryssel den 16.12.2020
COM(2020) 829 final

2020/0365 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

om kritiska entiteters motståndskraft

{SEC(2020) 433 final} - {SWD(2020) 358 final} - {SWD(2020) 359 final}

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

För att effektivt skydda EU-invånarna behöver Europeiska unionen fortsätta att minska sårbarheterna, bl.a. när det gäller den kritiska infrastruktur som är avgörande för samhällets och ekonomins funktion. EU-invånarnas försörjning och den inre marknadens funktion är beroende av olika infrastrukturer för att de tjänster som krävs för att upprätthålla kritisk verksamhet i samhället och i ekonomin ska kunna tillhandahållas på ett tillförlitligt sätt. Dessa tjänster, som är centrala under normala omständigheter, blir ännu viktigare när EU ska ta itu med effekterna av och utsikterna inför en återhämtning efter covid-19-pandemin. Det betyder att entiteter som tillhandahåller samhällsviktiga tjänster måste vara motståndskraftiga, dvs. kunna stå emot, absorbera, anpassa sig till och återhämta sig från incidenter som kan leda till allvarliga och eventuellt sektors- och gränsöverskridande störningar.

Syftet med detta förslag är att förbättra tillhandahållandet på den inre marknaden av tjänster som är nödvändiga för att upprätthålla centrala samhällsfunktioner eller central ekonomisk verksamhet genom att öka kritiska entiteters motståndskraft som tillhandahåller sådana tjänster. Det avspeglar de uppmaningar om åtgärder som nyligen har utfärdats av rådet[1] och Europaparlamentet,[2] som båda har uppmuntrat kommissionen att se över den nuvarande strategin för att bättre avspegla de ökade utmaningarna för kritiska entiteter och säkerställa en närmare överensstämmelse med direktivet om säkerhet i nätverks- och informationssystem[3]. Detta förslag är förenligt och skapar nära synergier med det föreslagna direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (nedan kallat *det andra direktivet om säkerhet i nätverks- och informationssystem*) som kommer att ersätta direktivet om säkerhet i nätverks- och informationssystem i syfte att ta itu med den ökade sammankopplingen mellan den fysiska och digitala världen genom en lagstiftningsram med kraftfulla åtgärder för motståndskraft för såväl cyberrelaterade som fysiska aspekter, i enlighet med strategin för EU:s säkerhetsunion[4].

Förslaget avspeglar dessutom nationella strategier inom alltfler medlemsstater, som tenderar att betona sektors- och gränsöverskridande ömsesidiga beroenden och i allt större utsträckning baseras på tankar på motståndskraft, där skydd enbart är en aspekt vid sidan av riskförebyggande och riskbegränsning, driftskontinuitet och återställning. Eftersom kritisk infrastruktur också är utsatt för risken att vara potentiell måltavla för terrorism bidrar de åtgärder som anges i detta förslag om att säkerställa kritiska entiteters motståndskraft också till målen för EU:s nyligen antagna agenda för terrorismbekämpning[5].

Europeiska unionen (EU) har länge varit medveten om den Europaomfattande betydelsen hos kritisk infrastruktur. EU inrättade t.ex. det europeiska programmet för skydd av kritisk

---

1 Rådets slutsatser av den 10 december 2019 om kompletterande insatser för förstärkning av motståndskraft och motverkande av hybridhot (14972/19).

2 Rapport om slutsatser och rekommendationer från särskilda utskottet för terrorismfrågor (2018/2044(INI)).

3 Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

4 COM(2020) 605.

5 COM(2020) 795.

infrastruktur 2006[6] och antog direktivet om europeisk kritisk infrastruktur 2008.[7] I direktivet om europeisk kritisk infrastruktur, som enbart är tillämpligt på energi- och transportsektorerna, föreskrivs ett förfarande för att identifiera och klassificera europeisk kritisk infrastruktur vars driftstörning eller förstörelse skulle få betydande gränsöverskridande konsekvenser i minst två medlemsstater. Där fastställs också särskilda skyddskrav för operatörer av europeisk kritisk infrastruktur och behöriga myndigheter i medlemsstaterna. Hittills har 94 europeiska infrastrukturer klassificerats som kritiska. Två tredjedelar av dessa ligger i tre medlemsstater i Central- och Östeuropa. EU:s insatser för motståndskraft hos kritisk infrastruktur sträcker sig dock längre än dessa åtgärder och omfattar sektorsbaserade och sektorsöverskridande åtgärder för bl.a. klimatsäkring, civilskydd, utländska direktinvesteringar och cybersäkerhet.[8] Samtidigt har medlemsstaterna vidtagit egna åtgärder inom detta område som drar åt olika håll.

Därför är det uppenbart att den nuvarande ramen för skydd av kritisk infrastruktur inte är tillräcklig för att bemöta de aktuella utmaningarna för kritisk infrastruktur och dess operatörer. Med tanke på den ökande sammankopplingen mellan infrastruktur, nätverk och operatörer som levererar samhällsviktiga tjänster på den inre marknaden är det nödvändigt att i grunden ändra den nuvarande inriktningen på att skydda specifika tillgångar till att förstärka motståndskraften hos de kritiska entiteter som driver dem.

Den operativa miljö som kritiska entiteter verkar inom har förändrats avsevärt på senare år. För det första är risklandskapet mer komplicerat än 2008 och omfattar i dag naturliga risker[9] (i många fall förvärrade av klimatförändringen), statligt understödda hybridaktioner, terrorism, insiderhot, pandemier och olyckor (t.ex. industriolyckor). För det andra ställs operatörer inför utmaningar när det gäller att integrera ny teknik, som 5G och obemannade fordon, i sin verksamhet och samtidigt hantera de sårbarheter som sådan teknik skulle kunna leda till. För det tredje innebär sådan teknik och andra trender att operatörerna blir allt mer beroende av varandra. Det är tydligt vad detta innebär – en störning som påverkar en operatörs tillhandahållande av tjänster inom en sektor skulle kunna generera kaskadeffekter på tillhandahållandet av tjänster inom andra sektorer och potentiellt även i andra medlemsstater eller i hela unionen.

Som framgår av 2019 års utvärdering av direktivet om europeisk kritisk infrastruktur[10] ger de europeiska och nationella åtgärderna begränsade möjligheter när det gäller att hjälpa operatörerna att hantera de operativa utmaningar som de står inför i dag och de sårbarheter som deras ömsesidiga beroende medför.

Det finns flera orsaker till detta, vilket beskrivs i den konsekvensbedömning som låg till grund för utvecklingen av förslaget. För det första är operatörerna inte fullständigt medvetna om, eller förstår inte fullt ut konsekvenserna av det dynamiska risklandskap som de bedriver sin verksamhet i. För det andra skiljer sig ansträngningarna för motståndskraft kraftigt åt mellan medlemsstater och sektorer. För det tredje erkänns liknande typer av entiteter som

---

6 Meddelande från kommissionen om ett europeiskt program för skydd av kritisk infrastruktur, COM(2006) 786.

7 Rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna.

8 Kommissionens meddelande om en EU-strategi för klimatanpassning, COM(2013) 216. Europaparlamentets och rådets beslut nr 1313/2013/EU av den 17 december 2013 om en civilskyddsmekanism för unionen. Förordning (EU) 2019/452 om upprättande av en ram för granskning av utländska direktinvesteringar i unionen. Direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

9 *Overview of natural and man-made disaster risks the European Union may face*. SWD(2020) 330.

10 SWD(2019) 308.

kritiska av vissa medlemsstater men inte av andra, vilket betyder att jämförbara entiteter får olika mycket officiellt stöd för kapacitetsuppbyggnad (t.ex. i form av vägledning, utbildning av och övning inom organisationen) beroende på var i unionen de är verksamma, och de omfattas av olika krav. Att kraven på och offentligt stöd till operatörer varierar från en medlemsstat till en annan skapar hinder för operatörer som bedriver verksamhet över gränserna, särskilt för kritiska entiteter som bedriver verksamhet i medlemsstater med strängare regelverk. Eftersom tillhandahållande av tjänster och sektorer blir allt mer sammankopplade inom medlemsstaterna och i hela unionen innebär bristande motståndskraft hos en operatör en allvarlig risk för entiteter i andra delar av den inre marknaden.

Utöver att äventyra den inre marknadens funktion kan störningar, särskilt sådana som har gränsöverskridande konsekvenser och eventuellt konsekvenser för hela Europa, få potentiellt allvarliga negativa följder för människor, företag, regeringar och miljön. På individnivå kan störningar också påverka människors möjlighet att resa fritt, arbeta och utnyttja samhällsviktiga offentliga tjänster som t.ex. hälso- och sjukvård. I många fall tillhandahålls dessa och andra centrala tjänster som utgör grunden för det dagliga livet av tätt sammankopplade nät av europeiska företag. En störning hos ett företag i en sektor kan få kaskadeffekter hos en mängd andra ekonomiska sektorer. Slutligen kan störningar som t.ex. stora strömavbrott och allvarliga transportolyckor bidra till att urholka tryggheten och den allmänna säkerheten. De kan utlösa osäkerhet och undergräva förtroendet för kritiska entiteter och för de myndigheter som ansvarar för tillsynen över dem samt för att se till att befolkningen är trygg och säker.

- **Förenlighet med befintliga bestämmelser inom området**

Detta förslag avspeglar prioriteringarna i kommissionens strategi för EU:s säkerhetsunion[11] där det efterfrågas en reviderad strategi för motståndskraft hos kritisk infrastruktur som bättre avspeglar det nuvarande och förväntade framtida risklandskapet, det allt starkare ömsesidiga beroendet mellan olika sektorer och även det allt större ömsesidiga beroendet mellan fysisk och digital infrastruktur.

Det föreslagna direktivet ersätter direktivet om europeisk kritisk infrastruktur och tar även hänsyn till och bygger vidare på andra befintliga och planerade instrument. Det föreslagna direktivet innebär en avsevärd förändring jämfört med direktivet om europeisk kritisk infrastruktur, som enbart är tillämpligt på energi- och transportsektorerna, uteslutande inriktas på skyddsåtgärder och innehåller ett förfarande för att identifiera och klassificera europeisk kritisk infrastruktur genom en gränsöverskridande dialog. För det första skulle det föreslagna direktivet ha en mycket bredare sektorsomfattning och täcka tio sektorer, nämligen energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, offentlig förvaltning och rymdsektorn. För det andra föreskrivs i direktivet ett förfarande för medlemsstaternas identifiering av kritiska entiteter med gemensamma kriterier på grundval av en nationell riskbedömning. För det tredje innehåller förslaget skyldigheter för medlemsstaterna och de kritiska entiteter som de identifierar, inbegripet entiteter av särskild europeisk betydelse, dvs. kritiska entiteter som tillhandahåller samhällsviktiga tjänster till eller i mer än en tredjedel av medlemsstaterna, som skulle omfattas av särskild tillsyn.

När så är lämpligt skulle kommissionen ge de behöriga myndigheterna och kritiska entiteterna stöd för att uppfylla sina skyldigheter enligt direktivet. Dessutom skulle gruppen för motståndskraft hos kritiska entiteter, som är kommissionens expertgrupp och omfattas av det

[11] Meddelande från kommissionen *Strategi för EU:s säkerhetsunion*, COM(2020) 605.

övergripande regelverk som är tillämpligt på sådana grupper, tillhandahålla rådgivning för kommissionen och främja strategiskt samarbete och utbyte av information. Slutligen, eftersom det ömsesidiga beroendet inte stannar vid EU:s yttre gränser, är även samarbete med partnerländer nödvändigt. I det föreslagna direktivet föreskrivs möjligheten till ett sådant samarbete, t.ex. i fråga om riskbedömningar.

Förenlighet med unionens politik inom andra områden

Det föreslagna direktivet har tydliga kopplingar till och stämmer överens med andra sektorsbaserade och sektorsövergripande EU-initiativ om bl.a. klimatsäkring, civilskydd, utländska direktinvesteringar, cybersäkerhet och lagstiftningen om finansiella tjänster. Framför allt är förslaget nära anpassat till och skapar synergier med det föreslagna andra direktivet om säkerhet i nätverks- och informationssystem, som syftar till att förstärka motståndskraften mot alla riskkällor för informations- och kommunikationsteknik (IKT) hos "väsentliga entiteter" och "viktiga entiteter" som uppnår vissa tröskelvärden i ett stort antal sektorer. Syftet med detta förslag till direktiv om kritiska entiteters motståndskraft är att säkerställa att de behöriga myndigheter som utses enligt det här direktivet och de som utses enligt det föreslagna andra direktivet om säkerhet i nätverks- och informationssystem vidtar kompletterande åtgärder och utbyter information när så behövs i fråga om cybermotståndskraft och annan motståndskraft och att särskilt kritiska entiteter i de sektorer som anses vara "väsentliga" enligt det föreslagna andra direktivet om säkerhet i nätverks- och informationssystem också omfattas av mer generella skyldigheter att öka sin motståndskraft för att ta itu med risker som inte är cyberrelaterade. Den fysiska säkerheten i nätverks- och informationssystem i sektorn för digital infrastruktur behandlas på ett heltäckande sätt i det föreslagna andra direktivet om säkerhet i nätverks- och informationssystem som ett led i dessa entiteters hantering av cybersäkerhetsrisker och rapporteringsskyldigheter. Dessutom baseras förslaget på den befintliga lagstiftningen om finansiella tjänster, där det införs heltäckande krav på att finansiella entiteter ska hantera operativa risker och säkerställa driftskontinuitet. Entiteter som tillhör sektorerna för digital infrastruktur och för bank- och finansinfrastruktur bör därför behandlas som entiteter som är likvärdiga med kritiska entiteter enligt detta direktiv med avseende på medlemsstaternas skyldigheter och åtgärder, men detta direktiv skulle inte medföra några ytterligare skyldigheter för dessa entiteter.

Förslaget tar också hänsyn till andra sektorsbaserade och sektorsöverskridande initiativ om t.ex. civilskydd, katastrofriskreducering och anpassning till klimatförändringen. I förslaget erkänns vidare att den befintliga EU-lagstiftningen i vissa fall innebär att entiteter är skyldiga att hantera vissa risker genom skyddsåtgärder. I sådana fall, t.ex. i fråga om luft- eller sjöfartssäkerhet, bör de kritiska entiteterna beskriva dessa åtgärder i sina planer för motståndskraft. Det föreslagna direktivet påverkar inte heller tillämpningen av de konkurrensregler som fastställs i fördraget om Europeiska unionens funktionssätt (EUF-fördraget).

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

- **Rättslig grund**

Till skillnad från direktiv 2008/114/EG, som baserades på artikel 308 i fördraget om upprättandet av Europeiska gemenskapen (motsvarande nuvarande artikel 352 i fördraget om Europeiska unionens funktionssätt, nedan kallat *EUF-fördraget*), har detta förslag till direktiv sin rättsliga grund i artikel 114 i EUF-fördraget, som rör tillnärmning av lagstiftning för att förbättra den inre marknaden. Detta är motiverat med hänsyn till förändringen i direktivets

syfte, räckvidd och innehåll, det ökade ömsesidiga beroendet och behovet av att skapa mer rättvisa villkor för kritiska entiteter. I stället för att skydda en begränsad uppsättning fysiska infrastrukturer vars driftstörning eller förstörelse skulle få betydande gränsöverskridande konsekvenser, är syftet att öka motståndskraften hos de entiteter i medlemsstaterna som är kritiska för tillhandahållandet av tjänster som är nödvändiga för att upprätthålla centrala samhällsfunktioner eller central ekonomisk aktivitet på den inre marknaden inom ett antal sektorer som understödjer funktionen hos många andra sektorer i EU:s ekonomi. På grund av det ökande gränsöverskridande ömsesidiga beroendet mellan tjänster som tillhandahålls med hjälp av kritisk infrastruktur i sådana sektorer skulle en driftstörning i en medlemsstat kunna få konsekvenser i andra medlemsstater eller i unionen som helhet.

Den nuvarande rättsliga ram som har inrättats på medlemsstatsnivå för att reglera de berörda tjänsterna innebär stora skillnader i de skyldigheter som införs, och dessa skillnader kommer sannolikt att öka. Skillnaderna i de nationella regler som kritiska entiteter omfattas av äventyrar inte enbart ett tillförlitligt tillhandahållande av tjänster i hela den inre marknaden utan riskerar också att påverka konkurrensen negativt. Detta beror framför allt på att liknande typer av entiteter som tillhandahåller liknande typer av tjänster betraktas som kritiska i vissa medlemsstater men inte i andra. Det innebär att entiteter som bedriver, eller som vill bedriva, verksamhet i mer än en medlemsstat omfattas av olika skyldigheter när de bedriver verksamhet i hela den inre marknaden och att entiteter med verksamhet i medlemsstater som har strängare krav kan ställas inför hinder jämfört med entiteter i medlemsstater som har mindre stränga regelverk. Dessa skillnader får en direkt negativ effekt på den inre marknadens funktion.

- **Subsidiaritetsprincipen**

En gemensam lagstiftningsram på EU-nivå inom detta område är motiverad med hänsyn till det ömsesidiga beroendet mellan och de gränsöverskridande egenskaperna hos förhållandena mellan operatörerna av kritisk infrastruktur och deras produktion, dvs. samhällsviktiga tjänster. En operatör som är etablerad i en medlemsstat skulle kunna tillhandahålla tjänster i flera andra medlemsstater eller i hela EU genom tätt sammanflätade nätverk. Det betyder att en driftstörning som drabbar den operatören skulle kunna få långtgående konsekvenser i andra sektorer och över nationella gränser. Störningarna kan potentiellt ha konsekvenser i hela Europa, vilket motiverar åtgärder på EU-nivå. Skillnaderna i nationella regler får dessutom en direkt negativ effekt på den inre marknadens funktion. Som framgår av konsekvensbedömningen anser många medlemsstater och berörda parter inom näringslivet att det behövs en mer gemensam och samordnad europeisk strategi för att säkerställa att entiteter har tillräckligt stor motståndskraft mot olika risker som visserligen kan variera något mellan olika medlemsstater men som skapar många gemensamma utmaningar som inte kan hanteras med enbart nationella åtgärder eller av enskilda operatörer.

- **Proportionalitetsprincipen**

Förslaget är proportionerligt i förhållande till det angivna övergripande målet för initiativet. Skyldigheterna för medlemsstater och kritiska entiteter kan i vissa fall medföra en viss ytterligare administrativ börda, t.ex. om medlemsstaterna behöver utveckla en nationell strategi eller om kritiska entiteter måste vidta vissa tekniska och organisatoriska åtgärder, men dessa förväntas i allmänhet vara begränsade. I detta avseende bör det påpekas att många entiteter redan har vidtagit vissa säkerhetsåtgärder för att skydda sin infrastruktur och säkerställa driftskontinuitet.

I vissa fall skulle det dock kunna krävas mer omfattande investeringar för att uppnå efterlevnad av direktivet. Även i sådana fall är dessa investeringar dock motiverade, eftersom de skulle bidra till ökad motståndskraft såväl hos operatörer som på systemnivå och även leda till en mer samstämmig strategi och större förmåga att tillhandahålla tillförlitliga tjänster i hela unionen. Eventuella ytterligare bördor till följd av direktivet väntas dessutom vara avsevärt mycket mindre än kostnaderna för att tvingas hantera och återhämta sig från stora störningar som hotar ett oavbrutet tillhandahållande av tjänster som rör centrala samhällsfunktioner och det ekonomiska välbefinnandet för operatörer, enskilda medlemsstater, unionen och dess invånare mer generellt.

- **Val av instrument**

Förslaget utformas som ett direktiv som syftar till att säkerställa en mer gemensam strategi för kritiska entiteters motståndskraft i ett antal sektorer i hela EU. I förslaget fastställs särskilda skyldigheter för behöriga myndigheter att identifiera kritiska entiteter på grundval av gemensamma kriterier och resultatet av riskbedömningen. Genom ett direktiv går det att säkerställa att medlemsstaterna tillämpar en enhetlig strategi för att identifiera kritiska entiteter och samtidigt ta hänsyn till särdrag på nationell nivå, däribland olika nivåer av riskexponering och ömsesidigt beroende mellan sektorer och över gränser.

3. RESULTAT AV EFTERHANDSUTVÄRDERINGAR, SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

- **Efterhandsutvärderingar/kontroller av ändamålsenligheten med befintlig lagstiftning**

Direktivet om europeisk kritisk infrastruktur utvärderades 2019 med syftet att bedöma genomförandet av direktivet i fråga om dess relevans, samstämmighet, effektivitet, ändamålsenlighet, mervärde för EU och hållbarhet.[12]

I utvärderingen konstaterades att sammanhanget hade förändrats avsevärt sedan direktivet trädde i kraft. Med hänsyn till dessa förändringar konstaterades att direktivet endast delvis var relevant. I utvärderingen konstaterades visserligen att direktivet generellt stämde överens med gällande europeisk sektorsbaserad lagstiftning och riktlinjer på internationell nivå, men det ansågs vara endast delvis ändamålsenligt, på grund av att vissa av direktivets bestämmelser var allmänt hållna. Det konstaterades att direktivet hade genererat mervärde för EU i den mån det hade gett resultat (dvs. en gemensam ram för skyddet av europeisk kritisk infrastruktur) som varken nationella eller andra europeiska initiativ hade kunnat uppnå utan att betydligt längre, dyrare och mindre väldefinierade processer inleddes. Vissa bestämmelser hade dock endast medfört begränsat mervärde för många medlemsstater.

När det gäller hållbarhet förväntades vissa effekter av direktivet (t.ex. gränsöverskridande diskussioner, rapporteringskrav) upphöra om direktivet skulle upphävas utan att ersättas. Det konstaterades i utvärderingen att det finns fortsatt stöd hos medlemsstaterna för att EU ska delta i arbetet med att stärka motståndskraften hos kritisk infrastruktur och att det finns en viss oro för att det skulle kunna uppstå negativa effekter inom detta område, särskilt för skyddet av utsedd europeisk kritisk infrastruktur, om direktivet upphävdes rakt av. Medlemsstaterna var angelägna om att säkerställa att EU:s engagemang på detta område även fortsättningsvis

[12] SWD(2019) 310.

respekterar subsidiaritetsprincipen, stöder åtgärder på nationell nivå och underlättar gränsöverskridande samarbete, även med tredjeländer.

- **Samråd med berörda parter**

Under utvecklingen av detta förslag har kommissionen haft samråd med ett brett spektrum av berörda parter, däribland Europeiska unionens institutioner och organ, internationella organisationer, medlemsstaternas myndigheter, privata entiteter, däribland enskilda operatörer och nationella och europeiska branschorganisationer som företräder operatörer inom många olika sektorer, experter och expertnätverk, däribland det europeiska referensnätverket för skydd av kritisk infrastruktur, universitet och högskolor, icke-statliga organisationer samt allmänheten.

Samrådet med berörda parter genomfördes på flera olika sätt, bl.a. genom en möjlighet för allmänheten att lämna synpunkter på den inledande konsekvensbedömningen för detta förslag, rådgivande seminarier, riktade frågeformulär, bilaterala utbyten och ett offentligt samråd (till stöd för 2019 års utvärdering av direktivet om europeisk kritisk infrastruktur). Den externa uppdragstagare som ansvarade för den genomförbarhetsstudie som låg till grund för utvecklingen av konsekvensbedömningen hade också samråd med många berörda parter, t.ex. genom en onlineundersökning, ett skriftligt frågeformulär, personliga intervjuer och virtuella ”besök på plats” i tio medlemsstater.

Dessa samråd gjorde det möjligt för kommissionen att undersöka effektiviteten, ändamålsenligheten, relevansen, samstämmigheten och EU-mervärdet hos den befintliga ramen för motståndskraft hos kritisk infrastruktur (dvs. utgångsläget), vilka problem den har lett till, olika handlingsalternativ och de specifika konsekvenser som dessa alternativ skulle kunna förväntas leda till. Generellt pekade samråden på ett antal områden där det fanns en övergripande samsyn hos de berörda parterna, inte minst om att den befintliga EU-ramen för motståndskraft hos kritisk infrastruktur borde göras om, med hänsyn till det ökande ömsesidiga beroendet mellan olika sektorer och ett hotlandskap under förändring.

Framför allt var de berörda parterna i allmänhet överens om att en eventuell ny strategi borde bestå av en kombination av bindande och icke-bindande åtgärder, inriktas på motståndskraft snarare än skydd centrerat kring tillgångar, och att den borde ha en tydligare koppling mellan åtgärder som syftade till att förstärka cyberrelaterad och icke-cyberrelaterad motståndskraft. Dessutom ställde de sig bakom en strategi som tar hänsyn till bestämmelser i befintlig sektorslagstiftning, omfattar åtminstone de sektorer som omfattas av det nuvarande direktivet om säkerhet i nätverks- och informationssystem, och mer enhetliga skyldigheter för kritiska entiteter på nationell nivå, som i sin tur borde ha förmåga att utföra en tillfredsställande säkerhetsgranskning av personal som har tillgång till känsliga anläggningar/känslig information. Dessutom föreslog de berörda parterna att en eventuell ny strategi borde skapa möjligheter för medlemsstaterna att utöva förstärkt tillsyn över verksamheten hos kritiska entiteter, men också säkerställa att kritiska entiteter av Europaomfattande betydelse identifieras och har tillräckligt stor motståndskraft. Slutligen argumenterade de för mer finansiering och stöd från EU, t.ex. för genomförande av ett eventuellt nytt instrument, kapacitetsuppbyggnad på nationell nivå och offentlig–privat samordning/samarbete samt utbyte av god praxis, kunskaper och expertis på olika nivåer. Föreliggande förslag innehåller bestämmelser som generellt motsvarar de synpunkter och preferenser som de berörda parterna gav uttryck för.

- **Insamling och användning av sakkunnigutlåtanden**

Som anges i föregående avsnitt har kommissionen tagit hjälp av extern expertis inom ramen för samråden med t.ex. oberoende experter, expertnätverk samt universitet och högskolor för att utveckla detta förslag.

- **Konsekvensbedömning**

I den konsekvensbedömning som låg till grund för utvecklingen av detta initiativ undersöktes olika alternativ för att avhjälpa de generella och specifika problem som beskrevs tidigare. Utöver utgångsläget, som inte skulle innebära någon förändring jämfört med nuvarande situation, undersöktes bl.a. följande alternativ:

– Alternativ 1: Det nuvarande direktivet om europeisk kritisk infrastruktur bibehålls, åtföljt av frivilliga åtgärder inom ramen för det befintliga europeiska programmet för skydd av kritisk infrastruktur.

– Alternativ 2: En översyn görs av det nuvarande direktivet om europeisk kritisk infrastruktur så att det omfattar samma sektorer som det befintliga direktivet om säkerhet i nätverks- och informationssystem och är mer inriktat på motståndskraft. Det nya direktivet om europeisk kritisk infrastruktur skulle innebära ändringar i den befintliga processen för att utse gränsöverskridande europeisk kritisk infrastruktur, inbegripet nya klassificeringskriterier och nya krav på medlemsstater och operatörer.

– Alternativ 3: Det befintliga direktivet om europeisk kritisk infrastruktur ersätts med ett nytt instrument som syftar till att stärka kritiska entiteters motståndskraft i de sektorer som betraktas som väsentliga enligt det föreslagna andra direktivet om säkerhet i nätverks- och informationssystem. Enligt detta alternativ skulle minimikrav fastställas för medlemsstaterna och för de kritiska entiteter som identifieras enligt den nya ramen. Ett förfarande för att identifiera kritiska entiteter som erbjuder tjänster till eller i flera eller samtliga EU-medlemsstater skulle införas. Genomförandet av lagstiftningen skulle få stöd av ett särskilt kunskapscentrum hos kommissionen.

– Alternativ 4: Det befintliga direktivet om europeisk kritisk infrastruktur ersätts med ett nytt instrument för att stärka kritiska entiteters motståndskraft inom de sektorer som betraktas som samhällsviktiga i det föreslagna andra direktivet om säkerhet i nätverks- och informationssystem, ge kommissionen en utökad roll när det gäller att identifiera kritiska entiteter och skapa en särskild EU-byrå med ansvar för kritisk infrastrukturs motståndskraft (som skulle ta på sig de arbetsuppgifter och ansvarsområden som det föreslagna kunskapscentrumet skulle ha enligt det föregående alternativet).

Med hänsyn till de olika ekonomiska, sociala och miljömässiga konsekvenserna som förknippades med vart och ett av alternativen, men också till deras värde i fråga om effektivitet, ändamålsenlighet och proportionalitet, kom man i konsekvensbedömningen fram att det alternativ som föredrogs var alternativ 3. Alternativ 1 och 2 skulle inte skapa de förändringar som behövdes för att lösa problemet, medan alternativ 3 skulle leda till en harmoniserad och mer heltäckande ram för motståndskraft som också skulle stämma överens med och ta hänsyn till befintlig unionslagstiftning inom närbesläktade områden. Alternativ 3 skulle också vara proportionerligt och föreföll vara politiskt genomförbart eftersom det stämmer överens med rådets och parlamentets uttalanden om behovet av unionsåtgärder inom detta område. Dessutom skulle detta alternativ sannolikt säkerställa flexibilitet och erbjuda en framtidssäkrad ram som skulle göra det möjligt för kritiska entiteter att bemöta olika risker över tid. Slutligen konstaterades det i konsekvensbedömningen att detta alternativ skulle komplettera befintliga sektorsbaserade och sektorsöverskridande ramar och instrument. Enligt

detta alternativ får t.ex. utsedda entiteter möjlighet att uppfylla vissa skyldigheter som fastställs i detta nya instrument genom skyldigheter i befintliga instrument och skulle i sådant fall inte vara skyldiga att vidta ytterligare åtgärder. Å andra sidan skulle de förväntas vidta åtgärder om de befintliga instrumenten inte omfattar saken i fråga eller är begränsade till enbart vissa typer av risker eller åtgärder.

Konsekvensbedömningen granskades av nämnden för lagstiftningskontroll som utfärdade ett positivt yttrande med förbehåll den 20 november 2020. Nämnden pekade på ett antal inslag i konsekvensbedömningen som borde åtgärdas. Framför allt begärde nämnden ytterligare förtydliganden när det gäller riskerna i samband med kritisk infrastruktur och den gränsöverskridande aspekten, kopplingen mellan initiativet och den pågående översynen av direktivet om säkerhet i nätverks- och informationssystem samt förhållandet mellan det rekommenderade alternativet och andra delar av sektorslagstiftningen. Nämnden ansåg också att en utökning av instrumentets sektorsbaserade räckvidd behövde motiveras ytterligare och begärde kompletterande upplysningar om kriterierna för att välja kritiska entiteter. När det slutligen gäller proportionalitet ville nämnden ha ett förtydligande av hur det rekommenderade alternativet skulle leda till bättre nationella åtgärder mot gränsöverskridande risker. Dessa och andra mer detaljerade synpunkter från nämnden har bemötts i den slutliga versionen av konsekvensbedömningen, som t.ex. innehåller en mer detaljerad beskrivning av de gränsöverskridande riskerna för kritisk infrastruktur och av förhållandet mellan detta förslag och förslaget till det andra direktivet om säkerhet i nätverks- och informationssystem. Hänsyn har också tagits till nämndens synpunkter i det följande förslaget till direktiv.

- **Lagstiftningens ändamålsenlighet och förenkling**

I enlighet med kommissionens program om lagstiftningens ändamålsenlighet och resultat (Refit-programmet) bör alla initiativ som syftar till att ändra befintlig EU-lagstiftning inriktas på att förenkla och mer effektivt genomföra fastställda politiska mål. Slutsatserna i konsekvensbedömningen tyder på att förslaget torde minska den totala bördan för medlemsstaterna. En närmare anpassning till den tjänsteinriktade strategin i det nuvarande direktivet om säkerhet i nätverks- och informationssystem kommer sannolikt att leda till minskade efterlevnadskostnader med tiden. Det betungande gränsöverskridande identifierings- och utseendeförfarande som fastställs i det nuvarande direktivet om säkerhet i nätverks- och informationssystem skulle t.ex. ersättas med ett riskbaserat förfarande på nationell nivå som enbart syftar till att identifiera kritiska entiteter som omfattas av olika skyldigheter. På grundval av riskbedömningen skulle medlemsstaterna identifiera kritiska entiteter, varav de flesta redan har utsetts som leverantörer av samhällsviktiga tjänster enligt det nuvarande direktivet om säkerhet i nätverks- och informationssystem.

Genom att vidta åtgärder för att stärka sin motståndskraft kommer de kritiska entiteterna dessutom att minska sannolikheten för att uppleva driftsstörningar. Det betyder att sannolikheten för störningsincidenter som påverkar tillhandahållandet av samhällsviktiga tjänster negativt i enskilda medlemsstater och i hela EU skulle minska. Detta skulle tillsammans med de positiva effekterna av en harmonisering på unionsnivå av olika nationella regler få positiva effekter för företagen, däribland mikroföretag och små och medelstora företag, den övergripande hälsan i unionens ekonomi och den tillförlitliga funktionen hos den inre marknaden.

- **Grundläggande rättigheter**

Den föreslagna lagstiftningen är avsedd att stärka kritiska entiteters motståndskraft, vilka tillhandahåller olika former av samhällsviktiga tjänster, och samtidigt undanröja

regleringshinder för deras förmåga att tillhandahålla tjänster i hela EU. På så sätt skulle den övergripande risken för driftsstörningar minska på såväl samhällsnivå som på individuell nivå och bördorna skulle minska. Detta skulle bidra till att säkerställa en högre nivå av allmän säkerhet och samtidigt ge positiva effekter för företagens frihet att bedriva verksamhet och för många andra ekonomiska aktörer som är beroende av tillhandahållandet av samhällsviktiga tjänster, vilket i förlängningen gynnar konsumenterna. De bestämmelser i förslaget som syftar till att säkerställa en effektiv säkerhetshantering av anställda kommer normalt sett att innefatta behandling av personuppgifter. Detta är motiverat av behovet av att göra säkerhetsprövningar av särskilda personalkategorier. All sådan behandling av personuppgifter kommer alltid att omfattas av kraven på efterlevnad av unionens regler om skydd av personuppgifter, däribland den allmänna dataskyddsförordningen.[13]

4. BUDGETKONSEKVENSER

Förslaget till direktiv påverkar unionens budget. De totala finansiella resurser som krävs för att genomföra det föreliggande förslaget beräknas uppgå till 42,9 miljoner euro för perioden 2021–2027, varav 5,1 miljoner euro för administrativa utgifter. Dessa kostnader kan delas in på följande sätt:

– Kommissionens stödverksamhet—inklusive personal, projekt, studier och stödverksamhet.

– Rådgivande uppdrag som anordnas av kommissionen.

– Regelbundna möten i gruppen för kritiska entiteters motståndskraft, kommittén inom kommittéförfarandet och andra möten.

Mer detaljerad information finns i den finansieringsöversikt som åtföljer detta förslag.

5. ÖVRIGA INSLAG

- **Genomförandeplaner samt åtgärder för övervakning, utvärdering och rapportering**

Genomförandet av det föreslagna direktivet kommer att granskas fyra och ett halvt år efter ikraftträdandet, varefter kommissionen kommer att lämna en rapport till Europaparlamentet och rådet. I rapporten ska det bedömas i vilken utsträckning medlemsstaterna har vidtagit nödvändiga åtgärder för att följa direktivet. Kommissionen ska lämna en rapport med en bedömning av direktivets konsekvenser och mervärde till Europaparlamentet och rådet senast sex år efter direktivets ikraftträdande.

- **Ingående redogörelse för de specifika bestämmelserna i förslaget**

Syfte, tillämpningsområde och definitioner (artiklarna 1–2)

I artikel 1 anges direktivets syfte och tillämpningsområde och det fastställs skyldigheter för medlemsstaterna att vidta vissa åtgärder för att säkerställa tillhandahållandet på den inre marknaden av tjänster som är nödvändiga för att upprätthålla centrala samhällsfunktioner eller central ekonomisk verksamhet, särskilt för att identifiera kritiska entiteter och ge dem möjlighet att uppfylla särskilda skyldigheter som syftar till att stärka deras motståndskraft och

[13] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG.

förbättra deras förmåga att tillhandahålla sådana tjänster på den inre marknaden. I direktivet fastställs också regler om tillsyn av och kontroll av efterlevnad hos kritiska entiteter och särskild tillsyn av kritiska entiteter som anses vara av särskild europeisk betydelse. I artikel 1 förklaras även förhållandet mellan direktivet och andra gällande rättsakter i unionsrätten samt på vilka villkor information som är konfidentiell i enlighet med unionsregler och nationella regler ska utväxlas med kommissionen och andra relevanta myndigheter. I artikel 2 finns en förteckning över gällande definitioner.

Nationella ramar för kritiska entiteters motståndskraft (artiklarna 3–9)

I artikel 3 fastställs att medlemsstaterna ska anta en strategi för att stärka kritiska entiteters motståndskraft. I artikeln beskrivs de delar som strategin ska innehålla, det fastställs att den bör uppdateras regelbundet och vid behov samt att medlemsstaterna ska underrätta kommissionen om sina strategier och om eventuella uppdateringar av dem. I artikel 4 fastställs att de behöriga myndigheterna ska upprätta en förteckning över samhällsviktiga tjänster och regelbundet göra en bedömning av alla relevanta risker som kan påverka tillhandahållandet av dessa samhällsviktiga tjänster i syfte att identifiera kritiska entiteter. Bedömningen ska ta hänsyn till de riskbedömningar som genomförs i enlighet med andra gällande rättsakter i unionsrätten, de risker som uppstår till följd av ömsesidigt beroende mellan särskilda sektorer och tillgänglig information om incidenter. Medlemsstaterna ska se till att de relevanta delarna i riskbedömningen görs tillgängliga för kritiska entiteter och att uppgifter om de typer av risker som har identifierats och resultatet av deras riskbedömningar regelbundet görs tillgängliga för kommissionen.

I artikel 5 fastställs att medlemsstaterna ska identifiera kritiska entiteter i specifika sektorer och undersektorer. Identifieringsprocessen bör ta hänsyn till resultatet av riskbedömningen och utföras med särskilda kriterier. Medlemsstaterna ska upprätta en förteckning över kritiska entiteter som ska uppdateras regelbundet och vid behov. De kritiska entiteterna ska underrättas om att de har identifierats och om vilka skyldigheter detta innebär. De behöriga myndigheter som ansvarar för genomförandet av direktivet ska underrätta de behöriga myndigheter som ansvarar för genomförandet av det andra direktivet om säkerhet i nätverks- och informationssystem om identifieringen av kritiska entiteter. Om en entitet har identifierats som kritisk av två eller fler medlemsstater ska medlemsstaterna samråda med varandra i syfte att minska bördan för den kritiska entiteten. Om kritiska entiteter tillhandahåller tjänster till eller i mer än en tredjedel av medlemsstaterna ska den berörda medlemsstaten underrätta kommissionen om identiteten på dessa kritiska entiteter.

I artikel 6 definieras begreppet *betydande störande effekt*, som det hänvisas till i artikel 5.2, och det krävs att medlemsstaterna ska ge kommissionen vissa typer av uppgifter om de kritiska entiteter som de har identifierat och om hur de identifierats. Genom artikel 6 får kommissionen också, efter samråd med gruppen för kritiska entiteters motståndskraft, befogenhet att anta relevanta riktlinjer.

I artikel 7 fastställs att medlemsstaterna bör identifiera entiteter inom sektorerna för infrastruktur för bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur som ska behandlas som likvärdiga med kritiska entiteter enbart vid tillämpningen av kapitel II. Dessa entiteter bör underrättas om att de har identifierats.

Enligt artikel 8 ska varje medlemsstat utse och säkerställa att lämpliga resurser ges till en eller flera behöriga myndigheter som är ansvariga för att direktivet tillämpas korrekt på nationell nivå och även utse en gemensam kontaktpunkt som har i uppdrag att säkerställa det

gränsöverskridande samarbetet. Den gemensamma kontaktpunkten ska regelbundet lämna en sammanfattande rapport om incidentrapporteringar till kommissionen. Enligt artikel 8 ska de behöriga myndigheter som ansvarar för direktivets tillämpning samarbeta med andra relevanta nationella myndigheter, däribland behöriga myndigheter som har utsetts enligt det andra direktivet om säkerhet i nätverks- och informationssystem. I artikel 9 fastställs att medlemsstaterna ska tillhandahålla stöd för kritiska entiteter i syfte att säkerställa deras motståndskraft och ska underlätta samarbete och frivilligt utbyte av information och god praxis mellan behöriga myndigheter och kritiska entiteter.

Kritiska entiteters motståndskraft (artiklarna 10–13)

Enligt artikel 10 ska de kritiska entiteterna regelbundet bedöma alla relevanta risker på grundval av nationella riskbedömningar och andra relevanta informationskällor. I artikel 11 föreskrivs att de kritiska entiteterna ska vidta lämpliga och proportionella tekniska och organisatoriska åtgärder för att säkerställa sin motståndskraft och att de ska säkerställa att dessa åtgärder beskrivs i en plan för motståndskraft eller i ett likvärdigt eller i likvärdiga dokument. Medlemsstaterna får begära att kommissionen ska anordna rådgivande uppdrag för att ge råd till kritiska entiteter om hur de kan uppfylla sina skyldigheter. Genom artikel 11 får kommissionen också befogenhet att anta delegerade akter och genomförandeakter när så är nödvändigt.

Enligt artikel 12 ska medlemsstaterna säkerställa att kritiska entiteter får ansöka om säkerhetskontroller av personer som ingår i eller kan komma att ingå i särskilda personalkategorier och att dessa ansökningar behandlas snabbt av de myndigheter som är ansvariga för att utföra sådana säkerhetsprövningar. I artikeln beskrivs säkerhetsprövningarnas syfte, räckvidd och innehåll och samtliga kontroller måste vara förenliga med den allmänna dataskyddsförordningen.

I artikel 13 fastställs att medlemsstaterna ska se till att kritiska entiteter rapporterar till den behöriga myndigheten om incidenter som medför en betydande störning eller kan medföra en betydande störning av deras verksamhet. De behöriga myndigheterna ska i sin tur lämna relevant uppföljningsinformation till den rapporterande kritiska entiteten. Via den gemensamma kontaktpunkten ska de behöriga myndigheterna också informera de gemensamma kontaktpunkterna i andra berörda medlemsstater, om incidenten har eller skulle kunna ha gränsöverskridande effekter i en eller flera medlemsstater.

Särskild tillsyn över kritiska entiteter med särskild europeisk betydelse (artiklarna 14–15)

I artikel 14 definieras kritiska entiteter av särskild europeisk betydelse som entiteter som har identifierats som kritiska entiteter och som tillhandahåller samhällsviktiga tjänster i mer än en tredjedel av medlemsstaterna. När kommissionen har tagit emot underrättelsen i enlighet med artikel 5.6 ska den informera den berörda entiteten om att den betraktas som en kritisk entitet av särskild europeisk betydelse, vilka skyldigheter det innebär och från vilket datum dessa skyldigheter ska börja tillämpas. I artikel 15 beskrivs de arrangemang för särskild tillsyn som är tillämpliga på kritiska entiteter av särskild europeisk betydelse. Bland dessa ingår att värdmedlemsstater på begäran ska ge kommissionen och gruppen för motståndskraft hos kritiska entiteter information om riskbedömningen i enlighet med artikel 10 och om de åtgärder som har vidtagits i enlighet med artikel 11 samt eventuella tillsyns- eller verkställighetsåtgärder. I artikel 15 fastställs också attkommissionen får anordna rådgivande uppdrag för att bedöma de åtgärder som specifika kritiska entiteter av särskild europeisk betydelse har vidtagit. På grundval av en analys av slutsatserna från det rådgivande uppdraget

som utförs av gruppen för kritiska entiteters motståndskraft ska kommissionen lämna sina synpunkter till den medlemsstat där entitetens infrastruktur är belägen om huruvida entiteten uppfyller sina skyldigheter och i förekommande fall vilka åtgärder som skulle kunna vidtas för att förbättra entitetens motståndskraft. Artikeln innehåller en beskrivning av de rådgivande uppdragens sammansättning, organisation och finansiering. Där föreskrivs också att kommissionen ska anta en genomförandeakt om regler om de procedurmässiga arrangemangen för genomförande av och rapporter från rådgivande uppdrag.

Samarbete och rapportering (artiklarna 16–17)

I artikel 16 beskrivs de roller och arbetsuppgifter som anförtros gruppen för kritiska entiteters motståndskraft, som ska bestå av företrädare för medlemsstaterna och kommissionen. Gruppen ska ge kommissionen stöd och underlätta strategiskt samarbete och informationsutbyte. I artikeln anges att kommissionen får anta genomförandeakter i vilka fastställs de procedurmässiga arrangemang som krävs för verksamheten i gruppen för kritiska entiteters motståndskraft. I artikel 17 fastställs att kommissionen när så är lämpligt ska ge stöd till medlemsstater och kritiska entiteter för att uppfylla sina skyldigheter enligt direktivet och komplettera medlemsstaternas verksamhet i enlighet med artikel 9.

Tillsyn och kontroll av efterlevnad (artiklarna 18–19)

I artikel 18 fastställs att medlemsstaterna har vissa befogenheter, medel och ansvar för att säkerställa att direktivet genomförs och efterlevs. Medlemsstaterna ska se till att när en behörig myndighet bedömer efterlevnaden hos en kritisk entitet ska den informera de behöriga myndigheterna i den berörda medlemsstaten som har utsetts enligt det andra direktivet om säkerhet i nätverks- och informationssystem och får begära att dessa myndigheter ska bedöma entitetens cybersäkerhet och bör samarbeta och utbyta information i detta syfte. I artikel 19 fastställs att medlemsstaterna i enlighet med långvarig praxis ska fastställa regler för de sanktioner som ska tillämpas på överträdelser och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas.

Slutbestämmelser (artiklarna 20–26)

I artikel 20 fastställs att kommissionen ska bistås av en kommitté i den mening som avses i förordning (EU) nr 182/2011. Detta är en standardartikel. Genom artikel 21 ges kommissionen befogenhet att anta delegerade akter, med förbehåll för de villkor som anges i den artikeln. Även detta är en standardartikel. I artikel 22 anges att kommissionen ska överlämna en rapport till Europaparlamentet och rådet med en bedömning av i vilken utsträckning medlemsstaterna har vidtagit de åtgärder som är nödvändiga för att följa direktivet. En rapport med en bedömning av direktivets konsekvenser och mervärde och av huruvida direktivets räckvidd bör utökas till andra sektorer eller undersektorer, inbegripet sektorn för produktion, bearbetning och distribution av livsmedel, ska regelbundet lämnas till Europaparlamentet och rådet.

I artikel 23 fastställs att direktiv 2008/114/EG ska upphävas från och med den dag som direktivet börjar tillämpas. I artikel 24 fastställs att medlemsstaterna inom den fastställda tidsperioden ska anta och offentliggöra de lagar, förordningar och administrativa bestämmelser som är nödvändiga för att följa direktivet och informera kommissionen om detta. Texten till de centrala bestämmelser i nationell rätt som de antar inom det område som omfattas av detta direktiv ska överlämnas till kommissionen. Enligt artikel 25 ska direktivet

träda i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*. I artikel 26 anges att direktivet riktar sig till medlemsstaterna.

2020/0365 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

om kritiska entiteters motståndskraft

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[14],

med beaktande av Regionkommitténs yttrande[15],

i enlighet med det ordinarie lagstiftningsförfarandet[16], och

av följande skäl:

(1) I rådets direktiv 2008/114/EG[17] föreskrivs ett förfarande för att identifiera och klassificera europeisk kritisk infrastruktur vars driftstörning eller förstörelse skulle få betydande gränsöverskridande konsekvenser i minst två medlemsstater. Detta direktiv var uteslutande inriktat på skyddet av sådan infrastruktur. Vid den utvärdering av direktiv 2008/114/EG som gjordes 2019[18] konstaterades dock att skyddsåtgärder som enbart gäller enskilda tillgångar inte är tillräckliga för att förhindra alla störningar från att uppstå, på grund av den alltmer sammankopplade och gränsöverskridande karaktären hos den verksamhet som bedrivs med kritisk infrastruktur. Därför är det nödvändigt att ändra strategin i riktning mot att säkerställa kritiska entiteters motståndskraft, dvs. deras förmåga att lindra, absorbera, anpassa sig till och återhämta sig från incidenter som skulle kunna störa den kritiska entitetens drift.

(2) Trots de befintliga åtgärderna på unionsnivå[19] och nationell nivå för att stödja skyddet av kritisk infrastruktur i unionen är de entiteter som driver sådan infrastruktur inte tillräckligt väl rustade för att hantera nuvarande och förväntade framtida risker för deras verksamhet som skulle kunna leda till störningar i tillhandahållandet av tjänster som är nödvändiga för att utföra centrala samhällsfunktioner eller central ekonomisk verksamhet. Detta beror på en dynamisk hotbild med ett framväxande terroristhot och ett ökande ömsesidigt beroende mellan infrastruktur och sektorer och även en ökad fysisk risk på grund av naturkatastrofer och klimatförändringen, som leder till att

---

14 EUT C , , s. .

15 EUT C […], […], s. […].

16 Europaparlamentets ståndpunkt […] och rådets ståndpunkt […].

17 Rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (EUT L 345, 23.12.2008, s. 75).

18 SWD(2019) 308.

19 Det europeiska programmet för skydd av kritisk infrastruktur (EPCIP).

extrema väderhändelser blir allt vanligare och mer omfattande och medför långsiktiga förändringar i genomsnittsklimatet som kan minska kapaciteten och effektiviteten hos vissa typer av infrastruktur om det inte vidtas åtgärder för att stärka motståndskraften eller anpassa sig till klimatet. Relevanta sektorer och typer av entiteter erkänns dessutom inte på ett enhetligt sätt som kritiska i alla medlemsstater.

(3) Det ökande ömsesidiga beroendet är ett resultat av ett alltmer gränsöverskridande och ömsesidigt beroende nätverk av tjänsteleveranser som använder viktig infrastruktur i hela unionen inom sektorerna för energi, transporter, infrastruktur för bankverksamhet och finansmarknadsinfrastruktur, digital infrastruktur, dricksvatten och avloppsvatten, hälso- och sjukvård, vissa aspekter av offentlig förvaltning samt rymdsektorn i den mån tillhandahållandet av vissa tjänster som är beroende av markbaserad infrastruktur som ägs, förvaltas och drivs av medlemsstater eller privata entiteter berörs och som därför inte omfattar infrastruktur som ägs, förvaltas eller drivs av unionen eller för unionens räkning inom ramen för dess rymdprogram. Detta ömsesidiga beroende innebär att alla störningar, även sådana som till en början är begränsade till en entitet eller en sektor, kan få bredare kaskadeffekter som skulle kunna leda till långtgående och långvariga negativa konsekvenser för tillhandahållandet av tjänster på hela den inre marknaden. Covid-19-pandemin har visat hur sårbara våra alltmer av varandra beroende samhällen är för risker med låg sannolikhet.

(4) De entiteter som deltar i tillhandahållandet av samhällsviktiga tjänster omfattas i allt högre grad av olika krav som införs enligt medlemsstaternas lagstiftning. Vissa medlemsstater ställer mindre hårda säkerhetskrav på dessa entiteter, vilket inte bara riskerar att ge negativa effekter för upprätthållandet av centrala samhällsfunktioner eller central ekonomisk verksamhet i EU utan skapar också hinder för den inre marknadens funktion. Likartade typer av entiteter betraktas som kritiska i vissa medlemsstater men inte i andra, och de som identifieras som kritiska omfattas av olika krav i olika medlemsstater. Detta leder till ytterligare och onödiga administrativa bördor för företag som bedriver gränsöverskridande verksamhet, särskilt för företag med verksamhet i medlemsstater som ställer hårdare krav.

(5) Därför är det nödvändigt att införa harmoniserade minimiregler för att säkerställa tillhandahållandet av samhällsviktiga tjänster på den inre marknaden och öka kritiska entiteters motståndskraft.

(6) För att uppnå det målet bör medlemsstaterna identifiera kritiska entiteter som bör omfattas av särskilda krav och tillsyn, men också särskilt stöd och vägledning för att uppnå en hög motståndskraft mot alla relevanta risker.

(7) Vissa sektorer inom ekonomin, t.ex. för energi och transporter, är redan reglerade eller kan komma att regleras i framtiden genom sektorsspecifika rättsakter i unionsrätten som innehåller regler som rör vissa aspekter av motståndskraft hos entiteter som är verksamma inom de sektorerna. För att på ett heltäckande sätt hantera motståndskraften hos de entiteter som är kritiska för att den inre marknaden ska fungera korrekt bör sådana sektorsspecifika åtgärder kompletteras med de åtgärder som fastställs i detta direktiv, vilket skapar en övergripande ram för att hantera kritiska entiteters motståndskraft med hänsyn till alla faror, dvs. naturliga faror och faror orsakade av människan, olyckshändelser och avsiktligt framkallade faror.

(8) Med tanke på hur viktig cybersäkerhet är för kritiska entiteters motståndskraft och för att skapa enhetlighet är det nödvändigt att använda en enhetlig strategi mellan detta

direktiv och Europaparlamentets och rådets direktiv (EU) XX/YY[20] [förslag till direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (nedan kallat *det andra direktivet om säkerhet i nätverks- och informationssystem*)] när så är möjligt. Med tanke på den högre frekvensen av och de särskilda egenskaperna hos cyberrisker införs det genom det andra direktivet om säkerhet i nätverks- och informationssystem heltäckande krav på en stor mängd entiteter för att säkerställa deras cybersäkerhet. Eftersom cybersäkerhet hanteras i tillräcklig grad genom det andra direktivet om säkerhet i nätverks- och informationssystem bör de frågor som omfattas av det direktivet uteslutas från tillämpningsområdet för detta direktiv, utan att det påverkar tillämpningen av den särskilda ordningen för entiteter inom sektorn för digital infrastruktur.

(9) Om det enligt bestämmelser i andra rättsakter i unionsrätten krävs att kritiska entiteter ska bedöma relevanta risker, vidta åtgärder för att säkerställa sin motståndskraft eller rapportera incidenter, och dessa krav minst är likvärdiga med motsvarande skyldigheter enligt det här direktivet, bör de relevanta bestämmelserna i det här direktivet inte vara tillämpliga, för att undvika dubbelarbete och onödiga bördor. I sådant fall bör de relevanta bestämmelserna i de andra rättsakterna tillämpas. Om de relevanta bestämmelserna i det här direktivet inte är tillämpliga bör direktivets bestämmelser om tillsyn och kontroll av efterlevnad inte heller vara tillämpliga. Medlemsstaterna bör dock ta med samtliga sektorer som förtecknas i bilagan i sin strategi för att stärka kritiska entiteters motståndskraft, sin riskbedömning och de stödåtgärder som vidtas enligt kapitel II och de bör kunna identifiera kritiska entiteter inom de sektorer där de tillämpliga villkoren har uppfyllts, med hänsyn till den särskilda ordningen för entiteter inom sektorn för bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur.

(10) I syfte att säkerställa en heltäckande strategi för kritiska entiteters motståndskraft bör varje medlemsstat ha en strategi där det fastställs mål och politiska åtgärder som ska vidtas. För att uppnå detta bör medlemsstaterna se till att deras strategier för cybersäkerhet innehåller en politisk ram för utökat samarbete mellan den behöriga myndigheten enligt detta direktiv och det andra direktivet om säkerhet i nätverks- och informationssystem i samband med utbyte av information om incidenter och cyberhot och fullgörandet av tillsynsuppgifter.

(11) Medlemsstaternas åtgärder för att identifiera och bidra till att säkerställa kritiska entiteters motståndskraft bör följa en riskbaserad strategi med inriktning på insatser för de entiteter som är mest relevanta för att centrala samhällsfunktioner och central ekonomisk verksamhet ska kunna upprätthållas. För att säkerställa en sådan riktad strategi bör varje medlemsstat inom en harmoniserad ram göra en bedömning av alla relevanta naturliga risker och risker orsakade av människan som kan komma att påverka tillhandahållandet av samhällsviktiga tjänster, däribland olyckor, naturkatastrofer, hot mot folkhälsan, t.ex. pandemier, och antagonistiska hot, inklusive terroristbrott. När medlemsstaterna gör dessa riskbedömningar bör de ta hänsyn till andra allmänna eller sektorsspecifika riskbedömningar som har gjorts i enlighet med andra rättsakter i unionsrätten och bör ta hänsyn till beroenden mellan sektorer, även från andra medlemsstater och tredjeländer. Resultatet av riskbedömningen bör användas i processen för att identifiera kritiska entiteter och för att bistå entiteterna med att uppfylla kraven på motståndskraft enligt detta direktiv.

[20] [Hänvisning till det andra direktivet för säkerhet i nätverks- och informationssystem, när det har antagits.]

(12) För att säkerställa att alla berörda entiteter omfattas av de kraven och minska skillnaderna i detta avseende är det viktigt att införa harmoniserade regler som möjliggör en enhetlig identifiering av kritiska entiteter i hela EU och samtidigt ge medlemsstaterna möjlighet att avspegla nationella särdrag. Därför bör det fastställas kriterier för identifiering av kritiska entiteter. För att skapa effektivitet, ändamålsenlighet, konsekvens och rättssäkerhet bör det också fastställas lämpliga regler för rapportering och samarbete i samband med, samt de rättsliga konsekvenserna av, en sådan identifiering. För att kommissionen ska kunna bedöma om detta direktiv har tillämpats korrekt bör medlemsstaterna lämna så detaljerad och specifik relevant information som möjligt till kommissionen och under alla omständigheter överlämna förteckningen över samhällsviktiga tjänster, antalet kritiska entiteter som har identifierats för varje sektor och undersektor som avses i bilagan och den samhällsviktiga tjänst eller de samhällsviktiga tjänster som varje entitet tillhandahåller samt eventuella tröskelvärden som har tillämpats.

(13) Det bör också upprättas kriterier för att fastställa hur betydande en störande effekt som uppstår till följd av sådana incidenter är. Dessa kriterier bör utgå från de kriterier som föreskrivs i Europaparlamentets och rådets direktiv (EU) 2016/1148[21] för att ta vara på medlemsstaternas ansträngningar för att identifiera dessa operatörer och de erfarenheter som har gjorts i detta avseende.

(14) Entiteter som tillhör sektorn för digital infrastruktur baseras i princip på nätverks- och informationssystem och omfattas av det andra direktivet om säkerhet i nätverks- och informationssystem, som behandlar den fysiska säkerheten hos sådana system som en del av deras skyldigheter i fråga om hantering och rapportering av cybersäkerhetsrisker. Eftersom dessa frågor omfattas av det andra direktivet om säkerhet i nätverks- och informationssystem är skyldigheterna i det här direktivet inte tillämpliga på sådana entiteter. Med tanke på hur viktiga de tjänster som tillhandahålls av entiteter inom sektorn för digital infrastruktur är för tillhandahållandet av andra samhällsviktiga tjänster bör medlemsstaterna dock, med utgångspunkt i de kriterier och med det förfarande som i tillämpliga delar föreskrivs i det här direktivet, identifiera de entiteter som ingår i sektorn för digital infrastruktur och som bör behandlas som likvärdiga med kritiska entiteter enbart vid tillämpningen av kapitel II, inklusive bestämmelsen om medlemsstaternas stöd för att öka motståndskraften hos sådana entiteter. Därför bör sådana entiteter inte omfattas av de skyldigheter som fastställs i kapitlen III–IVI. Eftersom de skyldigheter om att tillhandahålla viss information till de behöriga myndigheterna som fastställs för kritiska entiteter i kapitel II gäller tillämpningen av kapitlen III och IV bör de entiteterna inte heller omfattas av de skyldigheterna.

(15) I EU-lagstiftningen om finansiella tjänster införs heltäckande krav på att finansiella entiteter ska hantera alla risker de ställs inför, inklusive operativa risker, och säkerställa driftskontinuitet. Detta inbegriper Europaparlamentets och rådets förordning (EU) nr 648/2012[22], Europaparlamentets och rådets förordning () nr

[21] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

[22] Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister (EUT L 201, 27.7.2012, s. 1).

2014/65/EU[23], Europaparlamentets och rådets förordning (EU) nr 600/2014[24], Europaparlamentets och rådets förordning (EU) nr 575/2013[25] och Europaparlamentets och rådets direktiv 2013/36/EU[26]. Kommissionen har nyligen föreslagit att denna ram ska kompletteras med Europaparlamentets och rådets förordning XX/YYYY [förslag till förordning om digital operativ motståndskraft för finanssektorn, (nedan kallad *DORA-förordningen*)[27]], där det fastställs krav på finansföretagens hantering av IKT-risker, däribland skyddet av fysisk IKT-infrastruktur. Eftersom motståndskraften hos de entiteter som förtecknas i punkterna 3 och 4 i bilagan omfattas på ett heltäckande sätt av EU-lagstiftningen om finansiella tjänster bör även dessa entiteter behandlas som likvärdiga med kritiska entiteter enbart vid tillämpningen av kapitel II i det här direktivet. För att säkerställa en enhetlig tillämpning av reglerna för operativ risk och digital motståndskraft i finanssektorn bör medlemsstaternas stöd för att öka den övergripande motståndskraften hos finansiella entiteter som är likvärdiga med kritiska entiteter säkerställas av de myndigheter som har utsetts i enlighet med artikel 41 i [DORA-förordningen] och omfattas av de förfaranden som fastställs i den förordningen på ett fullständigt harmoniserat sätt.

(16) Medlemsstaterna bör utse myndigheter som är behöriga att övervaka tillämpningen av och vid behov verkställa reglerna i detta direktiv och säkerställa att dessa myndigheter har tillräckliga befogenheter och resurser. Med tanke på skillnaderna i nationella styrningsstrukturer och för att skydda redan befintliga sektorsbaserade arrangemang eller EU:s tillsyns- och regleringsorgan samt för att undvika dubbelarbete bör medlemsstaterna kunna utse mer än en behörig myndighet. I sådant fall bör de dock tydligt avgränsa de berörda myndigheternas respektive arbetsuppgifter och säkerställa att de samarbetar smidigt och effektivt. Alla behöriga myndigheter bör också samarbeta mer generellt med andra relevanta myndigheter, på både nationell nivå och unionsnivå.

(17) För att underlätta gränsöverskridande samarbete och kommunikation och för att göra det möjligt att genomföra detta direktiv effektivt bör varje medlemsstat, utan att det påverkar tillämpningen av sektorsspecifika unionsrättsliga krav, utse en gemensam kontaktpunkt inom en av de myndigheter som den har utsett som behörig myndighet enligt detta direktiv, som ska ansvara för samordning av frågor som rör kritiska entiteters motståndskraft och gränsöverskridande samarbete på unionsnivå i detta avseende.

(18) Eftersom entiteter som identifieras som kritiska entiteter enligt det andra direktivet om säkerhet i nätverks- och informationssystem och identifierade entiteter inom sektorn

---

23 Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (EUT L 173, 12.6.2014, s. 349).

24 Europaparlamentets och rådets förordning (EU) nr 600/2014 av den 15 maj 2014 om marknader för finansiella instrument och om ändring av förordning (EU) nr 648/2012 (EUT L 173, 12.6.2014, s. 84).

25 Europaparlamentets och rådets förordning nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och värdepappersföretag och om ändring av förordning (EU) nr 648/2012, (EUT L 176, 27.6.2013, s. 1).

26 Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG (EUT L 176, 27.6.2013, s. 338).

27 Förslag till Europaparlamentets och rådets förordning om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014, COM (2020) 595.

för digital infrastruktur och som ska behandlas som likvärdiga enligt det här direktivet omfattas av de cybersäkerhetskrav som fastställs i det andra direktivet om säkerhet i nätverks- och informationssystem bör de behöriga myndigheter som har utsetts enligt de båda direktiven samarbeta, framför allt i fråga om cybersäkerhetsrisker och incidenter som påverkar de entiteterna.

(19) Medlemsstaterna bör ge kritiska entiteter stöd för att stärka sin motståndskraft i enlighet med sina skyldigheter enligt detta direktiv, utan att detta påverkar entiteternas eget rättsliga ansvar för att säkerställa efterlevnaden. Framför allt skulle medlemsstaterna kunna utveckla vägledningsmaterial och metoder, stödja anordnandet av övningar för att testa deras motståndskraft och tillhandahålla utbildning för kritiska entiteters personal. Med tanke på det ömsesidiga beroendet mellan entiteter och sektorer bör medlemsstaterna dessutom skapa informationsdelningsverktyg till stöd för frivilligt informationsutbyte mellan kritiska entiteter utan att detta påverkar tillämpningen av de konkurrensregler som fastställs i fördraget om Europeiska unionens funktionssätt.

(20) För att kunna säkerställa sin motståndskraft bör kritiska entiteter ha en heltäckande bild av alla relevanta risker som de är utsatta för och analysera de riskerna. Därför bör de göra riskbedömningar, när det är nödvändigt med hänsyn till deras specifika omständigheter och utvecklingen av riskerna, och under alla omständigheter åtminstone vart fjärde år. De kritiska entiteternas riskbedömningar bör baseras på den riskbedömning som medlemsstaterna gör.

(21) De kritiska entiteterna bör vidta de organisatoriska och tekniska åtgärder som är lämpliga och proportionella i förhållande till de risker de ställs inför, i syfte att förebygga, stå emot, minska, absorbera, anpassa sig till och återhämta sig efter en incident. Även om kritiska entiteter bör vidta åtgärder avseende alla punkter som anges i detta direktiv, bör den detaljerade utformningen och omfattningen av åtgärderna avspegla de olika risker som varje entitet har identifierat inom ramen för sin riskbedömning och särdragen hos den entiteten på ett ändamålsenligt och proportionerligt sätt.

(22) För effektivitetens och ansvarsskyldighetens skull bör de kritiska entiteterna beskriva dessa åtgärder tillräckligt detaljerat för att uppnå sina syften, med hänsyn till de identifierade riskerna, i en plan för motståndskraft eller i ett eller flera dokument som motsvarar en plan för motståndskraft och tillämpa den planen i praktiken. Ett sådant eller sådana dokument får i förekommande fall upprättas i enlighet med de krav och normer som har utvecklats inom ramen för internationella överenskommelser om fysiskt skydd som medlemsstaterna är parter i, däribland konventionen om fysiskt skydd av kärnämnen och kärntekniska anläggningar.

(23) I Europaparlamentets och rådets förordning (EG) nr 300/2008[28], Europaparlamentets och rådets förordning (EG) nr 725/2004[29] och Europaparlamentets och rådets direktiv 2005/65/EG[30] fastställs de krav som är tillämpliga på entiteter inom luftfarts- och sjöfartssektorerna för att förebygga incidenter till följd av olagliga handlingar för att

[28] Europaparlamentets och rådets förordning (EG) nr 300/2008 av den 11 mars 2008 mars om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002 (EUT L 97/72, 9.4.2008, s. 72).

[29] Europaparlamentets och rådets förordning (EG) nr 725/2004 av den 31 mars 2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar (EUT L 129, 29.4.2004, s. 6).

[30] Europaparlamentets och rådets direktiv 2005/65/EG av den 26 oktober 2005 om ökat hamnskydd (EUT L 310, 25.11.2005, s. 28).

stå emot och lindra konsekvenserna av sådana incidenter. De åtgärder som krävs enligt det här direktivet är bredare i fråga om vilka risker som behandlas och de åtgärder som ska vidtas, men kritiska entiteter inom dessa sektorer bör i sin plan för motståndskraft eller motsvarande dokument återge de åtgärder som har vidtagits i enlighet med dessa andra unionsrättsakter. När de kritiska entiteterna genomför åtgärder för motståndskraft i enlighet med detta direktiv får de också överväga att hänvisa till icke-bindande riktlinjer och dokument över god praxis som har utarbetats inom ramen för sektorsbaserade arbetsflöden, t.ex. EU:s plattform för tågresenärers säkerhet[31].

(24) Risken för att anställda vid kritiska entiteter t.ex. missbrukar sina åtkomsträttigheter inom entitetens organisation för skadliga ändamål är ett växande problem. Denna risk förvärras av det framväxande fenomenet radikalisering som leder till våldsbejakande extremism och terrorism. Därför är det nödvändigt att ge kritiska entiteter möjlighet att begära säkerhetsprövningar av personer som ingår i specifika personalkategorier och att säkerställa att sådana ansökningar behandlas snabbt av de berörda myndigheterna i enlighet med gällande unionsrätt och nationell rätt, inbegripet om skydd av personuppgifter.

(25) De kritiska entiteterna bör så snart som det rimligen är möjligt under rådande omständigheter underrätta medlemsstaternas behöriga myndigheter om incidenter som medför en betydande störning eller kan medföra en betydande störning av deras verksamhet. Underrättelsen bör göra det möjligt för de behöriga myndigheterna att reagera snabbt och ändamålsenligt på incidenterna och få en heltäckande bild av de övergripande risker som kritiska entiteter är utsatta för. Därför bör det inrättas ett förfarande för underrättelse av vissa incidenter och det bör fastställas parametrar för att avgöra när en faktisk eller potentiell störning är betydande och incidenterna därför bör rapporteras. Med tanke på de möjliga gränsöverskridande konsekvenserna av sådana störningar bör det inrättas ett förfarande för att medlemsstaterna ska kunna informera andra drabbade medlemsstater via gemensamma kontaktpunkter.

(26) Kritiska entiteter bedriver i allmänhet sin verksamhet inom ramen för ett allt mer sammankopplat nätverk av tjänster och infrastrukturer och tillhandahåller ofta samhällsviktiga tjänster i mer än en medlemsstat, men vissa av dessa entiteter har särskild betydelse för unionen eftersom de tillhandahåller samhällsviktiga tjänster för ett stort antal medlemsstater och måste därför omfattas av särskild tillsyn på unionsnivå. Därför bör det fastställas regler om särskild tillsyn över sådana kritiska entiteter av särskild europeisk betydelse. Dessa regler påverkar inte de regler om tillsyn och kontroll av efterlevnad som fastställs i det här direktivet.

(27) Om en medlemsstat anser att det krävs ytterligare upplysningar för att den ska kunna hjälpa en kritisk entitet att uppfylla sina skyldigheter enligt kapitel III eller för att bedöma huruvida en kritisk entitet av särskild europeisk betydelse uppfyller dessa skyldigheter, bör kommissionen i samförstånd med den medlemsstat där entitetens infrastruktur är belägen anordna ett rådgivande uppdrag för att bedöma de åtgärder som entiteten har vidtagit. För att se till att sådana rådgivande uppdrag utförs korrekt bör kompletterande regler fastställas, framför allt om hur uppdragen ska anordnas och genomföras, hur de ska följas upp och vilka skyldigheter de berörda kritiska entiteterna av särskild europeisk betydelse har. Utan att det påverkar skyldigheten för den medlemsstat där uppdraget genomförs och för den berörda entiteten att följa

[31] Kommissionens beslut av den 29 juni 2018 om inrättandet av EU:s plattform för tågresenärers säkerhet C/2018/4014.

reglerna i detta direktiv, bör de rådgivande uppdragen genomföras i enlighet med de närmare föreskrifterna i den medlemsstatens lagstiftning, t.ex. om de exakta villkor som ska vara uppfyllda för att få åtkomst till relevanta lokaler eller handlingar och om rättslig prövning. Särskild expertis som behövs för sådana uppdrag skulle i förekommande fall kunna begäras via centrumet för samordning av katastrofberedskap.

(28) För att ge kommissionen stöd och underlätta strategiskt samarbete och utbyte av information, inbegripet bästa praxis, i frågor som rör detta direktiv bör det inrättas en grupp för kritiska entiteters motståndskraft, som kommissionens expertgrupp. Medlemsstaterna bör sträva efter att säkerställa att de utsedda företrädarna från deras behöriga myndigheter samarbetar effektivt och ändamålsenligt i gruppen för kritiska entiteters motståndskraft. Gruppen bör inleda sitt arbete sex månader efter ikraftträdandet av detta direktiv för att erbjuda ytterligare möjligheter till lämpligt samarbete under införlivandeperioden för detta direktiv.

(29) För att uppnå målen för detta direktiv och utan att det påverkar medlemsstaternas och de kritiska entiteternas rättsliga ansvar att säkerställa efterlevnad av sina respektive skyldigheter i enlighet med direktivet bör kommissionen, när den anser att det är lämpligt, utföra viss stödverksamhet för att underlätta efterlevnaden av de skyldigheterna. När kommissionen ger stöd till medlemsstater och kritiska entiteter i genomförandet av skyldigheter enligt detta direktiv bör den utgå från befintliga strukturer och verktyg, t.ex. inom ramen för unionens civilskyddsmekanism och det europeiska referensnätverket för skydd av kritisk infrastruktur.

(30) Medlemsstaterna bör säkerställa att deras behöriga myndigheter har vissa särskilda befogenheter för att tillämpa och verkställa detta direktiv korrekt i förhållande till de kritiska entiteterna, när dessa entiteter omfattas av deras jurisdiktion i enlighet med vad som fastställs i detta direktiv. Dessa befogenheter bör särskilt omfatta befogenheten att utföra inspektioner, tillsyn och revisioner, kräva att kritiska entiteter ska lämna information och bevis som rör de åtgärder de har vidtagit för att uppfylla sina skyldigheter och, vid behov, utfärda förelägganden om att avhjälpa konstaterade överträdelser. När medlemsstaterna utfärdar sådana förelägganden bör de inte kräva åtgärder som går utöver vad som är nödvändigt och proportionerligt för att säkerställa att den berörda kritiska entitetens uppfyller skyldigheterna, framför allt med hänsyn till överträdelsens allvarlighetsgrad och den kritiska entitetens ekonomiska kapacitet. Mer generellt bör dessa befogenheter åtföljas av lämpliga och effektiva skyddsåtgärder som ska fastställas i nationell rätt i enlighet med de krav som följer av Europeiska unionens stadga om de grundläggande rättigheterna. När de behöriga myndigheter som har utsetts enligt detta direktiv bedömer om en kritisk entitet uppfyller sina skyldigheter enligt detta direktiv bör de kunna begära att de behöriga myndigheter som har utsetts enligt det andra direktivet om säkerhet i nätverks- och informationssystem ska bedöma cybersäkerheten hos dessa entiteter. De behöriga myndigheterna bör samarbeta och utbyta information för detta ändamål.

(31) För att ta hänsyn till nya risker, teknisk utveckling eller tekniska särdrag hos en eller flera sektorer bör kommissionen delegeras befogenhet att anta akter i enlighet med artikel 290 i fördraget om Europeiska unionens funktionssätt för att komplettera de åtgärder för motståndskraft som kritiska entiteter ska vidta genom att närmare fastställa några eller samtliga sådana åtgärder. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, däribland på expertnivå,

och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet om bättre lagstiftning av den 13 april 2016[32]. För att särskilt säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

(32) För att säkerställa enhetliga villkor för genomförandet av detta direktiv bör kommissionen tilldelas genomförandebefogenheter. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011[33].

(33) Eftersom målen för detta direktiv, nämligen att säkerställa tillhandahållandet på den inre marknaden av tjänster som är nödvändiga för att upprätthålla centrala samhällsfunktioner eller central ekonomisk verksamhet och för att öka kritiska entiteters motståndskraft vilka tillhandahåller sådana tjänster, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens effekter, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i artikel 5 går detta direktiv inte utöver vad som är nödvändigt för att uppnå dessa mål.

(34) Direktiv 2008/114/EG bör därför upphävas.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I
SYFTE, TILLÄMPNINGSOMRÅDE OCH DEFINITIONER

Artikel 1
Syfte och tillämpningsområde

1. I detta direktiv

(a) fastställs skyldigheter för medlemsstaterna att vidta vissa åtgärder i syfte att säkerställa tillhandahållandet på den inre marknaden av tjänster som är nödvändiga för att upprätthålla centrala samhällsfunktioner eller central ekonomisk verksamhet, särskilt för att identifiera kritiska entiteter och entiteter som ska behandlas som likvärdiga i vissa avseenden samt göra det möjligt för dem att uppfylla sina skyldigheter,

(b) inrättas skyldigheter för kritiska entiteter i syfte att öka deras motståndskraft och förbättra deras förmåga att tillhandahålla sådana tjänster på den inre marknaden,

(c) fastställs regler om tillsyn och verkställighet för kritiska entiteter och särskild tillsyn av kritiska entiteter som anses vara av särskild europeisk betydelse.

---

32 EUT L 123, 12.5.2016, s. 1.

33 Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

2. Detta direktiv ska inte vara tillämpligt på frågor som omfattas av direktiv (EU) XX/YY [förslag till direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (nedan kallat *det andra direktivet om säkerhet i nätverks- och informationssystem*)], utan att detta påverkar tillämpningen av artikel 7.

3. Om det enligt bestämmelser i sektorsspecifika rättsakter i unionslagstiftningen krävs att kritiska entiteter ska vidta åtgärder i enlighet med vad som anges i kapitel III och om de kraven är åtminstone likvärdiga med de skyldigheter som fastställs i det här direktivet, ska de berörda bestämmelserna i det här direktivet inte vara tillämpliga, inbegripet de bestämmelser om tillsyn och kontroll av efterlevnad som fastställs i kapitel VI.

4. Utan att det påverkar tillämpningen av artikel 346 i EUF-fördraget får information som är konfidentiell enligt unionsbestämmelser och nationella bestämmelser, såsom bestämmelser om affärshemligheter, utbytas med kommissionen och andra relevanta myndigheter endast när sådant utbyte är nödvändigt för att tillämpa detta direktiv. Den information som utbyts ska begränsas till vad som är relevant och proportionellt för ändamålet med utbytet. Vid sådant utbyte ska informationens konfidentialitet bevaras och säkerhetsintressen och kommersiella intressen hos kritiska entiteter skyddas.

Artikel 2
Definitioner

I detta direktiv gäller följande definitioner:

(1) *kritisk entitet*: en offentlig eller privat entitet av en typ som avses i bilagan och som har identifierats som sådan av en medlemsstat i enlighet med artikel 5.

(2) *motståndskraft*: förmågan att förebygga, stå emot, lindra, absorbera, anpassa sig till och återhämta sig från en incident som stör eller skulle kunna störa verksamheten hos en kritisk entitet.

(3) *incident*: varje händelse som skulle kunna störa eller som stör verksamheten hos den kritiska entiteten.

(4) *infrastruktur*: en tillgång, ett system eller en del därav som är nödvändig för att tillhandahålla en samhällsviktig tjänst.

(5) *samhällsviktig tjänst*: en tjänst som är avgörande för att upprätthålla centrala samhällsfunktioner eller central ekonomisk verksamhet.

(6) *risk*: en omständighet eller händelse som skulle kunna få negativa effekter för kritiska entiteters motståndskraft.

(7) *riskbedömning*: en metod för att fastställa arten och omfattningen av en risk genom analys av potentiella hot och faror och utvärdering av befintliga sårbara förhållanden som skulle kunna störa verksamheten hos den kritiska entiteten.

KAPITEL II
NATIONELLA RAMAR FÖR KRITISKA ENTITETERS MOTSTÅNDSKRAFT

Artikel 3
Strategi för kritiska entiteters motståndskraft

1. Varje medlemsstat ska senast [tre år efter ikraftträdandet av detta direktiv] anta en strategi för att öka kritiska entiteters motståndskraft. Strategin ska innehålla strategiska mål och politiska åtgärder för att uppnå och upprätthålla en hög motståndskraft hos de kritiska entiteterna och den ska åtminstone omfatta de sektorer som avses i bilagan.

2. Strategin ska innehålla åtminstone följande delar:

   (a) Strategiska mål och prioriteringar för att öka kritiska entiteters övergripande motståndskraft, med hänsyn till gränsöverskridande och sektorsöverskridande ömsesidiga beroendeförhållanden.

   (b) En styrningsram för att uppnå de strategiska målen och prioriteringarna, inklusive en beskrivning av rollerna och ansvarsområdena för de olika myndigheter, kritiska entiteter och andra parter som deltar i genomförandet av strategin.

   (c) En beskrivning av de åtgärder som är nödvändiga för att stärka kritiska entiteters övergripande motståndskraft, inklusive en nationell riskbedömning, identifiering av kritiska entiteter och entiteter som är likvärdiga med kritiska entiteter, samt de åtgärder som har vidtagits för att stödja kritiska entiteter i enlighet med detta kapitel.

   (d) En politisk ram för förbättrat samarbete mellan de behöriga myndigheter som har utsetts i enlighet med artikel 8 i detta direktiv och i enlighet med [det andra direktivet om säkerhet i nätverks- och informationssystem] för att dela information om incidenter och cyberhot och utföra tillsynsuppgifter.

   Strategin ska uppdateras när det är nödvändigt och minst vart fjärde år.

3. Medlemsstaterna ska meddela kommissionen sina strategier och eventuella uppdateringar av dem inom tre månader efter det att de har antagits.

Artikel 4
Riskbedömning av medlemsstaterna

1. De behöriga myndigheter som har utsetts i enlighet med artikel 8 ska upprätta en förteckning över samhällsviktiga tjänster i de sektorer som avses i bilagan. De ska senast [tre år efter ikraftträdandet av detta direktiv] och därefter när så är nödvändigt och minst vart fjärde år göra en bedömning av alla relevanta risker som kan påverka tillhandahållandet av dessa samhällsviktiga tjänster i syfte att identifiera kritiska entiteter i enlighet med artikel 5.1 och bistå de kritiska entiteterna med att vidta åtgärder i enlighet med artikel 11.

   Riskbedömningen ska innehålla en redogörelse för alla relevanta naturliga risker och risker orsakade av människan, inbegripet olyckor, naturkatastrofer, hot mot

folkhälsan, antagonistiska hot, inklusive terroristbrott i enlighet med Europaparlamentets och rådets direktiv (EU) 2017/541[34].

2. När medlemsstaterna gör riskbedömningen ska de åtminstone ta hänsyn till följande:

   (a) Den allmänna riskbedömning som har utförts i enlighet med artikel 6.1 i Europaparlamentets och rådets beslut nr 1313/2013/EU[35].

   (b) Andra relevanta riskbedömningar som har utförts i enlighet med kraven i de relevanta sektorsspecifika rättsakterna i unionsrätten, inbegripet Europaparlamentets och rådets förordning (EU) 2019/941[36] och Europaparlamentets och rådets förordning (EU) 2017/1938[37].

   (c) Alla risker som uppstår till följd av beroendeförhållanden mellan de sektorer som avses i bilagan, inbegripet från andra medlemsstater och tredjeländer, samt de konsekvenser en störning i en sektor kan få för andra sektorer.

   (d) Eventuell information om incidenter som har rapporterats i enlighet med artikel 13.

   Vid tillämpningen av första stycket led c ska medlemsstaterna samarbeta med de behöriga myndigheterna i andra medlemsstater och tredjeländer, i förekommande fall.

3. Medlemsstaterna ska göra de relevanta delarna i den riskbedömning som avses i punkt 1 tillgängliga för de kritiska entiteter som de har identifierat i enlighet med artikel 5 för att bistå dessa entiteter när de utför sin riskbedömning i enlighet med artikel 10 och vidtar åtgärder för att säkerställa sin motståndskraft i enlighet med artikel 11.

4. Varje medlemsstat ska lämna uppgifter till kommissionen om de typer av risker som har identifierats och resultatet av riskbedömningarna, per sektor och undersektor i enlighet med vad som avses i bilagan, senast [tre år efter ikraftträdandet av detta direktiv] och därefter vid behov och minst vart fjärde år.

5. Kommissionen får i samarbete med medlemsstaterna utveckla en frivillig gemensam rapporteringsmall som kan användas för att uppfylla punkt 4.

Artikel 5
Identifiering av kritiska entiteter

1. Medlemsstaterna ska senast [tre år och tre månader efter ikraftträdandet av detta direktiv] identifiera de kritiska entiteterna för varje sektor och undersektor som avses i bilagan, med undantag för punkterna 3, 4 och 8 i bilagan.

---

34 Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF (EUT L 88, 31.3.2017, s. 6).

35 Europaparlamentets och rådets beslut nr 1313/2013/EU av den 17 december 2013 om en civilskyddsmekanism för unionen (EUT L 347, 20.12.2013, s. 924).

36 Europaparlamentets och rådets förordning (EU) 2019/941 av den 5 juni 2019 om riskberedskap inom elsektorn och om upphävande av direktiv 2005/89/EG (EUT L 158, 14.6.2019, s. 1).

37 Europaparlamentets och rådets förordning (EU) 2017/1938 av den 25 oktober 2017 om åtgärder för att säkerställa försörjningstryggheten för gas och om upphävande av förordning (EU) nr 994/2010 (EUT L 280, 28.10.2017, s. 1).

2. När medlemsstaterna identifierar kritiska entiteter i enlighet med punkt 1 ska de ta hänsyn till resultatet av riskbedömningen i enlighet med artikel 4 och tillämpa följande kriterier:

   (a) Entiteten tillhandahåller en eller flera samhällsviktiga tjänster.

   (b) (Tillhandahållandet av den tjänsten är beroende av infrastruktur som är belägen i den medlemsstaten.

   (c) En incident skulle få betydande störande effekter för tillhandahållandet av tjänsten eller av andra samhällsviktiga tjänster i de sektorer som avses i bilagan och som är beroende av tjänsten.

3. Varje medlemsstat ska upprätta en förteckning över de kritiska entiteter som har identifierats och säkerställa att dessa kritiska entiteter underrättas om att de har identifierats som kritiska entiteter inom en månad från identifieringen, varvid de ska informeras om sina skyldigheter i enlighet med kapitlen II och III och om från och med vilket datum bestämmelserna i de kapitlen är tillämpliga på dem.

   För de berörda kritiska entiteterna ska bestämmelserna i detta kapitel vara tillämpliga från och med dagen för underrättelsen och bestämmelserna i kapitel III ska vara tillämpliga från och med sex månader efter den dagen.

4. Medlemsstaterna ska säkerställa att deras behöriga myndigheter som har utsetts i enlighet med artikel 8 i det här direktivet underrättar de behöriga myndigheter som medlemsstaterna har utsett i enlighet med artikel 8 i [det andra direktivet om säkerhet i nätverks- och informationssystem] om identiteten på de kritiska entiteter som de har identifierat enligt denna artikel inom en månad efter den identifieringen.

5. Efter den underrättelse som avses i punkt 3 ska medlemsstaterna säkerställa att de kritiska entiteterna lämnar information till sina behöriga myndigheter som har utsetts i enlighet med artikel 8 i detta direktiv om huruvida de har identifierats som en kritisk entitet i en eller flera andra medlemsstater. Om en entitet har identifierats som kritisk av två eller fler medlemsstater ska dessa medlemsstater samråda med varandra i syfte att minska bördan för den kritiska entiteten med avseende på de skyldigheter som anges i kapitel III.

6. Vid tillämpningen av kapitel IV ska medlemsstaterna säkerställa att kritiska entiteter efter den underrättelse som avses i punkt 3 lämnar information till sina behöriga myndigheter som har utsetts enligt artikel 8 i det här direktivet om huruvida de tillhandahåller samhällsviktiga tjänster till eller i mer än en tredjedel av medlemsstaterna. Om så är fallet ska den berörda medlemsstaten utan dröjsmål underrätta kommissionen om identiteten på dessa kritiska entiteter.

7. Medlemsstaterna ska när så är nödvändigt och minst vart fjärde år se över och i förekommande fall uppdatera förteckningen över identifierade kritiska entiteter.

   Om dessa uppdateringar leder till att ytterligare kritiska entiteter identifieras ska punkterna 3, 4, 5 och 6 tillämpas. Dessutom ska medlemsstaterna säkerställa att entiteter som inte längre identifieras som kritiska till följd av en sådan uppdatering underrättas om detta och om att de inte längre omfattas av skyldigheterna enligt kapitel III från och med mottagandet av underrättelsen.

Artikel 6
Betydande störande effekt

1. När medlemsstaterna fastställer om en störande effekt som avses i artikel 5.2 c är betydande, ska de beakta följande kriterier:

   (a) Antalet användare som är beroende av den tjänst som entiteten tillhandahåller.

   (b) Beroendegraden avseende tjänsten hos andra sektorer som anges i bilagan.

   (c) Vilka effekter incidenter skulle kunna ha på ekonomisk och samhällelig verksamhet, miljön eller den allmänna säkerheten, uttryckt i grad och varaktighet.

   (d) Entitetens marknadsandel på marknaden för sådana tjänster.

   (e) Det geografiska område som skulle kunna påverkas av en incident, inbegripet eventuella gränsöverskridande konsekvenser.

   (f) Entitetens betydelse för upprätthållandet av en tillräcklig nivå på tjänsten, med beaktande av tillgången till alternativa sätt för att tillhandahålla tjänsten.

2. Medlemsstaterna ska lämna följande information till kommissionen senast [tre år och tre månader efter ikraftträdandet av detta direktiv]:

   (a) Den förteckning över tjänster som avses i artikel 4.1.

   (b) Det antal kritiska entiteter som har identifierats för varje sektor och undersektor som avses i bilagan och den tjänst eller de tjänster som avses i artikel 4.1 som varje entitet tillhandahåller.

   (c) Eventuella tröskelvärden som har tillämpats för att närmare fastställa ett eller flera av de kriterier som anges i punkt 1.

   Därefter ska de lämna denna information när så är nödvändigt och minst vart fjärde år.

3. Kommissionen får efter samråd med gruppen för motståndskraft hos kritiska entiteter anta riktlinjer för att underlätta tillämpningen av de kriterier som avses i punkt 1, med hänsyn till den information som avses i punkt 2.

Artikel 7
Entiteter som är likvärdiga med kritiska entiteter enligt detta kapitel

1. När det gäller de sektorer som avses i punkterna 3, 4 och 8 i bilagan ska medlemsstaterna senast [tre år och tre månader efter ikraftträdandet av detta direktiv] identifiera de entiteter som ska behandlas som likvärdiga med kritiska entiteter vid tillämpningen av detta kapitel. De ska tillämpa bestämmelserna i artiklarna 3, 4, 5.1–5.4, 5.7 och 9 med avseende på sådana entiteter.

2. Vid tillämpningen av artikel 8.1 ska medlemsstaterna när det gäller entiteter i de sektorer som avses i punkterna 3 och 4 i bilagan som har identifierats i enlighet med punkt 1 säkerställa att de myndigheter som har utsetts som behöriga myndigheter är de behöriga myndigheter som har utsetts i enlighet med artikel 41 i [DORA-förordningen].

3. Medlemsstaterna ska säkerställa att de entiteter som avses i punkt 1 utan dröjsmål underrättas om att de har identifierats som de entiteter som avses i denna artikel.

Artikel 8

Behöriga myndigheter och gemensam kontaktpunkt

1. Varje medlemsstat ska utse en eller flera behöriga myndigheter som ansvariga för den korrekta tillämpningen och, i förekommande fall, för verkställandet av reglerna i detta direktiv på nationell nivå (nedan kallade *behöriga myndigheter*). Medlemsstaterna får utse en eller flera befintliga myndigheter.

   Om medlemsstaterna utser mer än en myndighet ska de tydligt fastställa de berörda myndigheternas respektive arbetsuppgifter och säkerställa att de samarbetar effektivt för att fullgöra sina uppgifter enligt detta direktiv, inbegripet vad gäller utseendet av och verksamheten inom den gemensamma kontaktpunkt som avses i punkt 2.

2. Varje medlemsstat ska inom den behöriga myndigheten utse en gemensam kontaktpunkt som ska ha en sambandsfunktion för att säkerställa gränsöverskridande samarbete med behöriga myndigheter i andra medlemsstater och med den grupp för motståndskraft hos kritiska entiteter som avses i artikel 16 (nedan kallad *gemensam kontaktpunkt*).

3. Den gemensamma kontaktpunkten ska senast [tre år och sex månader efter ikraftträdandet av detta direktiv], och därefter en gång om året, lämna en sammanfattande rapport till kommissionen och gruppen för motståndskraft hos kritiska entiteter om de rapporter som har mottagits, inklusive antalet rapporter, de rapporterade incidenternas art och vilka åtgärder som vidtagits i enlighet med artikel 13.3.

4. Varje medlemsstat ska säkerställa att den behöriga myndigheten, inbegripet den gemensamma kontaktpunkt som har utsetts inom myndigheten, har de befogenheter och tillräckliga ekonomiska, mänskliga och tekniska resurser som krävs för att på ett effektivt och ändamålsenligt sätt fullgöra de uppgifter som den har ålagts.

5. Medlemsstaterna ska säkerställa att deras behöriga myndigheter i förekommande fall och i enlighet med unionsrätten och nationell rätt samråder och samarbetar med andra relevanta nationella myndigheter, särskilt de som ansvarar för civilskydd, brottsbekämpning och skydd av personuppgifter, samt med relevanta berörda parter, inbegripet kritiska entiteter.

6. Medlemsstaterna ska säkerställa att deras behöriga myndigheter som har utsetts enligt denna artikel samarbetar med de behöriga myndigheter som har utsetts i enlighet med [det andra direktivet om säkerhet i nätverks- och informationssystem] om cybersäkerhetsrisker och cyberincidenter som påverkar kritiska entiteter samt de åtgärder som vidtas av behöriga myndigheter som har utsetts i enlighet med [det andra direktivet om säkerhet i nätverks- och informationssystem] som är relevanta för kritiska entiteter.

7. Varje medlemsstat ska underrätta kommissionen om att den behöriga myndigheten och den gemensamma kontaktpunkten har utsetts inom tre månader efter utseendet, inbegripet deras exakta arbetsuppgifter och ansvarsområden enligt detta direktiv, deras kontaktuppgifter samt alla senare ändringar av dessa. Varje medlemsstat ska offentliggöra utseendet av den behöriga myndigheten och den gemensamma kontaktpunkten.

8. Kommissionen ska offentliggöra förteckningen över medlemsstaternas gemensamma kontaktpunkter.

Artikel 9
Medlemsstaternas stöd till kritiska entiteter

1. Medlemsstaterna ska stödja kritiska entiteter för att öka deras motståndskraft. Stödet får innefatta utveckling av vägledningsmaterial och metoder, stöd till anordnande av övningar för att testa deras motståndskraft och tillhandahållande av utbildning för kritiska entiteters personal.

2. Medlemsstaterna ska säkerställa att de behöriga myndigheterna samarbetar och utbyter information och god praxis med kritiska entiteter i de sektorer som avses i bilagan.

3. Medlemsstaterna ska införa informationsdelningsverktyg till stöd för frivillig informationsdelning mellan kritiska entiteter i frågor som omfattas av detta direktiv, i enlighet med unionsrätten och nationell rätt, särskilt i fråga om konkurrens och skydd av personuppgifter.

KAPITEL III
KRITISKA ENTITETERS MOTSTÅNDSKRAFT

Artikel 10
Riskbedömning av kritiska entiteter

Medlemsstaterna ska säkerställa att kritiska entiteter inom sex månader efter mottagandet av den underrättelse som avses i artikel 5.3 och därefter när det är nödvändigt och minst vart fjärde år, gör en bedömning av alla relevanta risker som kan störa deras verksamhet, på grundval av medlemsstaternas riskbedömningar och andra relevanta informationskällor.

Riskbedömningen ska innehålla en redogörelse för alla relevanta risker som avses i artikel 4.1 som skulle kunna leda till en störning i tillhandahållandet av samhällsviktiga tjänster. Bedömningen ska ta hänsyn till det eventuella beroendet hos andra sektorer som avses i bilagan av den samhällsviktiga tjänst som tillhandahålls av den kritiska entiteten, inbegripet i angränsande medlemsstater och tredjeländer i förekommande fall, samt de konsekvenser som en störning i tillhandahållandet av samhällsviktiga tjänster i en eller flera av dessa sektorer skulle kunna få för den samhällsviktiga tjänst som den kritiska entiteten tillhandahåller.

Artikel 11
Kritiska entiteters åtgärder för motståndskraft

1. Medlemsstaterna ska säkerställa att kritiska entiteter vidtar lämpliga och proportionella tekniska och organisatoriska åtgärder för att säkerställa sin motståndskraft, däribland åtgärder som är nödvändiga för att

   (a) förhindra incidenter från att uppstå, inbegripet genom åtgärder för katastrofriskreducering och anpassning till klimatförändringar,

   (b) säkerställa ett tillfredsställande fysiskt skydd av känsliga områden, anläggningar och annan infrastruktur, inbegripet stängsel, barriärer, verktyg och rutiner för övervakning av områdesgränser samt detektionsutrustning och åtkomstkontroller,

(c) stå emot och lindra konsekvenserna av incidenter, inbegripet genomförande av risk- och krishanteringsförfaranden och protokoll samt varningsrutiner,

(d) återhämta sig från incidenter, inklusive åtgärder för driftskontinuitet och identifiering av alternativa försörjningskedjor,

(e) säkerställa en ändamålsenlig hantering av personalsäkerhet, däribland genom att fastställa kategorier för personal som utför kritiska funktioner, fastställa åtkomsträttigheter för känsliga områden, lokaler och annan infrastruktur, och till känslig information, samt identifiera särskilda personalkategorier med avseende på artikel 12,

(f) öka medvetenheten om de åtgärder som avses i punkterna a–e hos berörd personal.

2. Medlemsstaterna ska säkerställa att kritiska entiteter har en plan för motståndskraft, som de tillämpar, eller ett eller flera likvärdiga dokument, med en detaljerade beskrivning av åtgärderna enligt punkt 1. Om kritiska entiteter har vidtagit åtgärder i enlighet med de skyldigheter som anges i andra rättsakter i unionsrätten som också är relevanta för de åtgärder som avses i punkt 1 ska entiteterna också beskriva dessa åtgärder i planen för motståndskraft eller i det likvärdiga dokumentet eller dokumenten.

3. På begäran av den medlemsstat som identifierade den kritiska entiteten och med den berörda kritiska entitetens samtycke ska kommissionen anordna rådgivande uppdrag i enlighet med de arrangemang som fastställs i artiklarna 15.4, 15.5, 15.7 och 15.8 för att tillhandahålla rådgivning för den berörda kritiska entiteten med att uppfylla sina skyldigheter i enlighet med kapitel III. Det rådgivande uppdraget ska rapportera sina slutsatser till kommissionen, medlemsstaten och den berörda kritiska entiteten.

4. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 21 för att komplettera punkt 1 genom att fastställa närmare bestämmelser om några eller samtliga åtgärder som ska vidtas i enlighet med den punkten. Den ska anta sådana delegerade akter i den utsträckning det är nödvändigt för att den punkten ska kunna tillämpas effektivt och konsekvent i enlighet med målen för detta direktiv, med beaktande av all relevant utveckling i fråga om risker, teknik eller tillhandahållande av de berörda tjänsterna och av eventuella särdrag för vissa sektorer och typer av entiteter.

5. Kommissionen ska anta genomförandeakter för att fastställa de nödvändiga tekniska och metodrelaterade specifikationerna för tillämpningen av de åtgärder som avses i punkt 1. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 20.2.

Artikel 12
Säkerhetskontroller

1. Medlemsstaterna ska säkerställa att kritiska entiteter får ansöka om säkerhetskontroller av personer som omfattas av särskilda personalkategorier, inbegripet personer som övervägs för rekrytering till tjänster som omfattas av de kategorierna, och att dessa ansökningar behandlas snabbt av de myndigheter som är ansvariga för att utföra sådana säkerhetskontroller.

2. I enlighet med gällande unionsrätt och nationell rätt, inklusive Europaparlamentets och rådets förordning (EU) 2016/679/EU [38] ska en sådan säkerhetskontroll som avses i punkt 1

(a) fastställa personens identitet på grundval av styrkande dokument,

(b) omfatta utdrag ur straffregistret för åtminstone de föregående fem åren och för högst tio år gällande brott som är relevanta för rekrytering till en viss tjänst i den eller de medlemsstater som personen är medborgare i och i alla medlemsstater eller tredjeländer som personen har varit bosatt i under den tidsperioden,

(c) omfatta tidigare anställningar, utbildning och eventuella luckor i utbildning eller anställning i personens meritförteckning under åtminstone de föregående fem åren och för högst tio år.

När det gäller första stycket led b ska medlemsstaterna säkerställa att deras myndigheter som är behöriga att göra säkerhetskontroller inhämtar uppgifter ur kriminalregister hos andra medlemsstater via Ecris i enlighet med de förfaranden som fastställs i rådets rambeslut 2009/315/RIF och, i förekommande fall, Europaparlamentets och rådets förordning (EU) 2019/816[39]. De centralmyndigheter som avses i artikel 3 i det rambeslutet och i artikel 3.5 i den förordningen ska besvara begäranden om sådana uppgifter inom tio arbetsdagar från och med den dag då begäran togs emot.

3. I enlighet med gällande unionsrätt och nationell rätt, inbegripet förordning (EU) 2016/679, ska varje medlemsstat säkerställa att en sådan säkerhetskontroll som avses i punkt 1 också kan utökas på grundval av en motiverad begäran från den kritiska entiteten, så att den omfattar underrättelser och all annan tillgänglig objektiv information som kan vara nödvändig för att avgöra om den berörda personen är lämplig för att arbeta i den befattning för vilken den kritiska entiteten har begärt en utökad säkerhetskontroll.

Artikel 13
Incidentrapportering

1. Medlemsstaterna ska säkerställa att kritiska entiteter utan onödigt dröjsmål underrättar den behöriga myndigheten om incidenter som medför en betydande störning eller kan medföra en betydande störning av deras verksamhet. Underrättelserna ska omfatta all tillgänglig information som är nödvändig för att den behöriga myndigheten ska kunna förstå incidentens art, orsak och möjliga konsekvenser, bl.a. för att kunna fastställa incidentens eventuella gränsöverskridande verkningar. Sådana underrättelser ska inte medföra ett ökat ansvar för de kritiska entiteterna.

2. För att fastställa störningens eller den potentiella störningens betydelse för den kritiska entitetens verksamhet till följd av en incident ska framför allt följande parametrar beaktas:

(a) Antalet användare som påverkas av störningen eller den potentiella störningen.

[38] EUT L 119, 4.5.2016, s. 1.
[39] EUT L 135, 22.5.2019, s. 1.

(b) Störningens varaktighet eller den förväntade varaktigheten av en potentiell störning.

(c) Det geografiska område som påverkas av störningen eller den potentiella störningen.

3. På grundval av den information som lämnas i underrättelsen från den kritiska entiteten ska den behöriga myndigheten via sin gemensamma kontaktpunkt informera den gemensamma kontaktpunkten hos andra medlemsstater som påverkas om incidenten har, eller kan ha, betydande verkningar på kritiska entiteter och kontinuiteten i tillhandahållandet av samhällsviktiga tjänster i en eller flera andra medlemsstater.

När de gemensamma kontaktpunkterna gör detta ska de i enlighet med unionsrätten eller nationell lagstiftning som är förenlig med unionsrätten behandla informationen på ett sätt som respekterar dess konfidentialitet och skyddar den berörda kritiska entitetens säkerhet och kommersiella intressen.

4. Så snart som möjligt efter att ha underrättats i enlighet med punkt 1 ska den behöriga myndigheten ge den kritiska entitet som underrättade den relevant information om uppföljningen av underrättelsen, inklusive information som skulle kunna hjälpa den kritiska entiteten att reagera ändamålsenligt på incidenten.

KAPITEL IV
SÄRSKILD TILLSYN ÖVER KRITISKA ENTITETER AV SÄRSKILD EUROPEISK BETYDELSE

Artikel 14
Kritiska entiteter av särskild europeisk betydelse

1. Kritiska entiteter av särskild europeisk betydelse ska omfattas av särskild tillsyn i enlighet med detta kapitel.

2. En entitet ska betraktas som en kritisk entitet av särskild europeisk betydelse när den har identifierats som en kritisk entitet och den tillhandahåller samhällsviktiga tjänster till eller i mer än en tredjedel av medlemsstaterna och har underrättats vara en sådan entitet till kommissionen i enlighet med artikel 5.1 respektive artikel 5.6.

3. När kommissionen har tagit emot underrättelsen i enlighet med artikel 5.6 ska den utan onödigt dröjsmål underrätta den berörda entiteten om att den betraktas som en kritisk entitet av särskild europeisk betydelse och informera entiteten om dess skyldigheter i enlighet med detta kapitel samt från och med vilken dag dessa skyldigheter är tillämpliga på den.

Bestämmelserna i detta kapitel ska tillämpas på den berörda kritiska entiteten av särskild europeisk betydelse från och med dagen för mottagandet av den underrättelsen.

Artikel 15
Särskild tillsyn

1. På begäran av en eller flera medlemsstater eller av kommissionen ska den medlemsstat där infrastrukturen för den kritiska entiteten av särskild europeisk betydelse är belägen, tillsammans med den entiteten, informera kommissionen och

gruppen för kritiska entiteters motståndskraft om resultatet av den riskbedömning som har utförts i enlighet med artikel 10 och de åtgärder som har vidtagits i enlighet med artikel 11.

Den medlemsstaten ska också, utan onödigt dröjsmål, informera kommissionen och gruppen för kritiska entiteters motståndskraft om eventuella tillsyns- eller verkställighetsåtgärder, inbegripet eventuella bedömningar av efterlevnad eller utfärdade förelägganden, som dess behöriga myndighet har vidtagit i enlighet med artiklarna 18 och 19 med avseende på den entiteten.

2. Kommissionen ska på begäran av en eller flera medlemsstater eller på eget initiativ, och med samtycke från den medlemsstat där infrastrukturen för den kritiska entiteten av särskild europeisk betydelse är belägen, anordna ett rådgivande uppdrag för att bedöma de åtgärder som entiteten har vidtagit för att uppfylla sina skyldigheter i enlighet med kapitel III. Vid behov får de rådgivande uppdragen begära särskild expertis inom området för riskhantering via Centrumet för samordning av katastrofberedskap.

3. Det rådgivande uppdraget ska rapportera sina slutsatser till kommissionen, gruppen för kritiska entiteters motståndskraft och den berörda kritiska entiteten av särskild europeisk betydelse inom tre månader efter det att det rådgivande uppdraget har avslutats.

Gruppen för kritiska entiteters motståndskraft ska analysera rapporten och, om så är nödvändigt, ge kommissionen råd om huruvida den berörda kritiska entiteten av särskild europeisk betydelse uppfyller sina skyldigheter i enlighet med kapitel III och, i förekommande fall, vilka åtgärder som skulle kunna vidtas för att förbättra entitetens motståndskraft.

Kommissionen ska på grundval av rådgivningen meddela sina synpunkter till den medlemsstat där entitetens infrastruktur är belägen, gruppen för kritiska entiteters motståndskraft och entiteten om huruvida entiteten uppfyller sina skyldigheter i enlighet med kapitel III och i förekommande fall vilka åtgärder som skulle kunna vidtas för att förbättra entitetens motståndskraft.

Den medlemsstaten ska ta vederbörlig hänsyn till dessa synpunkter och lämna information till kommissionen och gruppen för kritiska entiteters motståndskraft om alla åtgärder som den har vidtagit i enlighet med meddelandet.

4. Varje rådgivande uppdrag ska bestå av experter från medlemsstaterna och kommissionens företrädare. Medlemsstaterna får föreslå kandidater för att delta i ett rådgivande uppdrag. Kommissionen ska välja ut och utnämna medlemmarna i varje rådgivande uppdrag i enlighet med deras yrkesmässiga kapacitet och säkerställa en geografiskt balanserad representation mellan medlemsstaterna. Kommissionen ska täcka kostnaderna i samband med deltagandet i det rådgivande uppdraget.

Kommissionen ska anordna programmet för ett rådgivande uppdrag i samråd med deltagarna i det specifika rådgivande uppdraget och i överenskommelse med den medlemsstat där infrastrukturen för den kritiska entiteten eller den kritiska entiteten av särskild europeisk betydelse är belägen.

5. Kommissionen ska anta en genomförandeakt om regler för förfaranden för genomförande av och rapportering från rådgivande uppdrag. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 20.2.

6. Medlemsstaterna ska säkerställa att den berörda kritiska entiteten av särskild europeisk betydelse ger det rådgivande uppdraget åtkomst till alla uppgifter, system och anläggningar som rör tillhandahållandet av dess samhällsviktiga tjänster som är nödvändiga för utförandet av dess uppgifter.

7. Det rådgivande uppdraget ska genomföras i enlighet med gällande nationell rätt i den medlemsstat där infrastrukturen är belägen.

8. När kommissionen anordnar rådgivande uppdrag ska den ta hänsyn till rapporterna från alla inspektioner som kommissionen har genomfört i enlighet med förordning (EG) nr 300/2008 och förordning (EG) nr 725/2004 och till rapporterna från all övervakning som kommissionen har utfört i enlighet med direktiv 2005/65/EG med avseende på den kritiska entiteten eller den kritiska entiteten av särskild europeisk betydelse, i förekommande fall.

KAPITEL V
SAMARBETE OCH RAPPORTERING

Artikel 16
Gruppen för kritiska entiteters motståndskraft

1. En grupp för kritiska entiteters motståndskraft ska inrättas med verkan från och med [sex månader efter ikraftträdandet av detta direktiv]. Gruppen ska ge kommissionen stöd och underlätta strategiskt samarbete och informationsutbyte om frågor som rör detta direktiv.

2. Gruppen för kritiska entiteters motståndskraft ska bestå av företrädare för medlemsstaterna och kommissionen. Gruppen för kritiska entiteters motståndskraft får bjuda in företrädare från berörda parter att dela i sitt arbete när detta är relevant för fullgörandet av gruppens arbetsuppgifter.

   Kommissionens företrädare ska vara ordförande för gruppen för kritiska entiteters motståndskraft.

3. Gruppen för kritiska entiteters motståndskraft ska ha följande arbetsuppgifter:

   (a) Stödja kommissionen med att bistå medlemsstaterna för att stärka deras kapacitet att bidra till att säkerställa kritiska entiteters motståndskraft i enlighet med detta direktiv.

   (b) Utvärdera de strategier för kritiska entiteters motståndskraft som avses i artikel 3 och identifiera bästa praxis för sådana strategier.

   (c) Underlätta utbyte av bästa praxis i fråga om medlemsstaternas identifiering av kritiska entiteter i enlighet med artikel 5, inbegripet i förhållande till gränsöverskridande beroenden och med avseende på risker och incidenter.

   (d) På begäran bidra till utarbetandet av de riktlinjer som avses i artikel 6.3 och eventuella delegerade akter och genomförandeakter för detta direktiv.

   (e) Årligen studera de sammanfattande rapporter som avses i artikel 8.3.

   (f) Utbyta bästa praxis om informationsutbyte angående incidentrapportering som avses i artikel 13.

(g) Analysera och utfärda råd om rapporterna från rådgivande uppdrag i enlighet med artikel 15.3.

(h) Utbyta information och bästa praxis om forskning och utveckling som rör kritiska entiteters motståndskraft i enlighet med detta direktiv.

(i) Vid behov utbyta information om frågor som rör kritiska entiteters motståndskraft med unionens berörda institutioner, organ och byråer.

4. Gruppen för kritiska entiteters motståndskraft ska, senast [24 månader efter ikraftträdandet av detta direktiv] och därefter vartannat år, utarbeta ett arbetsprogram med åtgärder som ska vidtas för att genomföra dess mål och uppgifter, som ska överensstämma med kraven i och målen för detta direktiv.

5. Gruppen för kritiska entiteters motståndskraft ska regelbundet och minst en gång om året ha ett möte med den samarbetsgrupp som har inrättats i enlighet med [det andra direktivet om säkerhet i nätverks- och informationssystem] för att främja strategiskt samarbete och informationsutbyte.

6. Kommissionen får anta genomförandeakter i vilka fastställs de förfaranden som krävs för verksamheten i gruppen för kritiska entiteters motståndskraft. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 20.2.

7. Kommissionen ska till gruppen för kritiska entiteters motståndskraft lämna en sammanfattande rapport om den information som har lämnats av medlemsstaterna i enlighet med artiklarna 3.3 och 4.4 senast [tre år och sex månader efter ikraftträdandet av detta direktiv] och därefter vid behov och minst vart fjärde år.

Artikel 17
Kommissionens stöd till behöriga myndigheter och kritiska entiteter

1. Kommissionen ska i förekommande fall ge medlemsstaterna och de kritiska entiteterna stöd för att uppfylla sina skyldigheter enligt detta direktiv, särskilt genom att utarbeta en översikt på unionsnivå över gränsöverskridande och sektorsöverskridande risker för tillhandahållandet av samhällsviktiga tjänster, anordna de rådgivande uppdrag som avses i artiklarna 11.3 och 15.3 och underlätta informationsutbyte mellan experter i hela unionen.

2. Kommissionen ska komplettera medlemsstaternas verksamhet som avses i artikel 9 genom att utveckla bästa praxis och metoder och genom att utveckla gränsöverskridande utbildningstillfällen och övningar för att testa kritiska entiteters motståndskraft.

KAPITEL VI
TILLSYN OCH EFTERLEVNADSKONTROLL

Artikel 18
Genomförande och efterlevnad

1. För att bedöma om de entiteter som medlemsstaterna har identifierat som kritiska entiteter i enlighet med artikel 5 fullgör skyldigheter enligt detta direktiv ska de säkerställa att de behöriga myndigheterna har befogenheter och medel för att

(a) genomföra inspektioner på plats av de lokaler som den kritiska entiteten använder för att tillhandahålla sina samhällsviktiga tjänster och tillsyn på distans av kritiska entiteters åtgärder enligt artikel 11,

(b) utföra eller beställa revisioner av dessa entiteter.

2. Medlemsstaterna ska säkerställa att de behöriga myndigheterna har befogenheter och medel för att, när så är nödvändigt för att fullgöra deras uppgifter enligt detta direktiv, kräva att de entiteter som de har identifierat som kritiska entiteter enligt punkt 5 inom en rimlig tidsfrist, som fastställs av dessa myndigheter, lämnar

(a) den information som är nödvändig för att bedöma om de åtgärder som entiteterna har vidtagit för att säkerställa sin motståndskraft uppfyller kraven i artikel 11,

(b) bevis på att de åtgärderna faktiskt har genomförts, inklusive resultatet av en revision som har utförts av en oberoende och kvalificerad oberoende revisor som har valts av entiteten och som har utförts på entitetens bekostnad.

När de behöriga myndigheterna begär denna information ska de ange syftet med kravet och specificera vilken information som krävs.

3. Utan att det påverkar möjligheten att besluta om sanktioner i enlighet med artikel 19 får de behöriga myndigheterna, efter de tillsynsåtgärder som avses i punkt 1 eller den bedömning av information som avses i punkt 2, beordra de berörda kritiska entiteterna att vidta de åtgärder som är nödvändiga och proportionella för att avhjälpa alla konstaterade överträdelser av detta direktiv, inom en rimlig tidsfrist som fastställs av myndigheterna, och att lämna information om de åtgärder som har vidtagits till myndigheterna. Sådana förelägganden ska framför allt ta hänsyn till hur allvarlig överträdelsen är.

4. Medlemsstaterna ska säkerställa att de befogenheter som anges i punkterna 1, 2 och 3 endast kan utövas om de omfattas av lämpliga skyddsåtgärder. Sådana skyddsåtgärder ska framför allt garantera att befogenheterna utövas på ett objektivt, öppet och proportionerligt sätt och att de berörda kritiska entiteternas rättigheter och legitima intressen skyddas på vederbörligt sätt, däribland deras rätt att höras, rätt till försvar och rätt till rättslig prövning inför en oberoende domstol.

5. Medlemsstaterna ska säkerställa att när en behörig myndighet bedömer efterlevnaden hos en kritisk entitet enligt denna artikel ska den informera de behöriga myndigheter i den berörda medlemsstaten som har utsetts enligt [det andra direktivet om säkerhet i nätverks- och informationssystem] och får begära att dessa myndigheter ska bedöma entitetens cybersäkerhet samt samarbeta och utbyta information i detta syfte.

Artikel 19
Sanktioner

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av de nationella bestämmelser som antagits enligt detta direktiv och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska anmäla bestämmelserna till kommissionen senast [två år efter det att direktivet träder i kraft], och utan dröjsmål anmäla eventuella ändringar som berör dessa.

KAPITEL VII
SLUTBESTÄMMELSER

Artikel 20
Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.
2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

Artikel 21
Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.
2. Den befogenhet att anta delegerade akter som avses i artikel 11.4 ska ges till kommissionen för en period på fem år från och med den dag då detta direktiv träder i kraft eller ett annat datum som fastställs av medlagstiftarna.
3. Den delegering av befogenhet som avses i artikel 11.4 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.
4. Innan kommissionen antar en delegerad akt, ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet om bättre lagstiftning av den 13 april 2016.
5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.
6. En delegerad akt som antas enligt artikel 11.4 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 22
Rapportering och översyn

Kommissionen ska senast [54 månader efter ikraftträdandet av detta direktiv] överlämna en rapport till Europaparlamentet och rådet med en bedömning av i vilken utsträckning medlemsstaterna har vidtagit de åtgärder som är nödvändiga för att följa detta direktiv.

Kommissionen ska regelbundet se över hur detta direktiv fungerar och rapportera resultaten till Europaparlamentet och rådet. Rapporten ska framför allt bedöma effekten och mervärdet av detta direktiv när det gäller att säkerställa kritiska entiteters motståndskraft och huruvida

direktivets tillämpningsområde bör utökas till att omfatta andra sektorer eller undersektorer. Den första rapporten ska lämnas senast [sex år efter ikraftträdandet av detta direktiv] och ska särskilt innehålla en bedömning av huruvida direktivets tillämpningsområde bör utökas till att omfatta sektorn för produktion, bearbetning och distribution av livsmedel.

Artikel 23
Upphävande av direktiv 2008/114/EG

Direktiv 2008/114/EU ska upphöra att gälla med verkan från och med [dagen för detta direktivs ikraftträdande].

Artikel 24
Införlivande

1. Medlemsstaterna ska senast [18 månader efter detta direktivs ikraftträdande] anta och offentliggöra de lagar och andra författningar som är nödvändiga för att följa detta direktiv. De ska genast överlämna texten till dessa bestämmelser till kommissionen.

   De ska tillämpa bestämmelserna från och med [två år efter ikraftträdandet av detta direktiv plus en dag].

   När en medlemsstat antar dessa bestämmelser ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

2. Medlemsstaterna ska till kommissionen överlämna texten till de centrala bestämmelser i nationell rätt som de antar inom det område som omfattas av detta direktiv.

Artikel 25
Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 26
Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Bryssel den

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets titel

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

om kritiska entiteters motståndskraft

1.2. Berörda politikområden

Säkerhet

1.3. Typ av förslag eller initiativ

☐ **en ny åtgärd**

☐ **en ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd**[40]

☑ **en förlängning av en befintlig åtgärd**

☐ **en sammanslagning eller omdirigering av en eller flera åtgärder mot en annan/en ny åtgärd**

1.4. Mål

1.4.1. Allmänt/allmänna mål:

Operatörer av kritisk infrastruktur tillhandahåller tjänster inom ett antal sektorer (t.ex. transport, energi, hälso- och sjukvård, vatten osv.) som är nödvändiga för centrala samhällsfunktioner och central ekonomisk verksamhet. Därför behöver operatörerna vara motståndskraftiga, dvs. väl skyddade, men de bör också snabbt kunna återuppta driften vid en eventuell störning.

Det allmänna målet för förslaget är att stärka motståndskraften hos dessa operatörer (nedan kallade *kritiska entiteter*) mot en rad naturliga risker och risker orsakade av människan, avsiktligt eller oavsiktliga orsakade risker.

1.4.2. Specifikt/specifika mål:

Initiativet är inriktat på fyra särskilda mål:

– Säkerställa en ökad förståelse av de risker och ömsesidiga beroenden som kritiska entiteter ställs inför, samt hur de ska hanteras.

– Säkerställa att alla berörda entiteter i alla viktiga sektorer identifieras som ”kritiska entiteter” av medlemsstaternas myndigheter.

– Säkerställa att hela spektrumet av åtgärder för motståndskraft tas med i offentliga riktlinjer och operativ praxis.

– Stärka kapacitet och förbättra samarbete och kommunikation mellan berörda parter.

Dessa mål kommer att bidra till att det allmänna målet för initiativet uppnås.

1.4.3. Verkan eller resultat som förväntas

Beskriv den verkan som förslaget eller initiativet förväntas få på de mottagare eller den del av befolkningen som berörs.

[40] I den mening som avses i artikel 58.2 a eller b i budgetförordningen.

Initiativet väntas få positiva effekter på säkerheten hos kritiska entiteter, som skulle få större motståndskraft mot risker och störningar. De skulle kunna minska risker på ett bättre sätt, hantera potentiella störningar och minimera negativa konsekvenser om det inträffar incidenter.

Att kritiska entiteters motståndskraft ökar innebär också att deras verksamhet blir mer tillförlitlig och att deras tjänster i många centrala sektorer tillhandahålls fortlöpande, vilket bidrar till att den inre marknaden fungerar väl. Detta kommer i sin tur att få positiva effekter för allmänheten och företagen, eftersom de är beroende av dessa tjänster i sin dagliga verksamhet.

Offentliga myndigheter skulle också gynnas av den stabilitet som skapas av att central ekonomisk verksamhet kan bedrivas problemfritt och att samhällsviktiga tjänster tillhandahålls utan avbrott till invånarna.

1.4.4. Prestationsindikatorer

Ange indikatorer för övervakning av framsteg och resultat.

Indikatorerna för att övervaka framsteg och resultat kommer att vara knutna till de särskilda målen för initiativet:

– Antalet och omfattningen av de riskbedömningar som görs av myndigheter och kritiska entiteter kommer att vara ett proxyvärde för de centrala aktörernas ökade förståelse av riskerna.

– Det antal ”kritiska entiteter” som identifieras av medlemsstaterna kommer att avspegla hur heltäckande riktlinjerna för kritisk infrastruktur är.

– Integreringen av motståndskraft i offentliga riktlinjer och operativ praxis kommer att avspeglas i de nationella strategierna och de kritiska entiteternas åtgärder för motståndskraft.

– Förbättringar vad gäller kapacitet och samarbete kommer att bedömas på grundval av åtgärder för kapacitetsuppbyggnad och samarbetsinitiativ som har utvecklats.

1.5. Grunder för förslaget eller initiativet

1.5.1. Krav som ska uppfyllas på kort eller lång sikt, inbegripet en detaljerad tidsplan för genomförandet av initiativet

För att uppfylla kraven enligt initiativet kommer medlemsstaterna att på kort eller medellång sikt behöva utveckla en strategi för kritiska entiteters motståndskraft, genomföra en nationell riskbedömning och identifiera vilka operatörer som är ”kritiska entiteter” på grundval av resultatet av riskbedömningen och särskilda kriterier. Denna verksamhet kommer att genomföras regelbundet, när det behövs, och åtminstone vart fjärde år. Medlemsstaterna kommer också att behöva inrätta samarbetsmekanismer mellan berörda parter.

De operatörer som utses som ”kritiska entiteter” skulle på kort till medellång sikt behöva göra en egen riskbedömning, vidta lämpliga och proportionella tekniska och organisatoriska åtgärder för att säkerställa sin motståndskraft och rapportera incidenter till behöriga myndigheter.

1.5.2. Mervärdet i unionens intervention (som kan följa av flera faktorer, t.ex. samordningsfördelar, rättssäkerhet, ökad effektivitet eller komplementaritet). Med ”mervärdet i unionens intervention” i denna punkt avses det värde en åtgärd från

unionens sida tillför utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.

Skäl för åtgärder på europeisk nivå (ex ante): Målet för detta initiativ är att stärka kritiska entiteters motståndskraft mot en rad risker. Detta mål kan inte i tillräcklig utsträckning uppnås av medlemsstaterna var och en för sig: åtgärden på EU-nivå är motiverad på grund av de gemensamma egenskaperna hos de risker som kritiska entiteter ställs inför, de transnationella egenskaperna hos de tjänster som de tillhandahåller och de ömsesidiga beroendena och kopplingarna mellan dem (över sektorer och gränser). Detta betyder att en sårbarhet eller en störning i en enskild anläggning skulle kunna orsaka störningar över sektorer och gränser. Förväntat mervärde för unionen (ex post): Jämfört med den nuvarande situationen kommer det föreslagna initiativet att ge ett mervärde, särskilt genom att – upprätta en allmän ram som skulle främja en närmare anpassning mellan medlemsstaternas politik (enhetlig räckvidd i fråga om sektorer, enhetliga kriterier för att utse kritiska entiteter, gemensamma krav i fråga om riskbedömningar), – säkerställa att kritiska entiteter vidtar lämpliga åtgärder för motståndskraft, – sammanföra kunskaper och expertis från hela EU som skulle optimera insatserna från kritiska entiteter och myndigheter, – minska skillnaderna mellan medlemsstater och höja nivån på kritiska entiteters motståndskraft i hela EU.

1.5.3. Erfarenheter från tidigare liknande åtgärder

Förslaget bygger på lärdomarna av genomförandet av direktivet om europeisk kritisk infrastruktur (direktiv 2008/114/EG) och utvärderingen av det (SWD(2019 308).

1.5.4. Förenlighet med den fleråriga budgetramen och eventuella synergieffekter med andra relevanta instrument

Detta förslag är en av byggstenarna i den nya strategin för EU:s säkerhetsunion som syftar till att skapa en framtidssäkrad säkerhetsmiljö. Synergier kan utvecklas med unionens civilskyddsmekanism när det gäller att förebygga, lindra och hantera katastrofer.

1.6. Varaktighet för och budgetkonsekvenser av förslaget eller initiativet

☐ **begränsad varaktighet**

☐ verkan från och med [den DD/MM]ÅÅÅÅ till och med [den DD/MM]ÅÅÅÅ

☐ budgetkonsekvenser från och med YYYY till och med YYYY för åtagandebemyndiganden och från och med YYYY till och med YYYY för betalningsbemyndiganden.

☑ **obegränsad varaktighet**

- Efter en inledande period 2021–2027
- beräknas genomförandetakten nå en stabil nivå.

1.7. Planerad metod för genomförandet[41]

☑ **Direkt förvaltning** som sköts av kommissionen

☑ av dess avdelningar, vilket också inbegriper personalen vid unionens delegationer;

☐ av genomförandeorgan

☑ **Delad förvaltning** med medlemsstaterna

☐ **Indirekt förvaltning** genom att uppgifter som ingår i budgetgenomförandet anförtros

☐ tredjeländer eller organ som de har utsett

☐ internationella organisationer och organ kopplade till dem (ange vilka)

☐ EIB och Europeiska investeringsfonden

☐ organ som avses i artiklarna 70 och 71 i budgetförordningen

☐ offentligrättsliga organ

☐ privaträttsliga organ som har anförtrotts offentliga förvaltningsuppgifter i den utsträckning som de lämnar tillräckliga ekonomiska garantier

☐ organ som omfattas av privaträtten i en medlemsstat, som anförtrotts genomförandeuppgifter inom ramen för ett offentlig-privat partnerskap och som lämnar tillräckliga ekonomiska garantier

☐ personer som anförtrotts genomförandet av särskilda åtgärder inom Gusp enligt avdelning V i fördraget om Europeiska unionen och som fastställs i den relevanta grundläggande rättsakten.

Vid fler än en metod, ange kompletterande uppgifter under ”Anmärkningar”.

Kommentarer

Direkt förvaltning kommer i första hand att omfatta administrativa utgifter för GD Migration och inrikes frågor, administrativt arrangemang med JRC, bidrag som förvaltas av kommissionen.

[41] Närmare förklaringar av de olika metoderna för genomförande med hänvisningar till respektive bestämmelser i budgetförordningen återfinns på BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

Delad förvaltning kommer att omfatta projekt under delad förvaltning: medlemsstaterna kommer att behöva utveckla en strategi och riskbedömning och får använda sina nationella anslag för de ändamålen.

2. FÖRVALTNING

2.1. Regler om uppföljning och rapportering

Ange intervall och andra villkor för sådana åtgärder:

Enligt förslaget till Europaparlamentets och rådets förordning om att inrätta ett särskilt unionsinstrument för säkerhetsområdet inom ramen för Fonden för inre säkerhet (COM(2018) 472 final):

Delad förvaltning:

Varje medlemsstat ska inrätta ett förvaltnings- och kontrollsystem för programmet och säkerställa kvaliteten och tillförlitligheten i övervakningssystemet och uppgifterna om indikatorer, i enlighet med förordningen om gemensamma bestämmelser. För att göra det lättare att snabbt inleda genomförandet är det möjligt att förlänga befintliga välfungerande förvaltnings- och kontrollsystem till nästa programperiod.

I detta sammanhang kommer medlemsstaterna att ombes inrätta en övervakningskommitté som kommissionen ska delta i som rådgivare. Övervakningskommittén ska sammanträda minst en gång om året. Den ska granska alla frågor som påverkar programmets förmåga att förverkliga programmålen.

Medlemsstaterna kommer att sända en årlig prestationsrapport, som bör innehålla information om de framsteg som görs för att genomföra programmet och uppnå dess delmål och mål. Rapporten bör även ta upp eventuella problem som påverkar prestationerna inom programmet och de åtgärder som vidtagits för att lösa dem.

I slutet av perioden ska varje medlemsstat lämna in en slutlig resultatrapport. Slutrapporten bör inriktas på de framsteg som gjorts med att förverkliga programmålen och bör ge en översikt över de viktigaste faktorer som påverkat programprestationerna, de åtgärder som vidtagits för att ta itu med dessa faktorer och en bedömning av hur effektiva dessa åtgärder har varit. Dessutom bör den beskriva hur programmet har bidragit till att avhjälpa de brister som konstaterats i relevanta EU-rekommendationer till medlemsstaten, de framsteg som gjorts för att uppnå de mål som anges i prestationsramen, iakttagelserna från de relevanta utvärderingarna, uppföljningen av dessa iakttagelser och resultaten av kommunikationsåtgärderna.

Enligt förslaget till förordning om gemensamma bestämmelser ska medlemsstaterna årligen översända ett garantipaket som inbegriper årsredovisning, förvaltningsförklaring och revisionsmyndighetens yttrande om förvaltnings- och kontrollsystemet, den årliga kontrollrapporten enligt artikel 92.1 d i förordningen om gemensamma bestämmelser samt om lagligheten och korrektheten i de utgifter som deklarerats i årsräkenskaperna. Detta garantipaket kommer att användas av kommissionen för att fastställa det belopp som ska belasta fonden för räkenskapsåret.

Ett översynsmöte ska anordnas mellan kommissionen och varje medlemsstat vartannat år för att granska resultatet av varje program.

Sex gånger om året sänder medlemsstaterna uppgifter för varje program, indelat enligt särskilda mål. Dessa uppgifter avser kostnaderna för insatser och värdet av gemensamma output- och resultatindikatorer.

Som allmän regel:

Kommissionen ska göra en utvärdering efter halva tiden och en efterhandsutvärdering av de åtgärder som genomförts inom ramen för denna fond, i linje med förordningen om gemensamma bestämmelser. Halvtidsutvärderingen bör framför allt grundas på halvtidsutvärderingen av program som medlemsstaterna lämnat in till kommissionen senast den 31 december 2024.

2.2. Förvaltnings- och kontrollsystem

2.2.1. Motivering av den genomförandemetod, de finansieringsmekanismer, de betalningsvillkor och den kontrollstrategi som föreslås

Enligt förslaget till Europaparlamentets och rådets förordning om att inrätta ett särskilt unionsinstrument för säkerhetsområdet inom ramen för Fonden för inre säkerhet (COM(2018) 472 final):

Både efterhandsutvärderingarna av de fonder som lydde under GD Migration och inrikes frågor 2007–2013 och halvtidsutvärderingarna av generaldirektoratets befintliga fonder visar att en kombination av olika genomförandemodeller på området migration och inrikes frågor har gjort det möjligt att på ett effektivt sätt uppnå fondernas mål. Den övergripande utformningen av genomförandemodellerna bibehålls och omfattar delad, direkt och indirekt förvaltning.

Genom delad förvaltning genomför medlemsstaterna program som bidrar till unionens politiska mål på ett sätt som är skräddarsytt till deras nationella förhållanden. Delad förvaltning säkerställer att ekonomiskt stöd finns tillgängligt i alla deltagande stater. Delad förvaltning möjliggör dessutom förutsebar finansiering och ger medlemsstaterna, som bäst känner till de utmaningar de står inför, möjlighet att planera sin långsiktiga finansiering i enlighet med detta. En nyhet är att fonden också kan utnyttjas för bistånd i nödsituationer genom delad förvaltning, utöver direkt och indirekt förvaltning.

Genom direkt förvaltning stöder kommissionen andra åtgärder som bidrar till unionens gemensamma politiska mål. Åtgärderna gör det möjligt att vidta skräddarsydda åtgärder till stöd för akuta och särskilda behov i enskilda medlemsstater (”bistånd i nödsituationer”), stödja transnationella nätverk och verksamhet, testa innovativ verksamhet som kan utökas inom ramen för nationella program och utföra studier av intresse för unionen som helhet (”unionsåtgärder”).

Genom indirekt förvaltning bibehåller fonden möjligheten att för särskilda åtgärder delegera budgetgenomförande till bl.a. internationella organisationer och organ på området inrikes frågor.

Med tanke på de olika målen och behoven föreslås en tematisk del inom ramen för fonden, som ett sätt att balansera förutsägbarheten för den fleråriga tilldelningen av finansiering till de nationella programmen med flexibilitet när det gäller att periodvis betala ut medel till åtgärder med högt mervärde för unionen. Den tematiska delen kommer att användas för särskilda åtgärder inom och bland medlemsstaterna, unionsåtgärder, bistånd i nödsituationer. Den kommer att säkerställa att medel kan tilldelas och överföras mellan de olika förvaltningsformerna, på grundval av en tvåårig programplaneringscykel.

Betalningsvillkoren för delad förvaltning beskrivs i förslaget till förordning om gemensamma bestämmelser, som förutskickar en årlig förfinansiering, följd av maximalt fyra mellanliggande betalningar per program och år, med utgångspunkt i de ansökningar om utbetalning som skickats in av medlemsstaterna under

räkenskapsåret. Enligt förslaget till förslag till förordning om gemensamma bestämmelser avräknas förhandsfinansieringen inom programmens sista räkenskapsår.

Kontrollstrategin kommer att bygga på den nya budgetförordningen och förordningen om gemensamma bestämmelser. Den nya budgetförordningen och förslaget till förordning om gemensamma bestämmelser bör utvidga användningen av förenklade former av bidrag, såsom klumpsummor, schablonbelopp och enhetskostnader. I förordningarna införs också nya former av betalningar, som bygger på de resultat som uppnåtts, snarare än kostnaderna. Stödmottagarna kommer att kunna motta ett fast belopp om de styrker att viss verksamhet, såsom utbildning eller tillhandahållande av humanitärt bistånd, har ägt rum. Detta förväntas förenkla kontrollbördan både för stödmottagarna och medlemsstaterna (t.ex. kontroll av fakturor och kvitton för kostnaderna).

När det gäller delad förvaltning bygger förslaget till förordning om gemensamma bestämmelser på förvaltnings- och kontrollstrategin för programplaneringsperioden 2014–2020, men några åtgärder införs i syfte att förenkla genomförandet och minska kontrollbördan för både stödmottagare och medlemsstater. Följande nya aspekter ingår:

– Avskaffande av utseendeförfarandet (vilket torde göra det möjligt att påskynda genomförandet av programmen).

– Förvaltningskontroller (administrativa kontroller och kontroller på plats) som ska utföras av den förvaltande myndigheten på grundval av riskbedömningar (jämfört med 100 % administrativa kontroller som krävs under programperioden 2014–2020).
– Dessutom får de förvaltande myndigheterna, under vissa villkor, tillämpa proportionella kontrollstrategier i linje med nationella förfaranden.

– Villkor för att undvika flera olika revisioner av samma insats/utgift.

Programmyndigheterna kommer att lämna in ansökningar om mellanliggande betalningar till kommissionen på grundval av stödmottagarnas utgifter. Enligt förslaget till förordning om gemensamma bestämmelser ska de förvaltande myndigheterna få rätt att utföra förvaltningskontrollerna på grundval av riskbedömningar men också särskilda kontroller (t.ex. kontroller på plats av den förvaltande myndigheten och revisioner av insatser /utgifter av revisionsmyndigheten) efter att utgifterna har deklarerats till kommissionen i ansökningarna om mellanliggande betalningar. För att minska risken för att ersättning utgår till icke stödberättigande utgifter, fastställs i förslaget till förordning om gemensamma bestämmelser att kommissionens mellanliggande betalningar ska begränsas till högst 90 %, med tanke på att bara vissa nationella kontroller för närvarande har utförts. Kommissionen kommer att betala det återstående saldot efter det årliga avslutandet av räkenskaperna, efter mottagande av garantipaketet från programmyndigheterna. Eventuella oriktigheter som kommissionen eller revisionsrätten upptäcker efter det att det årliga garantipaketet har översänts kan leda till en finansiell nettokorrigering.

För den del som genomförs genom **direkt och indirekt förvaltning** inom ramen för den tematiska delen kommer förvaltnings- och kontrollsystemet att bygga på erfarenheterna från både unionsåtgärder och bistånd i nödsituationer under 2014–2020. Ett förenklat system kommer att införas som möjliggör snabb behandling av ansökningar om finansiering samtidigt som risken för fel minskas: endast

medlemsstater och internationella organisationer är berättigade att ansöka om stöd, finansieringen kommer att baseras på förenklade kostnadsalternativ, standardmallar kommer att utarbetas för finansieringsansökningar, bidragsavtal/överenskommelser om medverkan och rapportering, och en ständig utvärderingskommitté kommer att granska ansökningarna så snart de tas emot.

2.2.2. Uppgifter om identifierade risker och om det eller de interna kontrollsystem som inrättats för att begränsa riskerna

GD Migration och inrikes frågor inte har stött på betydande risker för fel i sina utgiftsprogram. Detta bekräftas genom att revisionsrätten vid upprepade tillfällen inte haft några betydande brister att ta upp i sina årsrapporter.

Vid delad förvaltning rör de allmänna riskerna i samband med genomförandet av de nuvarande programmen underutnyttjande av fonden av medlemsstaterna och möjliga fel som beror på komplicerade regler och brister i förvaltnings- och kontrollsystemen. Genom förslaget till förordning om gemensamma bestämmelser skulle regelverket förenklas genom en harmonisering av reglerna och förvaltnings- och kontrollsystemen i de olika fonderna med delad förvaltning. Det innebär också en förenkling av kontrollkraven (t.ex. riskbaserade förvaltningskontroller, möjlighet till proportionella kontrollarrangemang som grundar sig på nationella förfaranden samt begränsningar av revisionsarbetet i fråga om tidpunkt och/eller särskilda insatser).

2.2.3. Beräkning och motivering av kontrollernas kostnadseffektivitet (dvs. förhållandet mellan kostnaden för kontrollerna och värdet av de medel som förvaltas) och en bedömning av den förväntade risken för fel (vid betalning och vid avslutande)

Det är kommissionen som ska rapportera om förhållandet mellan kostnaderna för kontroller jämfört med värdet av de förvaltade medlen. I den årliga verksamhetsrapporten för GD Migration och inrikes frågor 2019 anges 0,72 % för detta förhållande i fråga om delad förvaltning, 1,31 % för bidrag i direkt förvaltning och 6,05 % för upphandling i direkt förvaltning. När det gäller delad förvaltning förväntas denna procentandel minska tack vare effektivitetsvinster i genomförandet av programmen och ökade utbetalningar till medlemsstaterna.

Med det riskbaserade tillvägagångssättet avseende förvaltning och kontroll som införs i förslaget till förordning om gemensamma bestämmelser, i kombination med en ökad satsning på att anta förenklade kostnadsalternativ, förväntas medlemsstaternas kostnader för kontrollerna att sjunka ytterligare.

I den årliga verksamhetsrapporten för 2019 rapporterades en sammanlagd kvarstående felprocent på 1,57 % för nationella program för asyl-, migrations- och integrationsfonden (Amif)/Fonden för inre säkerhet (ISF) och en sammanlagd kvarstående felprocent på 4,11 % för icke forskningsrelaterade bidrag i direkt förvaltning.

2.3. Åtgärder för att förebygga bedrägeri och oriktigheter

Beskriv förebyggande åtgärder (befintliga eller planerade), t.ex. från strategi för bedrägeribekämpning.

GD Migration och inrikes frågor kommer även fortsättningsvis att tillämpa sin strategi mot bedrägerier i linje med kommissionens strategi mot bedrägerier för att bl.a. säkerställa att dess interna bedrägerikontroller helt överensstämmer med

kommissionens strategi och att dess metod för hantering av risken för bedrägeri är anpassad för att fastställa områden med bedrägeririsk och lämpliga motåtgärder.

När det gäller delad förvaltning ska medlemsstaterna säkerställa lagligheten och regelbundenheten hos utgifter som ingår i de räkenskaper som lämnats till kommissionen. I detta sammanhang ska medlemsstaterna vidta alla åtgärder som krävs för att förebygga, upptäcka och korrigera oriktigheter. Liksom i den nuvarande programplaneringscykeln 2014–2020 är medlemsstaterna skyldiga att införa förfaranden för upptäckt av oriktigheter och bedrägeribekämpning i samband med kommissionens särskilda delegerade förordning om rapportering av oriktigheter. Åtgärder för att förebygga bedrägeri förblir en övergripande princip och skyldighet för medlemsstaterna.

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

(1) Ny budgetrubrik:

Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd.

Rubrik i den fleråriga budgetramen	Budgetrubrik	Type of anslag	Bidrag			
	Rubrik nr 5: Resiliens, säkerhet och försvar	Diff./Icke-diff.[42]	från Efta-länder[43]	från kandidat-länder[44]	från tredje-länder	enligt artikel 21.2 b i budgetförordningen
5	12.02.01 – Fonden för inre säkerhet	Diff.	NEJ	NEJ	JA	NEJ
5	12 01 01 – Stödutgifter för Fonden för inre säkerhet	Icke-diff.	NEJ	NEJ	JA	NEJ

Anmärkning:

Det bör noteras att de driftsanslag som begärs inom ramen för förslaget täcks av anslag som redan tagits upp i finansieringsöversikten för förordningen om instrumentet för gränsförvaltning och visering.

Ytterligare personalresurser begärs inom ramen för detta lagstiftningsförslag.

[42] Diff.= differentierade anslag / Icke-diff. = icke-differentierade anslag.

[43] Efta: Europeiska frihandelssammanslutningen.

[44] Kandidatländer och i förekommande fall potentiella kandidatländer i västra Balkan.

3.2. Förslagets beräknade budgetkonsekvenser på anslagen

3.2.1. Sammanfattning av beräknad inverkan på driftsanslagen

☐ Förslaget/initiativet kräver inte att driftsanslag tas i anspråk

☑Förslaget/initiativet kräver att driftsanslag tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

Rubrik i den fleråriga budget-ramen	5	Resiliens, säkerhet och försvar

GD: Migration och inrikes frågor			2021	2022	2023	2024	2025	2026	2027	**Efter 2027**	**TOTALT**
• Driftsanslag											
Budgetrubrik 12 02 01 – Fonden för inre säkerhet	Åtaganden	(1a)	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Betalningar	(2a)	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822
Anslag av administrativ natur som finansieras genom ramanslagen för särskilda program[45]											
Budgetrubrik		(3)									
TOTALA anslag för GD Migration och inrikes frågor	Åtaganden	=1a+1b +3	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Betalningar	=2a+2b +3	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822

[45] Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

• TOTALA driftsanslag	Åtaganden	(4)									
	Betalningar	(5)									
• TOTALA anslag av administrativ natur som finansieras genom ramanslagen för särskilda program		(6)									
TOTALA anslag för RUBRIK 5 i den fleråriga budgetramen	Åtaganden	=4+ 6	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Betalningar	=5+ 6	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822

Upprepa avsnittet ovan om flera rubriker avseende driftsanslag i budgetramen påverkas av förslaget eller initiativet:

• TOTALA driftsanslag (alla rubriker avseende driftsanslag)	Åtaganden	(4)									
	Betalningar	(5)									
TOTALA anslag av administrativ natur som finansieras genom ramanslagen för särskilda program (alla driftsrelaterade rubriker)		(6)									
TOTALA anslag för RUBRIKERNA 1–6 i den fleråriga budgetramen (referensbelopp)	Åtaganden	=4+ 6	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Betalningar	=5+ 6	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822

Rubrik i den fleråriga budget-ramen	**7**	”Administrativa utgifter”

Detta avsnitt ska fyllas i med hjälp av det datablad för budgetuppgifter av administrativ natur som först ska föras in i bilagan till finansieringsöversikt för rättsakt (bilaga V till de interna bestämmelserna), vilken ska laddas upp i DECIDE som underlag för samråden mellan kommissionens avdelningar.

Miljoner euro (avrundat till tre decimaler)

		2021	2022	2023	2024	2025	2026	2027	**TOTALT**
GD: Migration och inrikes frågor									
• Personalresurser		0,152	0,228	0,499	0,813	0,932	0,932	0,932	**4,488**
• Övriga administrativa utgifter		0,033	0,085	0,109	0,109	0,109	0,109	0,109	**0,663**
GD MIGRATION OCH INRIKES FRÅGOR **TOTALT**	Anslag	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,151**

TOTALA anslag för RUBRIK 7 i den fleråriga budgetramen	(summa åtaganden = summa betalningar)	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,151**

Miljoner euro (avrundat till tre decimaler)

		2021	2022	2023	2024	2025	2026	2027	**Efter 2027**	**TOTALT**
TOTALA anslag för RUBRIKERNA 1–7 i den fleråriga budgetramen	Åtaganden	**0,309**	**4,661**	**6,178**	**7,642**	**8,061**	**8,061**	**8,061**	**–**	**42,973**
	Betalningar	**0,725**	**4,636**	**5,965**	**6,325**	**6,444**	**6,444**	**6,444**	**5,989**	**42,973**

3.2.2. *Beräknad output som finansieras med driftsanslag*

Åtagandebemyndiganden i miljoner euro (avrundat till tre decimaler)

Indicate objectives and outputs			Year **2021**		Year **2022**		Year **2023**		Year **2024**		Year **2025**		Year **2026**		Year **2027**		TOTAL	
⇩	Type	Average cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost
SPECIFIC OBJECTIVE NO 1: Commission support to competent authorities and critical entities																		
Output	Developing and maintaining the knowledge and support capacity					2.000		2.000		2.000		2.000		2.000		2.000		12.000
Output	Support to competent authorities by fostering the exchange of best practices and information and by carrying out risk assessments (The financial costs covered by studies below)					-												
Output	Support to competent authorities and critical entities (i.e. operators) by developing guidance materials and methodologies, supporting the organisation of exercises simulating real-time incident scenarios, providing training					0.500		0.850		1.200		1.500		1.500		1.500		7.050
Output	Projects on various topics related to support activities mentioned above (risk assessment methodologies, simulations of real-time incident scenarios, trainings…)	0.400			3	1.200	5	2.000	7	2.800	7	2.800	7	2.800	7	2.800	36	14.400
Output	Studies (risk assessments) and consultations (related to implementation of the Directive)	0.100			4	0.400	4	0.400	4	0.400	4	0.400	4	0.400	4	0.400	24	2.400
Output	Other meetings, conference	0.031	4	0.124	8	0.248	8	0.248	8	0.248	8	0.248	8	0.248	8	0.248	52	1.612
Subtotal for specific objective N°1				0.124		4.348		5.498		6.648		6.948		6.948		6.948		37.462
SPECIFIC OBJECTIVE NO 2: Resilience Advisory teams																		
- Output	Organisation of Resilience advisory teams (Members: Member States representatives). COM to organise call for members (for MS participants)																	-
- Output	COM to organise the programme and advisory missions COM to provide substantial input to advisory missions (guidance and oversight of Critical entities of European significance – together with MS) Day-to-day coordination of Resilience advisory teams							0.072		0.072		0.072		0.072		0.072		0.360
Subtotal for specific objective N°2								0.072		0.072		0.072		0.072		0.072		0.360
TOTAL for objectives 1 to 2				**0.124**		**4.348**		**5.570**		**6.720**		**7.020**		**7.020**		**7.020**		**37.822**

3.2.3. Sammanfattning av beräknad inverkan på de administrativa anslagen

☐ Förslaget/initiativet kräver inte att anslag av administrativ natur tas i anspråk

☑ Förslaget/initiativet kräver att anslag av administrativ natur tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

	2021	2022	2023	2024	2025	2026	2027	TOTALT
HEADING 7 i den fleråriga budgetramen								
Personalresurser	0,152	0,228	0,499	0,813	0,932	0,932	0,932	4,488
Övriga administrativa utgifter	0,033	0,085	0,109	0,109	0,109	0,109	0,109	0,663
Subtotal HEADING 7 i den fleråriga budgetramen	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,188**

Belopp utanför RUBRIK 7[46] i den fleråriga budgetramen								
Personalresurser								
Other expenditure av administrativ natur								
Subtotal utanför RUBRIK 7 of the multiannual financial framework								

TOTALT	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,188**

Personalbehov och andra administrativa kostnader ska täckas genom anslag inom generaldirektoratet vilka redan har avdelats för förvaltningen av åtgärden i fråga, eller genom en omfördelning av anslag inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

[46] Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

3.2.3.1. Beräknat personalbehov

☐ Förslaget/initiativet kräver inte att personalresurser tas i anspråk.

☑ Förslaget/initiativet kräver att personalresurser tas i anspråk enligt följande:

Beräkningarna ska anges i heltidsekvivalenter

		Year **2021**	Year **2022**	År **2023**	År **2024**	2025	2026	2027
• Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)								
20 01 02 01 (Vid huvudkontoret eller vid kommissionens kontor i medlemsstaterna)		1	2	4	5	5	5	5
XX 01 01 02 (vid delegationer)								
XX 01 05 01/11/21 (indirekta forskningsåtgärder)								
10 01 05 01/11 (direkta forskningsåtgärder)								
• Extern personal (i heltidsekvivalenter:)[47]								
20 02 01 03 (kontraktsanställda, nationella experter och vikarier finansierade genom ramanslaget)				1	2	2	2	2
XX 01 02 02 (kontraktsanställda, lokalanställda, nationella experter, vikarier och unga experter som tjänstgör vid delegationerna)								
XX 01 04 **yy**[48]	– vid huvudkontoret							
	– vid delegationer							
XX 01 05 02/12/22 (kontraktsanställda, nationella experter och vikarier som arbetar med indirekta forskningsåtgärder)								
10 01 05 02/12 (kontraktsanställda, vikarier och nationella experter som arbetar med direkta forskningsåtgärder)								
Annan budgetrubrik (ange vilken)								
TOTALT		**1**	**2**	**5**	**7**	**7**	**7**	**7**

XX motsvarar det politikområde eller den avdelning i budgeten som avses.

Personalbehoven ska täckas med personal inom generaldirektoratet vilka redan har avdelats för förvaltningen av åtgärden i fråga, eller genom en omfördelning av personal inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

Beskrivning av arbetsuppgifter:

Tjänstemän och tillfälligt anställda	Förslaget utgår från 4 handläggare och 1 assistent AST som arbetar med genomförandet av direktivet från kommissionens sida, varav 1 handläggare redan finns internt och de återstående heltidsekvivalenterna utgörs av ytterligare personalresurser som ska rekryteras. Rekryteringsplan: 2022: +1 handläggare: en handläggare med ansvar för att bygga upp kunskapskapacitet och stödverksamhet 2023: +1 handläggare (med ansvar för de rådgivande grupperna), 1 assistent (assistent för grupperna för rådgivning om motståndskraft) 2024: +1 handläggare (som bidrar till stödinsatserna för myndigheter och operatörer)
Extern personal	Förslaget utgår från 2 nationella experter som arbetar med genomförandet av direktivet från kommissionens sida. Rekryteringsplan:

[47] [Denna fotnot förklarar vissa initialförkortningar som inte används i den svenska versionen].

[48] Särskilt tak för finansiering av extern personal genom driftsanslag (tidigare s.k. BA-poster).

	2023: + 1 kontraktsanställd (expert på motståndskraft hos kritisk infastruktur/bidrar till stödinsatser för myndigheter och operatörer). 2024: + 1 kontraktsanställd (expert på motståndskraft hos kritisk infastruktur/bidrar till stödinsatser för myndigheter och operatörer).

3.2.4. Förenlighet med den gällande fleråriga budgetramen

Förslaget/initiativet

☑ kan finansieras fullständigt genom omfördelningar inom den berörda rubriken i den fleråriga budgetramen.

Driftsutgifter som täcks av fonden för inre säkerhet i den fleråriga budgetplanen 2021–2027

☐ kräver användning av den outnyttjade marginalen under den relevanta rubriken i den fleråriga budgetramen och/eller användning av de särskilda instrument enligt definitionen i förordningen om den fleråriga budgetramen.

Beskriv vad som krävs, ange berörda rubriker och budgetrubriker, motsvarande belopp och de instrument som är föreslagna för användning.

☐ kräver en översyn av den fleråriga budgetramen.

Beskriv behovet av sådana åtgärder, och ange berörda rubriker i budgetramen, budgetrubriker i den årliga budgeten samt de motsvarande beloppen.

3.2.5. Bidrag från tredje part

Förslaget/initiativet

☑ innehåller inga bestämmelser om medfinansiering från tredje parter

☐ innehåller bestämmelser om medfinansiering från tredje parter enligt följande uppskattning:

Anslag i miljoner euro (avrundat till tre decimaler)

	Year **N**[49]	Year **N+1**	Year **N+2**	Year **N+3**	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)			Totalt
Ange vilket organ som deltar i medfinansieringen								
TOTALA anslag som tillförs genom medfinansiering								

[49] Med år n avses det år då förslaget eller initiativet ska börja genomföras. Ersätt ”n” med det förväntade första genomförandeåret (till exempel 2021). Detsamma för följande år.

3.3. Beräknad inverkan på inkomsterna

☑ Förslaget/initiativet påverkar inte budgetens inkomstsida.

☐ Förslaget/initiativet påverkar inkomsterna på följande sätt:

☐ Påverkan på egna medel

☐ Påverkan på andra inkomster

ange om inkomsterna har avsatts för utgiftsposter ☐

Miljoner euro (avrundat till tre decimaler)

Budgetrubrik i den årliga budgetens inkomstdel:	Belopp som förts in för det innevarande budgetåret	Förslagets/initiativets inverkan på inkomsterna[50]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)		
Artikel …….								

För inkomster avsatta för särskilda ändamål, ange vilka budgetrubriker i utgiftsdelen som berörs.

[…]

Övriga anmärkningar (t.ex. vilken metod/formel som har använts för att beräkna inverkan på inkomsterna eller andra relevanta uppgifter).

[…]

[50] Vad gäller traditionella egna medel (tullar, sockeravgifter) ska nettobeloppen anges, dvs. bruttobeloppen minus 20 % avdrag för uppbördskostnader.