Rada
Európskej únie

V Bruseli 18. decembra 2020
(OR. en)

14262/20

Medziinštitucionálny spis:
2020/0365(COD)

PROCIV 105	**ECOFIN 1182**
JAI 1132	**ENV 832**
COSI 258	**SAN 490**
ENFOPOL 354	**CHIMIE 69**
CT 121	**RECH 539**
COTER 120	**DENLEG 90**
ENER 512	**RELEX 1037**
TRANS 621	**HYBRID 49**
TELECOM 277	**CYBER 283**
ATO 91	**ESPACE 85**

SPRIEVODNÁ POZNÁMKA

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	16. decembra 2020
Komu:	Jeppe TRANHOLM-MIKKELSEN, generálny tajomník Rady Európskej únie
Č. dok. Kom.:	COM(2020) 829 final
Predmet:	Návrh SMERNICE EURÓPSKEHO PARLAMENTU A RADY o odolnosti kritických subjektov

Delegáciám v prílohe zasielame dokument COM(2020) 829 final.

Príloha: COM(2020) 829 final

EURÓPSKA
KOMISIA

V Bruseli 16. 12. 2020
COM(2020) 829 final

2020/0365 (COD)

Návrh

SMERNICA EURÓPSKEHO PARLAMENTU A RADY

o odolnosti kritických subjektov

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

DÔVODOVÁ SPRÁVA

1. KONTEXT NÁVRHU

• Dôvody a ciele návrhu

Európska únia musí v záujme účinnej ochrany Európanov naďalej zmierňovať zraniteľnosť, a to aj pokiaľ ide o kritické infraštruktúry, ktoré sú nevyhnutné pre fungovanie našich spoločností a hospodárstva. Životytie európskych občanov a dobré fungovanie vnútorného trhu závisia od rôznych infraštruktúr, ktorých úlohou je spoľahlivé poskytovanie služieb nevyhnutných na zachovanie kritických spoločenských a hospodárskych činností. Tieto služby, ktoré sú za bežných okolností životne dôležité, sú o to dôležitejšie, že Európa sa snaží zvládnuť účinky pandémie COVID-19 a usiluje sa o to, aby sa z nej zotavila. Z toho vyplýva, že subjekty poskytujúce základné služby musia byť odolné, t. j. musia byť schopné odolávať incidentom, ktoré môžu viesť k vážnym, prípadne medziodvetvovým a cezhraničným narušeniam, absorbovať ich, prispôsobiť sa im a zotaviť sa z nich.

Cieľom tohto návrhu je posilniť poskytovanie služieb na vnútornom trhu, ktoré sú nevyhnutné na zachovanie životne dôležitých spoločenských funkcií alebo hospodárskych činností, a to zvýšením odolnosti kritických subjektov, ktoré takéto služby poskytujú. Návrh je odpoveďou na nedávne výzvy na prijatie opatrení, ktoré vyjadrili Rada[1] a Európsky parlament[2], ktorí vyzvali Komisiu k tomu, aby prehodnotila súčasný prístup s cieľom lepšie zohľadniť rastúce výzvy pre kritické subjekty a zabezpečiť užší súlad so smernicou o sieťovej a informačnej bezpečnosti (ďalej len „smernica NIS“)[3]. Tento návrh je v súlade a vytvára úzke synergie s navrhovanou smernicou o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (ďalej len „smernica o kybernetickej bezpečnosti“), ktorá nahradí smernicu NIS s cieľom riešiť zvýšenú prepojenosť fyzického a digitálneho sveta prostredníctvom legislatívneho rámca so spoľahlivými opatreniami na zabezpečenie odolnosti, pokiaľ ide o kybernetické aj fyzické aspekty, ako sa stanovuje v Stratégii EÚ pre bezpečnostnú úniu[4].

Návrh okrem toho odzrkadľuje vnútroštátne prístupy v čoraz väčšom počte členských štátov, ktoré majú tendenciu klásť dôraz na vzájomnú závislosť naprieč odvetviami a hranicami a čoraz viac sa zaoberajú úvahami o odolnosti, v rámci ktorých je ochrana len jedným prvkom popri predchádzaní rizikám a ich zmierňovaní, kontinuite činností a obnove. Vzhľadom na to, že kritickým infraštruktúram hrozí riziko, že by sa mohli stať aj teroristickými cieľmi, opatrenia zamerané na zabezpečenie odolnosti kritických subjektov uvedené v tomto návrhu prispievajú k cieľom nedávno prijatého programu EÚ na boj proti terorizmu[5].

---

1 Závery Rady z 10. decembra 2019 o komplementárnom úsilí zameranom na zvyšovanie odolnosti a boj proti hybridným hrozbám (14972/19).

2 Správa o zisteniach a odporúčaniach Osobitného výboru Európskeho parlamentu pre terorizmus [2018/2044(INI)].

3 Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.

4 COM(2020) 605.

5 COM(2020) 795.

Európska únia už dlho uznáva celoeurópsky význam kritických infraštruktúr. Európska únia napríklad v roku 2006 zriadila Európsky program na ochranu kritickej infraštruktúry (EPCIP)[6] a v roku 2008 prijala smernicu o európskej kritickej infraštruktúre (ďalej len „smernica ECI“)[7]. V smernici ECI, ktorá sa vzťahuje len na odvetvia energetiky a dopravy, sa stanovuje postup na identifikáciu a označovanie európskych kritických infraštruktúr, ktorých narušenie alebo zničenie by malo závažné cezhraničné dôsledky minimálne v dvoch členských štátoch. Takisto sa v nej stanovujú osobitné požiadavky na ochranu pre prevádzkovateľov európskych kritických infraštruktúr a príslušné orgány členských štátov. K dnešnému dňu bolo označených 94 európskych kritických infraštruktúr, z ktorých dve tretiny sa nachádzajú v troch členských štátoch strednej a východnej Európy. Rozsah opatrení Európskej únie v oblasti odolnosti kritickej infraštruktúry však presahuje rámec týchto opatrení a zahŕňa odvetvové a medziodvetvové opatrenia, ktoré sa okrem iného týkajú zvýšenia odolnosti proti zmene klímy, civilnej ochrany, priamych zahraničných investícií a kybernetickej bezpečnosti[8]. Samotné členské štáty medzitým prijali v tejto oblasti vlastné opatrenia, ktoré sa navzájom líšia.

Je preto zrejmé, že v súčasnosti platný rámec na ochranu kritickej infraštruktúry nepostačuje na riešenie súčasných výziev pre kritické infraštruktúry a subjekty, ktoré ich prevádzkujú. Vzhľadom na čoraz väčšiu prepojenosť infraštruktúr, sietí a prevádzkovateľov poskytujúcich základné služby na celom vnútornom trhu je nevyhnutné zásadne zmeniť súčasný prístup a prejsť od ochrany konkrétnych štruktúr k zvýšeniu odolnosti kritických subjektov, ktoré ich prevádzkujú.

Prevádzkové prostredie, v ktorom kritické subjekty pôsobia, sa v posledných rokoch výrazne zmenilo. Po prvé, rizikové prostredie je zložitejšie ako v roku 2008 a v súčasnosti zahŕňa aj prírodné nebezpečenstvá[9] (v mnohých prípadoch zhoršené zmenou klímy), štátom podporované hybridné akcie, terorizmus, vnútorné hrozby, pandémie a havárie (ako sú priemyselné havárie). Po druhé, prevádzkovatelia čelia výzvam pri integrácii nových technológií, ako napríklad 5G a bezpilotných vozidiel, do svojej prevádzky, a zároveň riešia slabé miesta, ktoré by takéto technológie mohli potenciálne vytvoriť. Po tretie, vďaka týmto technológiám a iným trendom sa prevádzkovatelia čoraz viac spoliehajú jeden na druhého. Dôsledky sú jasné – narušenie, ktoré ovplyvní poskytovanie služieb jedným prevádzkovateľom v jednom odvetví môže vyvolať kaskádové účinky na poskytovanie služieb v iných odvetviach a prípadne aj v iných členských štátoch alebo v celej Únii.

Ako vyplýva z hodnotenia smernice ECI z roku 2019[10], existujúce európske a vnútroštátne opatrenia čelia obmedzeniam, pokiaľ ide o pomoc prevádzkovateľom vysporiadať sa s operačnými výzvami, s ktorým sa v súčasnosti stretávajú, a zraniteľnosťami, ktoré so sebou prináša ich vzájomná závislosť.

---

6 Oznámenie Komisie o Európskom programe na ochranu kritickej infraštruktúry [KOM(2006) 786].

7 Smernica Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu.

8 Oznámenie Komisie s názvom Stratégia EÚ pre adaptáciu na zmenu klímy [COM(2013) 216], rozhodnutie Európskeho parlamentu a Rady č. 1313/2013/EÚ zo 17. decembra 2013 o mechanizme Únie v oblasti civilnej ochrany, nariadenie Európskeho parlamentu a Rady (EÚ) 2019/452, ktorým sa ustanovuje rámec na preverovanie priamych zahraničných investícií do Únie, smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.

9 Prehľad rizík prírodných katastrof a katastrof spôsobených ľudskou činnosťou, ktorým môže čeliť Európska únia [SWD(2020) 330].

10 SWD(2019) 308.

Dôvodov je niekoľko, ako sa uvádza v posúdení vplyvu, ktoré podporilo vypracovanie návrhu. Po prvé, prevádzkovatelia si nie sú plne vedomí dôsledkov meniaceho sa rizikového prostredia, v rámci ktorého pôsobia, alebo mu úplne nerozumejú. Po druhé, úsilie o zvýšenie odolnosti sa medzi členskými štátmi a odvetviami výrazne líši. Po tretie, podobné typy subjektov sú niektorými členskými štátmi uznávané za kritické, ale inými nie, čo znamená, že porovnateľným subjektom sa dostáva rôzna miera oficiálnej podpory v oblasti budovania kapacít (napr. vo forme usmernení, organizácie odbornej prípravy a výcviku) v závislosti od toho, kde v Únii pôsobia, a vzťahujú sa na ne rôzne požiadavky. Skutočnosť, že sa požiadavky a vládna podpora poskytovaná prevádzkovateľom v jednotlivých členských štátoch líšia, vytvára pre prevádzkovateľov prekážky pri cezhraničnom pôsobení, najmä pre tie kritické subjekty, ktoré pôsobia v členských štátoch s prísnejšími rámcami. Vzhľadom na čoraz prepojenejšiu povahu poskytovania služieb a väčšiu prepojenosť odvetví v členských štátoch a celej Európskej únii predstavuje nedostatočná úroveň odolnosti jedného prevádzkovateľa vážne riziko pre subjekty, ktoré pôsobia na inom mieste v rámci vnútorného trhu.

Okrem ohrozenia hladkého fungovania vnútorného trhu môžu mať narušenia, najmä tie, ktoré majú cezhraničné a prípadne celoeurópske dôsledky, vážny negatívny vplyv na občanov, podniky, vlády a životné prostredie. Na individuálnej úrovni môžu narušenia skutočne ovplyvniť schopnosť Európanov slobodne cestovať, pracovať a využívať základné verejné služby, ako je zdravotná starostlivosť. V mnohých prípadoch sú tieto a ďalšie základné služby, ktoré sú základom každodenného života, poskytované úzko prepojenými sieťami európskych podnikov a narušenie jedného podniku v jednom odvetví môže mať kaskádové účinky v mnohých ďalších hospodárskych odvetviach. Napokon, narušenia, ako sú napríklad rozsiahle výpadky energie a vážne dopravné nehody, môžu viesť k narušeniu všeobecnej a verejnej bezpečnosti, čo môže vyvolať neistotu a podkopať dôveru v kritické subjekty, ako aj v orgány zodpovedné za dohľad nad kritickými subjektmi a za zachovanie bezpečnosti a ochrany obyvateľstva.

- **Súlad s existujúcimi ustanoveniami v tejto oblasti politiky**

Tento návrh zohľadňuje priority Komisie, ktoré sú obsiahnuté v Stratégii EÚ pre bezpečnostnú úniu[11], v ktorej sa požaduje revidovaný prístup k odolnosti kritickej infraštruktúry, ktorý lepšie odráža súčasné a očakávané budúce rizikové prostredie, čoraz užšiu vzájomnú závislosť rôznych odvetví, ako aj čoraz viac vzájomne závislé vzťahy medzi fyzickými a digitálnymi infraštruktúrami.

Navrhovaná smernica nahrádza smernicu ECI a zároveň zohľadňuje iné existujúce a plánované nástroje a vychádza z nich. Navrhovaná smernica predstavuje podstatnú zmenu v porovnaní so smernicou ECI, ktorá sa vzťahuje len na odvetvia energetiky a dopravy, zameriava sa výlučne na ochranné opatrenia a stanovuje postup na identifikáciu a označovanie európskych kritických infraštruktúr prostredníctvom cezhraničného dialógu. V prvom rade by navrhovaná smernica mala mať oveľa širší rozsah pôsobnosti, ktorý by zahŕňal desať odvetví, a to energetiku, dopravu, bankovníctvo, infraštruktúru finančného trhu, zdravotníctvo, pitnú vodu, odpadovú vodu, digitálnu infraštruktúru, verejnú správu a vesmírny priestor. Po druhé, v smernici sa pre členské štáty stanovuje postup na identifikáciu kritických subjektov pomocou spoločných kritérií na základe vnútroštátneho

[11] Oznámenie Komisie o stratégii EÚ pre bezpečnostnú úniu [COM(2020) 605].

posúdenia rizík. Po tretie, v návrhu sa stanovujú povinnosti pre členské štáty a nimi identifikované kritické subjekty, vrátane tých, ktoré majú osobitný európsky význam, t. j. kritické subjekty, ktoré poskytujú základné služby do viac ako tretiny členských štátov, resp. vo viac ako tretine členských štátov a ktoré by podliehali osobitnému dohľadu.

V prípade potreby by Komisia poskytla príslušným orgánom a kritickým subjektom podporu pri plnení ich povinností vyplývajúcich z tejto smernice. Skupina pre odolnosť kritických subjektov, ktorá je expertnou skupinou Komisie podliehajúcou horizontálnemu rámcu vzťahujúcemu sa na takéto skupiny, by okrem toho poskytovala Komisii poradenstvo a podporovala by strategickú spoluprácu a výmenu informácií. Napokon, keďže vzájomná závislosť nekončí na vonkajších hraniciach Európskej únie, je potrebná aj spolupráca s partnerskými krajinami. V navrhovanej smernici sa stanovuje možnosť takejto spolupráce, napríklad v oblasti posudzovania rizík.

Súlad s ostatnými politikami Únie

Navrhovaná smernica má zjavné väzby a je v súlade s ostatnými odvetvovými a medziodvetvovými iniciatívami Európskej únie okrem iného v oblasti zvýšenia odolnosti proti zmene klímy, civilnej ochrany, priamych zahraničných investícií, kybernetickej bezpečnosti a *acquis* v oblasti finančných služieb. Návrh je predovšetkým v úzkom súlade a vytvára úzke synergie s navrhovanou smernicou o kybernetickej bezpečnosti, ktorej cieľom je zvýšiť odolnosť informačných a komunikačných technológií „kľúčových subjektov“ a „dôležitých subjektov“, ktoré spĺňajú konkrétne prahové hodnoty vo veľkom počte odvetví, proti všetkým nebezpečenstvám. Cieľom tohto návrhu smernice o odolnosti kritických subjektov je zabezpečiť, aby príslušné orgány určené podľa tejto smernice a orgány určené podľa navrhovanej smernice o kybernetickej bezpečnosti prijali doplnkové opatrenia a podľa potreby si vymieňali informácie, pokiaľ ide o kybernetickú a nekybernetickú odolnosť, a aby mimoriadne kritické subjekty v odvetviach, ktoré sa podľa navrhovanej smernice o kybernetickej bezpečnosti považujú za „kľúčové“, takisto podliehali povinnostiam súvisiacim so všeobecnejším zvyšovaním odolnosti s cieľom riešiť nekybernetické riziká. Fyzická bezpečnosť sietí a informačných systémov subjektov v odvetví digitálnej infraštruktúry sa komplexne rieši v navrhovanej smernici o kybernetickej bezpečnosti ako súčasť povinností týchto subjektov v oblasti riadenia kybernetických rizík a oznamovania. Návrh okrem toho vychádza z existujúceho *acquis* v oblasti finančných služieb, v ktorom sa stanovujú komplexné požiadavky na finančné subjekty, pokiaľ ide o riadenie prevádzkových rizík a zaistenie kontinuity činností. Preto by sa so subjektmi pôsobiacimi v odvetví digitálnej infraštruktúry, bankovníctva a finančnej infraštruktúry malo na účely povinností a činností členských štátov zaobchádzať ako so subjektmi, ktoré sú rovnocenné kritickým subjektom podľa tejto smernice, pričom z tejto smernice by pre tieto subjekty nevyplývali dodatočné povinnosti.

Návrh zohľadňuje aj ďalšie odvetvové a medziodvetvové iniciatívy týkajúce sa napr. civilnej ochrany, znižovania rizika katastrof a adaptácie na zmenu klímy. Okrem toho sa v návrhu uznáva, že existujúce právne predpisy Európskej únie ukladajú v niektorých prípadoch subjektom povinnosť riešiť určité riziká prostredníctvom ochranných opatrení. V takýchto prípadoch, napr. v oblasti leteckej alebo námornej bezpečnosti, by mali kritické subjekty opísať tieto opatrenia vo svojich plánoch odolnosti. Navyše, navrhovanou smernicou nie je dotknuté uplatňovanie pravidiel hospodárskej súťaže, ktoré sú stanovené v Zmluve o fungovaní Európskej únie (ZFEÚ).

2. PRÁVNY ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

- **Právny základ**

Na rozdiel od smernice 2008/114/ES, ktorá bola založená na článku 308 Zmluvy o založení Európskeho spoločenstva (zodpovedajúcom súčasnému článku 352 Zmluvy o fungovaní Európskej únie), sa tento návrh smernice zakladá na článku 114 ZFEÚ, ktorý zahŕňa aproximáciu práva na účely zlepšenia vnútorného trhu. Je to odôvodnené posunutím cieľa, rozsahu pôsobnosti a obsahu smernice, väčšou vzájomnou závislosťou a potrebou vytvoriť spravodlivejšie podmienky pre kritické subjekty. Namiesto ochrany obmedzeného súboru fyzických infraštruktúr, ktorých narušenie alebo zničenie by malo závažné cezhraničné dôsledky, je cieľom zvýšiť odolnosť subjektov v členských štátoch, ktoré sú kritické pre poskytovanie služieb nevyhnutných na zachovanie životne dôležitých spoločenských funkcií alebo hospodárskych činností na vnútornom trhu vo viacerých odvetviach, ktoré sú základom pre fungovanie mnohých ďalších odvetví hospodárstva Únie. Vzhľadom na zvýšenú cezhraničnú vzájomnú závislosť služieb poskytovaných prostredníctvom kritických infraštruktúr v týchto odvetviach môže mať narušenie v jednom členskom štáte dôsledky v iných členských štátoch alebo v Únii ako celku.

Súčasný právny rámec stanovený na úrovni členských štátov, ktorý upravuje predmetné služby, zahŕňa podstatne odlišné povinnosti, ktoré budú pravdepodobne narastať. Rozdielne vnútroštátne pravidlá, ktorým kritické subjekty podliehajú, nielenže ohrozujú spoľahlivé poskytovanie služieb na celom vnútornom trhu, ale takisto by mohli mať negatívny vplyv na hospodársku súťaž. Dôvodom je najmä skutočnosť, že podobné typy subjektov poskytujúcich podobné druhy služieb sa v niektorých členských štátoch považujú za kritické, ale v iných nie. To znamená, že subjekty, ktoré sú alebo chcú byť aktívne vo viac ako jednom členskom štáte, podliehajú v rámci pôsobenia na vnútornom trhu rozdielnym povinnostiam a subjekty pôsobiace v členských štátoch s prísnejšími požiadavkami môžu v porovnaní so subjektmi v členských štátoch s miernejšími rámcami čeliť prekážkam. Tieto rozdiely sú takého charakteru, že majú priamy negatívny vplyv na fungovanie vnútorného trhu.

- **Subsidiarita**

Spoločný právny rámec na európskej úrovni v tejto oblasti je odôvodnený vzájomnou závislou cezhraničnou povahou vzťahov medzi prevádzkami kritickej infraštruktúry a jej výstupmi, t. j. základnými službami. Operátor so sídlom v jednom členskom štáte môže v skutočnosti poskytovať služby vo viacerých iných členských štátoch alebo v celej Európskej únii prostredníctvom úzko prepojených sietí. Z toho vyplýva, že narušenie s vplyvom na tohto prevádzkovateľa, by mohlo mať ďalekosiahle následky v iných odvetviach a presahujúce vnútroštátne hranice. Potenciálne celoeurópske dôsledky narušení si vyžadujú prijímanie opatrení na úrovni Európskej únie. Rozdielne vnútroštátne pravidlá majú navyše priamy negatívny vplyv na fungovanie vnútorného trhu. Ako sa ukázalo v posúdení vplyvu, mnohé členské štáty a zainteresované strany z jednotlivých odvetví vidia potrebu jednotnejšieho a koordinovanejšieho európskeho prístupu zameraného na zabezpečenie toho, aby boli subjekty dostatočne odolné voči rôznym rizikám, ktoré sa síce v jednotlivých členských štátoch líšia, ale vytvárajú mnohé spoločné výzvy, ktoré nie je možné riešiť prostredníctvom vnútroštátnych opatrení alebo ktoré nemôžu riešiť jednotliví prevádzkovatelia samostatne.

- **Proporcionalita**

Návrh je vo vzťahu k stanovenému hlavnému cieľu iniciatívy primeraný. Zatiaľ čo povinnosti členských štátov a kritických subjektov môžu v určitých prípadoch viesť k ďalšej administratívnej záťaži, napr. ak členské štáty musia vypracovať národnú stratégiu alebo ak kritické subjekty musia zaviesť určité technické a organizačné opatrenia, očakáva sa, že budú celkovo obmedzené. V tejto súvislosti treba poznamenať, že mnohé subjekty už prijali určité bezpečnostné opatrenia na ochranu svojich infraštruktúr a zabezpečenie kontinuity činností.

V niektorých prípadoch si však dosiahnutie súladu so smernicou môže vyžadovať rozsiahlejšie investície. Aj v takýchto prípadoch sú však tieto investície odôvodnené tým, že by prispeli k zvýšeniu odolnosti na úrovni prevádzkovateľov a systému, ako aj k súdržnejšiemu prístupu a zvýšenej schopnosti poskytovať spoľahlivé služby v celej Únii. Okrem toho sa predpokladá, že akúkoľvek ďalšiu záťaž vyplývajúcu zo smernice by výrazne prevýšili náklady spojené s potrebou riadiť a prekonať vážne narušenia, ktoré ohrozujú nepretržité poskytovanie služieb súvisiacich so životne dôležitými spoločenskými funkciami a hospodárskou prosperitou prevádzkovateľov, jednotlivých členských štátov, Únie a jej občanov vo všeobecnosti.

- **Výber nástroja**

Návrh má podobu smernice, ktorej cieľom je zabezpečiť jednotnejší prístup k odolnosti kritických subjektov vo viacerých odvetviach v celej Únii. V návrhu sa stanovujú osobitné povinnosti pre príslušné orgány s cieľom identifikovať kritické subjekty na základe spoločných kritérií a výsledkov posúdenia rizík. Prostredníctvom smernice je možné zabezpečiť, aby členské štáty uplatňovali jednotný prístup pri identifikácii kritických subjektov a zároveň zohľadňovali osobitosti na vnútroštátnej úrovni vrátane rôznych úrovní vystavenia riziku a vzájomnej závislosti medzi odvetviami a krajinami.

3. VÝSLEDKY HODNOTENÍ *EX POST*, KONZULTÁCIÍ SO ZAINTERESOVANÝMI STRANAMI A POSÚDENÍ VPLYVU

- **Hodnotenia *ex post*/kontroly vhodnosti existujúcich právnych predpisov**

Smernica o európskej kritickej infraštruktúre bola v roku 2019 predmetom hodnotenia zameraného na posúdenie vykonávania smernice z hľadiska jej relevantnosti, súdržnosti, účinnosti, efektívnosti, pridanej hodnoty EÚ a udržateľnosti[12].

V hodnotení sa zistilo, že od nadobudnutia účinnosti smernice sa kontext výrazne zmenil. Vzhľadom na tieto zmeny sa zistilo, že smernica má len čiastočnú relevantnosť. Hoci sa v hodnotení ukázalo, že smernica je vo všeobecnosti v súlade s príslušnými európskymi odvetvovými právnymi predpismi a politikou na medzinárodnej úrovni, z dôvodu všeobecného charakteru niektorých jej ustanovení sa považovala len za čiastočne účinnú. Zistilo sa, že smernica priniesla pridanú hodnotu EÚ, keďže priniesla výsledky (t. j. spoločný rámec na ochranu európskych kritických infraštruktúr), ktoré by inak nebolo možné dosiahnuť ani vnútroštátnymi, ani inými európskymi iniciatívami bez toho, aby sa iniciovali oveľa dlhšie, nákladnejšie a menej dobre vymedzené procesy. Zároveň sa však zistilo, že niektoré ustanovenia mali pre mnohé členské štáty len obmedzenú pridanú hodnotu.

[12] SWD(2019) 310.

Pokiaľ ide o udržateľnosť, očakávalo sa, že určité účinky smernice (napr. cezhraničné diskusie, požiadavky na podávanie správ) zaniknú, ak sa smernica zruší a nenahradí. Z hodnotenia vyplynulo, že členské štáty naďalej podporujú zapojenie Európskej únie do úsilia o posilnenie odolnosti kritickej infraštruktúry a že existujú určité obavy, že úplné zrušenie smernice by mohlo mať v tejto oblasti negatívne účinky, a to najmä na ochranu označených európskych kritických infraštruktúr. Členské štáty sa usilovali o zaistenie toho, aby EÚ naďalej konala v tejto oblasti v súlade so zásadou subsidiarity, podporovala opatrenia na vnútroštátnej úrovni a uľahčovala cezhraničnú spoluprácu, a to aj s tretími krajinami.

- **Konzultácie so zainteresovanými stranami**

Pri vypracúvaní tohto návrhu uskutočnila Komisia konzultácie so širokou škálou zainteresovaných strán vrátane: inštitúcií a agentúr Európskej únie, medzinárodných organizácií, orgánov členských štátov, súkromných subjektov, ako aj jednotlivých prevádzkovateľov a vnútroštátnych a európskych priemyselných združení zastupujúcich prevádzkovateľov v mnohých rôznych odvetviach, expertov a sietí expertov, ako aj Európskej referenčnej siete na ochranu kritickej infraštruktúry (ERNCIP), členov akademickej obce, mimovládnych organizácií a verejnosti.

Konzultácie so zainteresovanými stranami sa uskutočnili rôznymi spôsobmi vrátane: možnosti verejnej spätnej väzby, pokiaľ ide o úvodné posúdenie vplyvu tohto návrhu, konzultačných seminárov, cielených dotazníkov, dvojstranných výmen a verejnej konzultácie (na podporu hodnotenia smernice ECI z roku 2019). Okrem toho externý dodávateľ zodpovedný za štúdiu uskutočniteľnosti, ktorá predstavovala podklad pre vypracovanie posúdenia vplyvu, uskutočnil konzultácie s mnohými zainteresovanými stranami, napríklad prostredníctvom online prieskumu, písomného dotazníka, individuálnych rozhovorov a virtuálnych „návštev na mieste“ v 10 členských štátoch.

Tieto konzultácie umožnili Komisii preskúmať účinnosť, efektívnosť, relevantnosť, súdržnosť a pridanú hodnotu EÚ, pokiaľ ide o existujúci rámec pre odolnosť kritickej infraštruktúry (t. j. východiskovú situáciu), analyzovať, aké problémy vytvorila, aké rôzne možnosti politiky by sa mohli zvážiť pri riešení týchto problémov a aké konkrétne vplyvy by tieto možnosti mohli mať. Vo všeobecnosti sa v rámci konzultácií poukázalo na niekoľko oblastí, v ktorých sa zainteresované strany celkovo zhodli, a v neposlednom rade aj na to, že existujúci rámec Európskej únie pre odolnosť kritickej infraštruktúry by sa mal vzhľadom na rastúcu vzájomnú závislosť medzi odvetviami a meniacu sa panorámu hrozieb prepracovať.

Konkrétne sa zainteresované strany celkovo zhodli na tom, že akýkoľvek nový prístup by mal pozostávať z kombinácie záväzných a nezáväzných opatrení, zamerať sa skôr na odolnosť než na ochranu štruktúr a poskytnúť jasnejšie prepojenie medzi opatreniami zameranými na zvýšenie kybernetickej a nekybernetickej odolnosti. Okrem toho podporili prístup, ktorý zohľadňuje ustanovenia existujúcich odvetvových právnych predpisov, zahŕňa aspoň tie odvetvia, na ktoré sa vzťahuje súčasná smernica NIS, ako aj jednotnejšie povinnosti pre kritické subjekty na vnútroštátnej úrovni, ktoré by zase mali byť schopné vykonávať dostatočnú bezpečnostnú previerku zamestnancov s prístupom k citlivým zariadeniam/informáciám. Zainteresované strany navyše navrhli, že akýkoľvek nový prístup by mal pre členské štáty vytvoriť príležitosti na vykonávanie posilneného dohľadu nad činnosťami kritických subjektov, ale mal by takisto zabezpečiť, aby sa identifikovali kritické subjekty celoeurópskeho významu a aby sa zaistila ich dostatočná odolnosť. Napokon sa

zainteresované strany zasadzovali za väčšie financovanie a podporu zo strany Európskej únie, napr. pokiaľ ide o vykonávanie akéhokoľvek nového nástroja, budovanie kapacít na vnútroštátnej úrovni a koordináciu/spoluprácu verejného a súkromného sektora či výmenu osvedčených postupov, poznatkov a odborných znalostí na rôznych úrovniach. Tento návrh obsahuje ustanovenia, ktoré vo všeobecnosti zodpovedajú názorom a preferenciám vyjadreným zainteresovanými stranami.

- **Získavanie a využívanie expertízy**

Ako sa uvádza v predchádzajúcej časti, Komisia pri vypracúvaní tohto návrhu vychádzala z odborných poznatkov získaných v rámci konzultácií, napr. s externými nezávislými expertmi, sieťami expertov a členmi akademickej obce.

- **Posúdenie vplyvu**

V posúdení vplyvu, ktoré podporilo vypracovanie tejto iniciatívy, sa skúmali rôzne možnosti politiky na riešenie už opísaných všeobecných a konkrétnych problémov. Okrem východiskovej situácie, ktorá by neviedla k žiadnej zmene súčasnej situácie, tieto možnosti zahŕňali:

– Možnosť 1: Zachovanie existujúcej smernice ECI, ktorá by bola sprevádzaná dobrovoľnými opatreniami v rámci existujúceho európskeho programu na ochranu kritickej infraštruktúry (EPCIP),

– Možnosť 2: Revízia existujúcej smernice ECI s cieľom pokryť rovnaké odvetvia ako existujúca smernica NIS a zamerať sa viac na odolnosť. Nová smernica ECI by priniesla zmeny do existujúceho cezhraničného procesu označovania európskej kritickej infraštruktúry vrátane nových kritérií na označovanie a nových požiadaviek na členské štáty a prevádzkovateľov,

– Možnosť 3: Nahradenie existujúcej smernice ECI novým nástrojom zameraným na zvýšenie odolnosti kritických subjektov v odvetviach, ktoré sa považujú za kľúčové v navrhovanej smernici o kybernetickej bezpečnosti. Touto možnosťou by sa stanovili minimálne požiadavky pre členské štáty a kritické subjekty identifikované podľa nového rámca. Stanovil by sa postup identifikácie kritických subjektov ponúkajúcich služby viacerým, ak nie všetkým, členským štátom Európskej únie alebo vo viacerých, ak nie vo všetkých, členských štátoch Európskej únie. Vykonávanie právneho predpisu by podporovalo osobitné vedomostné centrum v rámci Komisie,

– Možnosť 4: Nahradenie existujúcej smernice ECI novým nástrojom zameraným na zvýšenie odolnosti kritických subjektov v odvetviach, ktoré sa považujú za kľúčové v navrhovanej smernici o kybernetickej bezpečnosti, ako aj zaistenie významnejšej úlohy Komisie pri identifikácii kritických subjektov a vytvorenie špecializovanej agentúry EÚ zodpovednej za odolnosť kritickej infraštruktúry (ktorá by prevzala úlohy a povinnosti pridelené vedomostnému centru navrhnutému v predchádzajúcej možnosti).

Vzhľadom na rôzne hospodárske, sociálne a environmentálne vplyvy spojené s každou z možností, ale aj na ich hodnotu z hľadiska účinnosti, efektívnosti a proporcionality sa

v posúdení vplyvu zistilo, že uprednostňovanou možnosťou je možnosť 3. Zatiaľ čo možnosti 1 a 2 by nepriniesli zmeny potrebné na riešenie problému, možnosť 3 by viedla k vytvoreniu harmonizovaného a komplexnejšieho rámca odolnosti, ktorý by bol takisto v súlade s existujúcim právom Únie v súvisiacich oblastiach a zohľadňoval by ho. Možnosť 3 sa takisto považovala za primeranú a pravdepodobne politicky uskutočniteľnú, keďže je v súlade s vyhláseniami Rady a Parlamentu o potrebe prijatia opatrení Únie v tejto oblasti. Okrem toho sa zistilo, že táto možnosť pravdepodobne zabezpečí flexibilitu a ponúkne nadčasový rámec, ktorý by umožnil kritickým subjektom reagovať na rôzne riziká, ktorým budú postupom času vystavené. V posúdení vplyvu sa napokon zistilo, že táto možnosť by dopĺňala existujúce odvetvové a medziodvetvové rámce a nástroje. Táto možnosť napríklad počíta s tým, že ak by označené subjekty spĺňali určité povinnosti obsiahnuté v tomto novom nástroji spĺňaním povinností podľa už existujúcich nástrojov, neboli by v takomto prípade povinné prijať ďalšie opatrenia. Na druhej strane by sa od nich očakávalo, že prijmú určité opatrenia, ak sa existujúce nástroje nevzťahujú na danú záležitosť alebo sa obmedzujú len na určité druhy rizík alebo opatrení.

Posúdenie vplyvu preskúmal výbor pre kontrolu regulácie, ktorý 20. novembra 2020 vydal kladné stanovisko s výhradami. Výbor poukázal na niekoľko prvkov posúdenia vplyvu, ktoré by sa mali riešiť. Konkrétne požiadal o ďalšie objasnenie týkajúce sa rizík súvisiacich s kritickou infraštruktúrou a cezhraničným rozmerom, prepojenia medzi touto iniciatívou a prebiehajúcou revíziou smernice NIS a vzťahu medzi uprednostňovanou možnosťou politiky a inými odvetvovými právnymi predpismi. Okrem toho výbor videl potrebu, aby sa ďalej odôvodnilo rozšírenie rozsahu pôsobnosti nástroja naprieč odvetviami, a požiadal o dodatočné informácie týkajúce sa kritérií výberu kritických subjektov. Napokon, pokiaľ ide o proporcionalitu, výbor sa usiloval o ďalšie objasnenie toho, ako by uprednostňovaná možnosť viedla k lepším vnútroštátnym reakciám na cezhraničné riziká. Tieto a ďalšie podrobnejšie pripomienky výboru sa riešili v konečnej verzii posúdenia vplyvu, v ktorej sa napríklad podrobnejšie opisujú cezhraničné riziká pre kritické infraštruktúry a vzťah medzi týmto návrhom a návrhom smernice o kybernetickej bezpečnosti. Pripomienky výboru boli zohľadnené aj v tejto navrhovanej smernici.

- **Regulačná vhodnosť a zjednodušenie**

V súlade s Programom regulačnej vhodnosti a efektívnosti (REFIT) Komisie by sa všetky iniciatívy zamerané na zmenu existujúcich právnych predpisov EÚ mali snažiť o efektívnejšie zjednodušenie a dosiahnutie stanovených politických cieľov. Zo zistení posúdenia vplyvu vyplýva, že návrh by mal znížiť celkovú záťaž členských štátov. Užšie zosúladenie s prístupom súčasnej smernice NIS zameraným na služby pravdepodobne časom povedie k zníženiu nákladov na dodržiavanie predpisov. Napríklad zaťažujúci proces cezhraničnej identifikácie a označovania obsiahnutý v existujúcej smernici ECI by sa nahradil postupom založeným na rizikách na vnútroštátnej úrovni zameraným len na identifikáciu kritických subjektov, na ktoré by sa vzťahovali rôzne povinnosti. Na základe posúdenia rizík by členské štáty identifikovali kritické subjekty, z ktorých väčšina už je označená za prevádzkovateľov základných služieb podľa súčasnej smernice NIS.

Prijatím opatrení na zvýšenie ich odolnosti sa navyše zníži pravdepodobnosť, že kritické subjekty budú vystavené narušeniam. Pravdepodobnosť rušivých incidentov negatívne ovplyvňujúcich poskytovanie základných služieb v jednotlivých členských štátoch a v celej Európe by sa preto znížila. Spolu s pozitívnymi účinkami vyplývajúcimi z harmonizácie rozdielnych vnútroštátnych pravidiel na úrovni Únie by to malo pozitívny vplyv na podniky

vrátane mikropodnikov a malých a stredných podnikov, celkové zdravie hospodárstva Únie a spoľahlivé fungovanie vnútorného trhu.

- **Základné práva**

Cieľom navrhovaného právneho predpisu je zvýšiť odolnosť kritických subjektov poskytujúcich rôzne formy základných služieb a zároveň odstrániť regulačné prekážky, ktoré bránia ich schopnosti poskytovať služby v celej Únii. Tým by sa znížilo celkové riziko narušení na spoločenskej aj individuálnej úrovni a znížila by sa záťaž. Prispelo by to k zabezpečeniu vyššej úrovne verejnej bezpečnosti a zároveň by to pozitívne ovplyvnilo slobodu podnikania spoločností, ako aj mnohých ďalších hospodárskych subjektov závislých od poskytovania základných služieb, z čoho by mali v konečnom dôsledku prospech spotrebitelia. Ustanovenia návrhu zamerané na zabezpečenie účinného riadenia bezpečnosti zamestnancov budú obvykle zahŕňať spracovanie osobných údajov. Je to odôvodnené potrebou vykonávať previerky konkrétnych kategórií zamestnancov. Každé takéto spracovanie osobných údajov navyše vždy bude podliehať súladu s pravidlami Únie o ochrane osobných údajov vrátane všeobecného nariadenia o ochrane údajov[13].

4. VPLYV NA ROZPOČET

Navrhovaná smernica má vplyv na rozpočet Únie. Celkové finančné zdroje potrebné na podporu vykonávania tohto návrhu sa na obdobie 2021 – 2027 odhadujú na 42,9 milióna EUR, z čoho 5,1 milióna EUR predstavujú administratívne výdavky. Tieto náklady možno rozčleniť takto:

– podporné činnosti Komisie vrátane personálneho obsadenia, projektov, štúdií a podporných činností,

– poradné misie organizované Komisiou,

– pravidelné zasadnutia skupiny pre odolnosť kritických subjektov, komitologického výboru a iné zasadnutia.

Podrobnejšie informácie sú k dispozícii v legislatívnom finančnom výkaze, ktorý je pripojený k tomuto návrhu.

5. ĎALŠIE PRVKY

- **Plány vykonávania, spôsob monitorovania, hodnotenia a podávania správ**

Vykonávanie navrhovanej smernice sa preskúma do štyroch a pol roka po nadobudnutí jej účinnosti, a potom Komisia predloží správu Európskemu parlamentu a Rade. V tejto správe sa posúdi rozsah, v akom členské štáty prijali opatrenia potrebné na dosiahnutie súladu s touto smernicou. Správu, v ktorej sa posúdi vplyv a pridaná hodnota smernice, predloží Komisia Európskemu parlamentu a Rade do šiestich rokov od nadobudnutia účinnosti tejto smernice.

[13] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES.

- **Podrobné vysvetlenie konkrétnych ustanovení návrhu**

Predmet úpravy, rozsah pôsobnosti a vymedzenie pojmov (články 1 – 2)

V článku 1 sa stanovuje predmet úpravy a rozsah pôsobnosti tejto smernice, ktorá stanovuje pre členské štáty povinnosť prijať určité opatrenia zamerané na zabezpečenie poskytovania služieb na vnútornom trhu, ktoré sú nevyhnutné na zachovanie životne dôležitých spoločenských funkcií alebo hospodárskych činností, najmä s cieľom identifikovať kritické subjekty a umožniť im plniť si konkrétne povinnosti zamerané na zvýšenie ich odolnosti a zlepšenie ich schopnosti poskytovať tieto služby na vnútornom trhu. V smernici sa takisto stanovujú pravidlá dohľadu nad kritickými subjektmi a pravidlá presadzovania v tejto súvislosti, ako aj osobitný dohľad nad kritickými subjektmi, ktoré sa považujú za kritické subjekty osobitného európskeho významu. V článku 1 sa takisto vysvetľuje vzťah medzi smernicou a inými príslušnými právnymi predpismi Únie a podmienky, za ktorých sa s Komisiou a inými príslušnými orgánmi vymieňajú informácie, ktoré sú podľa právnych predpisov Únie a vnútroštátnych predpisov dôverné. V článku 2 sa uvádza zoznam pojmov, ktoré sa uplatňujú.

Vnútroštátne rámce v oblasti odolnosti kritických subjektov (články 3 – 9)

V článku 3 sa stanovuje, že členské štáty prijmú stratégiu na zvýšenie odolnosti kritických subjektov, opisujú sa v ňom prvky, ktoré by mala táto stratégia obsahovať, vysvetľuje sa v ňom, že by sa mala pravidelne a v prípade potreby aktualizovať, a stanovuje sa v ňom, že členské štáty oznámia svoje stratégie a akékoľvek ich aktualizácie Komisii. V článku 4 sa stanovuje, že príslušné orgány vypracujú zoznam základných služieb a pravidelne vykonávajú posúdenie všetkých relevantných rizík, ktoré môžu ovplyvniť poskytovanie týchto základných služieb, s cieľom identifikovať kritické subjekty. V tomto posúdení sa zohľadňujú posúdenia rizík vykonávané v súlade s inými príslušnými právnymi predpismi Únie, riziká vyplývajúce zo závislostí medzi konkrétnymi odvetviami a dostupné informácie o incidentoch. Členské štáty zabezpečia, aby boli kritickým subjektom sprístupnené relevantné prvky posúdenia rizík a aby sa Komisii pravidelne poskytovali údaje o typoch zistených rizík a výsledkoch ich posúdení rizík.

V článku 5 sa stanovuje, že členské štáty identifikujú kritické subjekty v konkrétnych odvetviach a pododvetviach. V procese identifikácie by sa mali zohľadňovať výsledky posúdenia rizík a uplatňovať osobitné kritériá. Členské štáty zostavia zoznam kritických subjektov, ktorý sa v prípade potreby a pravidelne aktualizuje. Kritické subjekty musia byť náležite informované o ich identifikácii a povinnostiach, ktoré im z toho vyplývajú. Príslušné orgány zodpovedné za vykonávanie tejto smernice informujú príslušné orgány zodpovedné za vykonávanie smernice o kybernetickej bezpečnosti o identifikácii kritických subjektov. Ak dva alebo viaceré členské štáty identifikujú ako kritický ten istý subjekt, tieto členské štáty navzájom konzultujú s cieľom znížiť zaťaženie kritického subjektu. Ak kritické subjekty poskytujú služby do viac ako tretiny členských štátov, resp. vo viac ako tretine členských štátov, dotknutý členský štát oznámi Komisii totožnosť týchto kritických subjektov.

V článku 6 sa vymedzuje pojem „závažný rušivý vplyv“, ako sa uvádza v článku 5 ods. 2, a vyžaduje sa v ňom, aby členské štáty predložili Komisii určité formy informácií týkajúce sa kritických subjektov, ktoré identifikujú, a spôsob ich identifikácie. V článku 6 sa okrem toho

Komisia splnomocňuje prijímať po konzultácii so skupinou pre odolnosť kritických subjektov príslušné usmernenia.

V článku 7 sa stanovuje, že členské štáty by mali identifikovať subjekty v odvetví bankovníctva, infraštruktúry finančného trhu a digitálnej infraštruktúry, s ktorými sa má zaobchádzať ako s kritickými subjektmi len na účely kapitoly II. Tieto subjekty by mali byť informované o ich identifikácii.

V článku 8 sa stanovuje, že každý členský štát určí jeden alebo viac príslušných orgánov zodpovedných za správne uplatňovanie tejto smernice na vnútroštátnej úrovni, ako aj miesto jednotného kontaktu poverené zabezpečením cezhraničnej spolupráce a zaistí, aby tieto orgány a miesto jednotného kontaktu mali k dispozícii primerané zdroje. Miesto jednotného kontaktu pravidelne predkladá Komisii súhrnnú správu o oznámeniach o incidentoch. V článku 8 sa vyžaduje, aby príslušné orgány zodpovedné za uplatňovanie smernice spolupracovali s inými príslušnými vnútroštátnymi orgánmi vrátane príslušných orgánov určených podľa smernice o kybernetickej bezpečnosti. V článku 9 sa stanovuje, že členské štáty poskytujú podporu kritickým subjektom pri zaisťovaní ich odolnosti a uľahčujú spoluprácu a dobrovoľnú výmenu informácií a osvedčených postupov medzi príslušnými orgánmi a kritickými subjektmi.

Odolnosť kritických subjektov (články 10 – 13)

V článku 10 sa stanovuje, že kritické subjekty pravidelne posudzujú všetky relevantné riziká na základe vnútroštátnych posúdení rizík a iných relevantných informačných zdrojov. V článku 11 sa stanovuje, že kritické subjekty prijmú vhodné a primerané technické a organizačné opatrenia na zabezpečenie svojej odolnosti a zabezpečia, aby boli tieto opatrenia opísané v pláne odolnosti alebo v rovnocennom dokumente či dokumentoch. Členské štáty môžu požiadať Komisiu, aby zorganizovala poradné misie s cieľom poskytovať poradenstvo kritickým subjektom pri plnení ich povinností. V článku 11 sa okrem toho Komisia splnomocňuje prijímať v prípade potreby delegované a vykonávacie akty.

V článku 12 sa stanovuje, že členské štáty zabezpečia, aby kritické subjekty mohli predkladať žiadosti o previerku osôb, ktoré patria alebo by mohli patriť do určitých osobitných kategórií zamestnancov, a aby tieto žiadosti urýchlene posúdili orgány zodpovedné za vykonávanie takýchto previerok osôb. V článku sa opisuje účel, rozsah a obsah previerok osôb, ktoré musia byť v súlade so všeobecným nariadením o ochrane údajov.

V článku 13 sa stanovuje, že členské štáty zabezpečia, aby kritické subjekty oznamovali príslušnému orgánu incidenty, ktoré významne narúšajú alebo by mohli významne narušiť ich prevádzku. Príslušné orgány zase poskytnú oznamujúcemu kritickému subjektu relevantné informácie týkajúce sa následných opatrení. Príslušné orgány prostredníctvom miesta jednotného kontaktu informujú aj miesta jednotného kontaktu ostatných dotknutých členských štátov v prípade, že incident má alebo by mohol mať cezhraničné dôsledky v jednom alebo vo viacerých iných členských štátoch.

Osobitný dohľad nad kritickými subjektmi osobitného európskeho významu (články 14 – 15)

V článku 14 sa kritické subjekty osobitného európskeho významu vymedzujú ako subjekty, ktoré boli identifikované ako kritické subjekty a ktoré poskytujú základné služby do viac ako tretiny členských štátov, resp. vo viac ako tretine členských štátov. Komisia po prijatí oznámenia podľa článku 5 ods. 6 oznámi dotknutému subjektu, že sa považuje za kritický subjekt osobitného európskeho významu, a informuje ho o jeho povinnostiach, ktoré mu z toho vyplývajú, a o dni, od ktorého sa na neho tieto povinnosti vzťahujú. V článku 15 sa opisujú osobitné mechanizmy dohľadu vzťahujúce sa na kritické subjekty osobitného európskeho významu, ktoré zahŕňajú skutočnosť, že hostiteľské členské štáty poskytnú na požiadanie Komisii a skupine pre odolnosť kritických subjektov informácie týkajúce sa posúdenia rizík podľa článku 10 a opatrení prijatých v súlade s článkom 11, ako aj akýchkoľvek opatrení v oblasti dohľadu alebo presadzovania. V článku 15 sa takisto stanovuje, že Komisia môže organizovať poradné misie s cieľom posúdiť opatrenia zavedené konkrétnymi kritickými subjektmi osobitného európskeho významu. Komisia na základe analýzy zistení poradnej misie skupiny pre odolnosť kritických subjektov oznámi členskému štátu, v ktorom sa nachádza infraštruktúra daného subjektu, svoje stanoviská k tomu, či si tento subjekt plní svoje povinnosti, a ak je to vhodné, aké opatrenia by sa mohli prijať na zlepšenie odolnosti tohto subjektu. V článku sa opisuje zloženie, organizácia a financovanie poradných misií. Takisto sa v ňom stanovuje, že Komisia prijme vykonávací akt, v ktorom stanoví pravidlá týkajúce sa procedurálnych mechanizmov na účely realizácie poradných misií a podávania správ o týchto misiách.

Spolupráca a podávanie správ (články 16 – 17)

V článku 16 sa opisuje rola a úlohy skupiny pre odolnosť kritických subjektov, ktorá sa skladá zo zástupcov členských štátov a Komisie. Skupina podporuje Komisiu a uľahčuje strategickú spoluprácu a výmenu informácií. V článku sa vysvetľuje, že Komisia môže prijať vykonávacie akty stanovujúce procesné mechanizmy potrebné na fungovanie skupiny pre odolnosť kritických subjektov. V článku 17 sa stanovuje, že Komisia tam, kde je to vhodné, podporuje členské štáty a kritické subjekty pri plnení ich povinností podľa tejto smernice a dopĺňa činnosti členských štátov uvedené v článku 9.

Dohľad a presadzovanie (články 18 – 19)

V článku 18 sa stanovuje, že členské štáty majú určité právomoci, prostriedky a zodpovednosť pri zabezpečovaní vykonávania a presadzovania smernice. Členské štáty zabezpečia, aby príslušný orgán pri posudzovaní toho, či kritický subjekt dodržuje povinnosti podľa tejto smernice, informoval príslušné orgány dotknutého členského štátu určené podľa smernice o kybernetickej bezpečnosti a aby tieto orgány mohol požiadať o posúdenie kybernetickej bezpečnosti takéhoto subjektu, pričom by tieto orgány mali na tento účel spolupracovať a vymieňať si informácie. V článku 19 sa stanovuje, že v súlade s dlhodobou praxou členské štáty stanovia pravidlá, pokiaľ ide o sankcie uplatniteľné pri porušení, a prijmú všetky opatrenia potrebné na zabezpečenie ich uplatňovania.

Záverečné ustanovenia (články 20 – 26)

V článku 20 sa stanovuje, že Komisii pomáha výbor, ktorý je výborom v zmysle nariadenia (EÚ) č. 182/2011. Ide o štandardný článok. Článkom 21 sa Komisii udeľuje právomoc prijímať delegované akty za podmienok stanovených v tomto článku. Takisto ide o štandardný článok. V článku 22 sa stanovuje, že Komisia predloží Európskemu parlamentu

a Rade správu, v ktorej posúdi rozsah, v akom členské štáty prijali opatrenia potrebné na dosiahnutie súladu s touto smernicou. Európskemu parlamentu a Rade sa musí pravidelne predkladať správa, v ktorej sa posúdi vplyv a pridaná hodnota smernice a či by sa rozsah pôsobnosti smernice mal rozšíriť na iné odvetvia alebo pododvetvia vrátane odvetvia výroby, spracovania a distribúcie potravín.

V článku 23 sa stanovuje, že smernica 2008/114/ES sa zrušuje s účinnosťou odo dňa nadobudnutia účinnosti tejto smernice. V článku 24 sa stanovuje, že členské štáty v stanovenej lehote prijmú a zverejnia zákony, iné právne predpisy a správne opatrenia potrebné na dosiahnutie súladu s touto smernicou a informujú o tom Komisiu. Znenie hlavných ustanovení vnútroštátnych právnych predpisov, ktoré prijmú v oblasti pôsobnosti tejto smernice, oznámia Komisii. V článku 25 sa stanovuje, že táto smernica nadobúda účinnosť dvadsiatym dňom po jej uverejnení v *Úradnom vestníku Európskej únie*. V článku 26 sa stanovuje, že táto smernica je určená členským štátom.

2020/0365 (COD)

Návrh

SMERNICA EURÓPSKEHO PARLAMENTU A RADY

o odolnosti kritických subjektov

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 114,

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru[14],

so zreteľom na stanovisko Výboru regiónov[15],

konajúc v súlade s riadnym legislatívnym postupom[16],

keďže:

(1) V smernici Rady 2008/114/ES[17] sa stanovuje postup na označenie európskych kritických infraštruktúr v odvetviach energetiky a dopravy, ktorých narušenie alebo zničenie by malo významný cezhraničný vplyv na najmenej dva členské štáty. Uvedená smernica sa zameriavala výlučne na ochranu takýchto infraštruktúr. V hodnotení smernice 2008/114/ES, ktoré sa uskutočnilo v roku 2019[18], sa však zistilo, že vzhľadom na čoraz prepojenejšiu a cezhraničnú povahu operácií využívajúcich kritickú infraštruktúru nie sú ochranné opatrenia týkajúce sa samotných jednotlivých aktív dostatočné na to, aby zabránili všetkým narušeniam. Preto je potrebné zmeniť prístup k zabezpečeniu odolnosti kritických subjektov, t. j. ich schopnosti zmierniť incidenty, ktoré majú potenciál narušiť prevádzku kritického subjektu, absorbovať ich, prispôsobiť sa im a zotaviť sa z nich.

(2) Napriek existujúcim opatreniam na úrovni Únie[19] a na vnútroštátnej úrovni zameraným na podporu ochrany kritických infraštruktúr v Únii subjekty prevádzkujúce tieto infraštruktúry nie sú primerane vybavené na riešenie súčasných a predpokladaných budúcich rizík pre ich prevádzku, ktoré môžu viesť k narušeniu

---

14 Ú. v. EÚ C , , s. .

15 Ú. v. EÚ C […], […], s. […].

16 Pozícia Európskeho parlamentu […] a Rady […].

17 Smernica Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu (Ú. v. EÚ L 345, 23.12.2008, s. 75).

18 SWD(2019) 308.

19 Európsky program na ochranu kritickej infraštruktúry (EPCIP).

poskytovania služieb, ktoré sú nevyhnutné na vykonávanie životne dôležitých spoločenských funkcií alebo hospodárskych činností. Je tomu tak v dôsledku dynamickej panorámy hrozieb s vyvíjajúcou sa teroristickou hrozbou a rastúcej vzájomnej závislosti medzi infraštruktúrami a odvetviami, ako aj z dôvodu zvýšeného fyzického rizika v dôsledku prírodných katastrof a zmeny klímy, čo zvyšuje frekvenciu a rozsah extrémnych poveternostných javov a prináša dlhodobé zmeny priemernej klímy, ktoré môžu znížiť kapacitu a efektívnosť určitých typov infraštruktúry, ak nie sú zavedené opatrenia na zvýšenie odolnosti alebo adaptáciu na zmenu klímy. Okrem toho príslušné odvetvia a typy subjektov nie sú vo všetkých členských štátoch konzistentne uznávané ako kritické.

(3) Tieto rastúce vzájomné závislosti sú výsledkom čoraz viac cezhraničnej a vzájomne prepojenej siete poskytovania služieb využívajúcej kľúčové infraštruktúry v celej Únii v odvetviach energetiky, dopravy, bankovníctva, infraštruktúry finančného trhu, digitálnej infraštruktúry, pitnej a odpadovej vody, zdravotníctva, určitých aspektov verejnej správy, ako aj vesmírnych služieb, pokiaľ ide o poskytovanie určitých služieb závislých od pozemných infraštruktúr, ktoré vlastnia, spravujú a prevádzkujú buď členské štáty, alebo súkromné strany, a preto sa nevzťahujú na infraštruktúry, ktoré vlastní, spravuje alebo prevádzkuje Únia ako súčasť svojich vesmírnych programov, resp. ktoré sú vlastnené, spravované alebo prevádzkované v jej mene. Tieto vzájomné závislosti znamenajú, že akékoľvek narušenie, dokonca čo len jedno, sprvoti obmedzené na jeden subjekt alebo jedno odvetvie, môže mať kaskádové účinky vo všeobecnosti, čo môže viesť k ďalekosiahlym a dlhotrvajúcim negatívnym vplyvom na poskytovanie služieb na celom vnútornom trhu. Pandémia COVID-19 ukázala zraniteľnosť našich čoraz prepojenejších spoločností voči rizikám s nízkou pravdepodobnosťou.

(4) Na subjekty zapojené do poskytovania základných služieb sa čoraz viac vzťahujú odlišné požiadavky stanovené právnymi predpismi členských štátov. Skutočnosť, že v niektorých členských štátoch sa na tieto subjekty vzťahujú menej prísne bezpečnostné požiadavky, nielenže môže mať negatívny vplyv na zachovanie životne dôležitých spoločenských funkcií alebo hospodárskych činností v celej Únii, ale vedie aj k prekážkam riadneho fungovania vnútorného trhu. Podobné typy subjektov sa v niektorých členských štátoch považujú za kritické, pričom v iných nie, a tie, ktoré sú identifikované ako kritické, podliehajú v rôznych členských štátoch rôznym požiadavkám. To vedie k dodatočnej a zbytočnej administratívnej záťaži pre spoločnosti, ktoré vykonávajú cezhraničné činnosti, najmä pre spoločnosti pôsobiace v členských štátoch s prísnejšími požiadavkami.

(5) Je preto potrebné stanoviť harmonizované minimálne pravidlá s cieľom zabezpečiť poskytovanie základných služieb na vnútornom trhu a zvýšiť odolnosť kritických subjektov.

(6) Na dosiahnutie tohto cieľa by členské štáty mali identifikovať kritické subjekty, ktoré by mali podliehať osobitným požiadavkám a dohľadu, ale ktoré by mali zároveň získať osobitnú podporu a poradenstvo zamerané na dosiahnutie vysokej úrovne odolnosti voči všetkým relevantným rizikám.

(7) Určité odvetvia hospodárstva, ako je energetika a doprava, sú už regulované alebo môžu byť v budúcnosti regulované odvetvovými aktmi práva Únie, ktoré obsahujú pravidlá týkajúce sa určitých aspektov odolnosti subjektov pôsobiacich v týchto

odvetviach. S cieľom komplexne riešiť odolnosť subjektov, ktoré sú rozhodujúce pre riadne fungovanie vnútorného trhu, by tieto opatrenia pre jednotlivé odvetvia mali byť doplnené opatreniami stanovenými v tejto smernici, čím sa vytvára zastrešujúci rámec, ktorý rieši odolnosť kritických subjektov, pokiaľ ide o všetky nebezpečenstvá, t. j. prírodné a ľudskou činnosťou spôsobené, náhodné i úmyselné.

(8) Vzhľadom na význam kybernetickej bezpečnosti pre odolnosť kritických subjektov a v záujme konzistentnosti je jednotný prístup medzi touto smernicou a smernicou Európskeho parlamentu a Rady (EÚ) XX/YY[20] [navrhovaná smernica o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, (ďalej len „smernica o kybernetickej bezpečnosti“)] potrebný vždy, keď je to možné. So zreteľom na vyšší výskyt a osobitné charakteristiky kybernetických rizík sa v smernici o kybernetickej bezpečnosti ukladajú komplexné požiadavky veľkému množstvu subjektov s cieľom zabezpečiť ich kybernetickú bezpečnosť. Vzhľadom na to, že kybernetická bezpečnosť sa dostatočne rieši v smernici o kybernetickej bezpečnosti, záležitosti, na ktoré sa vzťahuje, by sa mali vylúčiť z rozsahu pôsobnosti tejto smernice, a to bez toho, aby bol dotknutý osobitný režim pre subjekty v odvetví digitálnej infraštruktúry.

(9) Ak sa v ustanoveniach iných aktov práva Únie vyžaduje, aby kritické subjekty posúdili príslušné riziká, prijali opatrenia na zabezpečenie svojej odolnosti alebo oznamovali incidenty, a tieto požiadavky sú prinajmenšom rovnocenné zodpovedajúcim povinnostiam stanoveným v tejto smernici, príslušné ustanovenia tejto smernice by sa nemali uplatňovať, aby sa zabránilo duplicite a zbytočnému zaťaženiu. V takom prípade by sa mali uplatňovať príslušné ustanovenia týchto iných aktov. Ak sa príslušné ustanovenia tejto smernice neuplatňujú, nemali by sa uplatňovať ani jej ustanovenia o dohľade a presadzovaní. Členské štáty by však mali do svojej stratégie na posilnenie odolnosti kritických subjektov, posúdenia rizika a podporných opatrení podľa kapitoly II zahrnúť všetky odvetvia uvedené v prílohe a mali by byť schopné identifikovať kritické subjekty v týchto odvetviach, ak boli splnené príslušné podmienky, pričom by mali zohľadniť osobitný režim pre subjekty v odvetví bankovníctva, infraštruktúry finančného trhu a digitálnej infraštruktúry.

(10) S cieľom zabezpečiť komplexný prístup k odolnosti kritických subjektov by každý členský štát mal mať stratégiu stanovujúcu ciele a politické opatrenia, ktoré sa majú vykonať. Na dosiahnutie tohto cieľa by členské štáty mali zabezpečiť, aby sa v ich stratégiách kybernetickej bezpečnosti stanovil politický rámec pre posilnenú koordináciu medzi príslušným orgánom podľa tejto smernice a príslušným orgánom podľa smernice o kybernetickej bezpečnosti v kontexte výmeny informácií o incidentoch a kybernetických hrozbách a plnenia úloh v oblasti dohľadu.

(11) Opatrenia členských štátov zamerané na identifikáciu a pomoc pri zabezpečovaní odolnosti kritických subjektov by sa mali riadiť prístupom založeným na riziku, ktorý zameriava úsilie na subjekty, ktoré sú najdôležitejšie z hľadiska výkonu životne dôležitých spoločenských funkcií alebo hospodárskych činností. S cieľom zabezpečiť takýto cielený prístup by mal každý členský štát v harmonizovanom rámci vykonať posúdenie všetkých relevantných prírodných a ľudskou činnosťou spôsobených rizík, ktoré môžu ovplyvniť poskytovanie základných služieb vrátane nehôd, prírodných

[20] [Odkaz na smernicu o kybernetickej bezpečnosti po jej prijatí.]

katastrof, ohrozenia verejného zdravia, ako sú pandémie, a antagonistických hrozieb vrátane trestných činov terorizmu. Pri vykonávaní týchto posúdení rizík by členské štáty mali zohľadniť ďalšie všeobecné alebo odvetvové posúdenia rizika, ktoré sa vykonávajú podľa iných aktov práva Únie, a mali by zvážiť závislosť medzi odvetviami, a to aj pokiaľ ide o odvetvia z iných členských štátov a tretích krajín. Výsledky posúdenia rizika by sa mali použiť v procese identifikácie kritických subjektov a na pomoc týmto subjektom pri plnení požiadaviek tejto smernice v oblasti odolnosti.

(12) S cieľom zabezpečiť, aby sa na všetky príslušné subjekty vzťahovali tieto požiadavky, a znížiť rozdiely v tejto súvislosti, je dôležité stanoviť harmonizované pravidlá umožňujúce jednotnú identifikáciu kritických subjektov v celej Únii a zároveň umožniť členským štátom, aby mohli zohľadniť vnútroštátne špecifiká. Preto by sa mali stanoviť kritériá na identifikáciu kritických subjektov. V záujme účinnosti, efektívnosti, konzistentnosti a právnej istoty by sa mali stanoviť aj vhodné pravidlá týkajúce sa oznamovania a spolupráce v súvislosti s takouto identifikáciou, ako aj právnych dôsledkov takejto identifikácie. S cieľom umožniť Komisii posúdiť správne uplatňovanie tejto smernice by členské štáty mali Komisii predložiť čo najpodrobnejšie a najkonkrétnejšie relevantné informácie a v každom prípade zoznam základných služieb, počet kritických subjektov identifikovaných pre každé odvetvie a pododvetvie uvedené v prílohe a základné služby alebo služby, ktoré každý subjekt poskytuje, a všetky uplatňované prahové hodnoty.

(13) Mali by sa stanoviť aj kritériá na určenie závažnosti rušivého účinku vyvolaného takýmito incidentmi. Tieto kritériá by mali vychádzať z kritérií stanovených v smernici Európskeho parlamentu a Rady (EÚ) 2016/1148[21], aby sa využilo úsilie členských štátov pri identifikácii daných prevádzkovateľov a skúsenosti získané v tejto súvislosti.

(14) Subjekty patriace do odvetvia digitálnej infraštruktúry sú v podstate založené na sieťach a informačných systémoch a patria do rozsahu pôsobnosti smernice o kybernetickej bezpečnosti, ktorá sa zaoberá fyzickou bezpečnosťou takýchto systémov ako súčasti ich povinností v oblasti riadenia kybernetických rizík a oznamovania. Keďže sa na tieto záležitosti vzťahuje smernica o kybernetickej bezpečnosti, táto smernica takýmto subjektom povinnosti neukladá. Vzhľadom na význam služieb poskytovaných subjektmi v odvetví digitálnej infraštruktúry pre poskytovanie iných základných služieb by však členské štáty mali na základe kritérií a s použitím postupu stanoveného v tejto smernici primerane identifikovať subjekty patriace do odvetvia digitálnej infraštruktúry, s ktorými by sa malo zaobchádzať ako s rovnocennými kritickým subjektom len na účely kapitoly II, a to aj pokiaľ ide o ustanovenie o podpore členských štátov pri zvyšovaní odolnosti týchto subjektov. V dôsledku toho by sa na takéto subjekty nemali vzťahovať povinnosti stanovené v kapitolách III až VI. Keďže povinnosti kritických subjektov poskytovať príslušným orgánom určité informácie, ktoré sú stanovené v kapitole II, sa týkajú uplatňovania kapitol III a IV, tieto subjekty by nemali podliehať ani týmto povinnostiam.

---

[21] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).

(15) V *acquis* EÚ v oblasti finančných služieb sa stanovujú komplexné požiadavky na finančné subjekty, aby mohli riadiť všetky riziká, ktorým čelia, vrátane prevádzkových rizík a zabezpečiť kontinuitu činností. Patrí sem nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012[22], smernica Európskeho parlamentu a Rady 2014/65/EÚ[23] a nariadenie Európskeho parlamentu a Rady (EÚ) č. 600/2014[24], ako aj nariadenie Európskeho parlamentu a Rady (EÚ) č. 575/2013[25] a smernica Európskeho parlamentu a Rady 2013/36/EÚ[26]. Komisia nedávno navrhla doplniť tento rámec nariadením Európskeho parlamentu a Rady XX/YYYY [navrhované nariadenie o digitálnej prevádzkovej odolnosti finančného sektora (ďalej len „nariadenie DORA“)[27]], ktorým sa stanovujú požiadavky na finančné spoločnosti, pokiaľ ide o riadenie IKT rizík vrátane ochrany fyzických infraštruktúr IKT. Keďže na odolnosť subjektov uvedených v bodoch 3 a 4 prílohy sa komplexne vzťahuje *acquis* EÚ v oblasti finančných služieb, aj s týmito subjektmi by sa malo zaobchádzať ako s rovnocennými kritickým subjektom len na účely kapitoly II tejto smernice. S cieľom zabezpečiť jednotné uplatňovanie pravidiel týkajúcich sa prevádzkového rizika a digitálnej odolnosti vo finančnom sektore by podporu členských štátov zameranú na zvýšenie celkovej odolnosti finančných subjektov rovnocenných kritickým subjektom mali zabezpečiť orgány určené podľa článku 41 [nariadenia DORA], pričom by sa na túto podporu mali vzťahovať postupy stanovené v uvedených právnych predpisoch úplne harmonizovaným spôsobom.

(16) Členské štáty by mali určiť orgány príslušné na dohľad nad uplatňovaním a v prípade potreby presadzovaním pravidiel tejto smernice a zabezpečiť, aby tieto orgány mali primerané právomoci a zdroje. Vzhľadom na rozdiely vo vnútroštátnych riadiacich štruktúrach a s cieľom chrániť už existujúce odvetvové mechanizmy alebo orgány dohľadu a regulačné orgány Únie a zabrániť duplicite by členské štáty mali mať možnosť určiť viac ako jeden príslušný orgán. V takom prípade by však mali jasne vymedziť príslušné úlohy dotknutých orgánov a zabezpečiť ich hladkú a účinnú spoluprácu. Všetky príslušné orgány by mali vo všeobecnosti spolupracovať aj s ostatnými príslušnými orgánmi na vnútroštátnej úrovni, ako aj na úrovni Únie.

(17) S cieľom uľahčiť cezhraničnú spoluprácu a komunikáciu a umožniť účinné vykonávanie tejto smernice by mal každý členský štát bez toho, aby boli dotknuté odvetvové právne požiadavky Únie, určiť jeden z orgánov, ktoré určil za príslušné orgány podľa tejto smernice, za miesto jednotného kontaktu zodpovedné

---

22 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov (Ú. v. EÚ L 201, 27.7.2012, s. 1).

23 Smernica Európskeho parlamentu a Rady 2014/65/EÚ z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorou sa mení smernica 2002/92/ES a smernica 2011/61/EÚ (Ú. v. EÚ L 173, 12.6.2014, s. 349).

24 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 600/2014 z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorým sa mení nariadenie (EÚ) č. 648/2012 (Ú. v. EÚ L 173, 12.6.2014, s. 84).

25 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 575/2013 z 26. júna 2013 o prudenciálnych požiadavkách na úverové inštitúcie a investičné spoločnosti a o zmene nariadenia (EÚ) č. 648/2012 (Ú. v. EÚ L 176, 27.6.2013, s. 1).

26 Smernica Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami a investičnými spoločnosťami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES (Ú. v. EÚ L 176, 27.6.2013, s. 338).

27 Návrh nariadenia Európskeho parlamentu a Rady o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014 a (EÚ) č. 909/2014 – COM(2020) 595.

za koordináciu otázok týkajúcich sa odolnosti kritických subjektov a cezhraničnej spolupráce v tejto oblasti na úrovni Únie.

(18) Vzhľadom na to, že podľa smernice o kybernetickej bezpečnosti subjekty identifikované ako kritické subjekty, ako aj identifikované subjekty v odvetví digitálnej infraštruktúry, s ktorými sa má podľa tejto smernice zaobchádzať ako s rovnocennými, podliehajú požiadavkám smernice o kybernetickej bezpečnosti týkajúcim sa kybernetickej bezpečnosti, by mali príslušné orgány určené podľa týchto dvoch smerníc spolupracovať, najmä pokiaľ ide o kybernetické riziká a incidenty, ktoré majú vplyv na tieto subjekty.

(19) Členské štáty by mali podporovať kritické subjekty pri posilňovaní ich odolnosti v súlade s ich povinnosťami podľa tejto smernice bez toho, aby bola dotknutá ich právna zodpovednosť za zabezpečenie takéhoto dodržiavania povinností. Členské štáty by mohli vypracovať najmä poradenský materiál a metodiky, podporovať organizovanie cvičení na testovanie ich odolnosti a poskytovať odbornú prípravu zamestnancom kritických subjektov. Okrem toho vzhľadom na vzájomnú závislosť medzi subjektmi a odvetviami by členské štáty mali vytvoriť nástroje na výmenu informácií na podporu dobrovoľnej výmeny informácií medzi kritickými subjektmi bez toho, aby bolo dotknuté uplatňovanie pravidiel hospodárskej súťaže stanovených v Zmluve o fungovaní Európskej únie.

(20) Aby boli kritické subjekty schopné zabezpečiť svoju odolnosť, mali by mať komplexné znalosti o všetkých relevantných rizikách, ktorým sú vystavené, a mali by tieto riziká analyzovať. Na tento účel by mali vykonávať posúdenie rizík vždy, keď je to potrebné vzhľadom na ich osobitnú situáciu a vývoj predmetných rizík, v každom prípade však každé štyri roky. Posúdenia rizík, ktoré vykonávajú kritické subjekty, by mali vychádzať z posúdenia rizika, ktoré vykonali členské štáty.

(21) Kritické subjekty by mali prijať organizačné a technické opatrenia, ktoré sú vhodné a primerané rizikám, ktorým čelia, aby predišli incidentu, odolali mu, zmierňovali ho, absorbovali ho, prispôsobili sa mu a zotavili sa z neho. Hoci kritické subjekty by mali prijať opatrenia vo všetkých bodoch uvedených v tejto smernici, podrobnosti a rozsah opatrení by mali odrážať rôzne riziká, ktoré každý subjekt identifikoval ako súčasť svojho posúdenia rizika, a osobitosti takéhoto subjektu vhodným a primeraným spôsobom.

(22) V záujme účinnosti a zodpovednosti by kritické subjekty mali opísať tieto opatrenia so zreteľom na zistené riziká a s mierou podrobnosti postačujúcou na dosiahnutie týchto cieľov v pláne odolnosti alebo v dokumente či dokumentoch, ktoré sú rovnocenné plánom odolnosti, pričom by tento plán mali uplatňovať v praxi. Takýto rovnocenný dokument alebo dokumenty sa môžu vypracovať v súlade s požiadavkami a normami vypracovanými v kontexte medzinárodných dohôd o fyzickej ochrane, ktorých sú členské štáty zmluvnými stranami, vrátane Dohovoru o fyzickej ochrane jadrových materiálov a jadrových zariadení.

(23) Nariadením Európskeho parlamentu a Rady (ES) č. 300/2008[28], nariadením Európskeho parlamentu a Rady (ES) č. 725/2004[29] a smernicou Európskeho parlamentu a Rady 2005/65/ES[30] sa stanovujú požiadavky uplatniteľné na subjekty v odvetviach leteckej a námornej dopravy s cieľom predchádzať incidentom spôsobeným protiprávnymi činmi a odolávať takýmto incidentom a zmierňovať ich následky. Zatiaľ čo opatrenia požadované v tejto smernici sú širšie, pokiaľ ide o riešené riziká a druhy opatrení, ktoré sa majú prijať, kritické subjekty v týchto odvetviach by mali vo svojom pláne odolnosti alebo rovnocenných dokumentoch zohľadniť opatrenia prijaté podľa týchto iných aktov Únie. Okrem toho pri vykonávaní opatrení na zabezpečenie odolnosti podľa tejto smernice môžu kritické subjekty zvážiť odkaz na nezáväzné usmernenia a dokumenty o osvedčených postupoch vypracované v rámci odvetvových pracovných tokov, ako je napríklad platforma EÚ pre bezpečnosť cestujúcich v železničnej doprave[31].

(24) Riziko, že zamestnanci kritických subjektov zneužijú napríklad svoje prístupové práva v rámci organizácie subjektu na poškodenie a spôsobenie škody, vyvoláva čoraz väčšie obavy. Toto riziko ešte zhoršuje rastúci jav radikalizácie, ktorý vedie k násilnému extrémizmu a terorizmu. Je preto potrebné umožniť kritickým subjektom žiadať o previerku osôb, ktoré patria do osobitných kategórií ich zamestnancov, a zabezpečiť, aby príslušné orgány tieto žiadosti urýchlene posúdili v súlade s uplatniteľnými pravidlami práva Únie a vnútroštátneho práva vrátane pravidiel o ochrane osobných údajov.

(25) Kritické subjekty by mali čo najskôr za daných okolností informovať príslušné orgány členských štátov o incidentoch, ktoré významne narúšajú alebo môžu významne narušiť ich prevádzku. Takáto informácia by mala príslušným orgánom umožniť rýchlo a primerane reagovať na predmetné incidenty a získať komplexný prehľad o celkových rizikách, ktorým čelia kritické subjekty. Na tento účel by sa mal stanoviť postup oznamovania určitých incidentov a mali by sa stanoviť parametre na určenie toho, kedy je skutočné alebo potenciálne narušenie závažné, a preto by sa incidenty mali oznamovať. Vzhľadom na možné cezhraničné vplyvy takýchto narušení by sa mal stanoviť postup, na základe ktorého by členské štáty informovali ostatné dotknuté členské štáty prostredníctvom miest jednotného kontaktu.

(26) Zatiaľ čo kritické subjekty vo všeobecnosti pôsobia ako súčasť čoraz prepojenejšej siete poskytovania služieb a infraštruktúr a často poskytujú základné služby vo viac ako jednom členskom štáte, niektoré z týchto subjektov majú pre Úniu osobitný význam, pretože poskytujú základné služby veľkému počtu členských štátov, a preto si vyžadujú osobitný dohľad na úrovni Únie. Preto by sa mali stanoviť pravidlá týkajúce sa osobitného dohľadu nad takýmito kritickými subjektmi osobitného európskeho

---

28 Nariadenie Európskeho parlamentu a Rady (ES) č. 300/2008 z 11. marca 2008 o spoločných pravidlách v oblasti bezpečnostnej ochrany civilného letectva a o zrušení nariadenia (ES) č. 2320/2002 (Ú. v. EÚ L 97, 9.4.2008, s. 72).

29 Nariadenie Európskeho parlamentu a Rady (ES) č. 725/2004 z 31. marca 2004 o zvýšení bezpečnosti lodí a prístavných zariadení (Ú. v. EÚ L 129, 29.4.2004, s. 6).

30 Smernica Európskeho parlamentu a Rady 2005/65/ES z 26. októbra 2005 o zvýšení bezpečnosti prístavov (Ú. v. EÚ L 310, 25.11.2005, s. 28).

31 Rozhodnutie Komisie C/2018/4014 z 29. júna 2018, ktorým sa zriaďuje platforma EÚ pre bezpečnosť cestujúcich v železničnej doprave.

významu. Týmito pravidlami nie sú dotknuté pravidlá dohľadu a presadzovania stanovené v tejto smernici.

(27) Ak sa ktorýkoľvek členský štát domnieva, že sú potrebné dodatočné informácie na to, aby mohol na základe dohody s členským štátom, v ktorom sa nachádza infraštruktúra kritického subjektu, poskytnúť poradenstvo tomuto kritickému subjektu pri plnení jeho povinností podľa kapitoly III alebo posúdiť, či tento kritický subjekt osobitného európskeho významu dodržiava tieto povinnosti, Komisia by mala zorganizovať poradnú misiu s cieľom posúdiť opatrenia zavedené týmto subjektom. S cieľom zabezpečiť riadne vykonávanie takýchto poradných misií by sa mali stanoviť doplňujúce pravidlá týkajúce sa najmä ich organizácie a riadenia, následných opatrení, ktoré sa majú vykonať, a povinností kritických subjektov osobitného európskeho významu. Poradné misie by sa mali bez toho, aby bola dotknutá potreba členského štátu, v ktorom sa poradná misia vedie, a dotknutého subjektu, dodržiavať pravidlá tejto smernice, vykonávať na základe podrobných pravidiel práva daného členského štátu, napríklad pokiaľ ide o presné podmienky, ktoré treba splniť na získanie prístupu do príslušných priestorov alebo k dokumentom, a pravidiel o prostriedkoch súdnej nápravy. Osobitné odborné znalosti potrebné pre takéto misie by sa v prípade potreby mohli požadovať prostredníctvom Koordinačného centra pre reakcie na núdzové situácie.

(28) S cieľom podporiť Komisiu a uľahčiť strategickú spoluprácu a výmenu informácií vrátane najlepších postupov v otázkach týkajúcich sa tejto smernice by sa mala zriadiť skupina pre odolnosť kritických subjektov, ktorá bude expertnou skupinou Komisie. Členské štáty by sa mali usilovať zabezpečiť účinnú a efektívnu spoluprácu určených zástupcov svojich príslušných orgánov v skupine pre odolnosť kritických subjektov. Skupina by mala začať plniť svoje úlohy šesť mesiacov po nadobudnutí účinnosti tejto smernice, aby bola ďalším z nástrojov na primeranú spoluprácu počas transpozičného obdobia tejto smernice.

(29) V záujme dosiahnutia cieľov tejto smernice a bez toho, aby bola dotknutá právna zodpovednosť členských štátov a kritických subjektov zabezpečiť dodržiavanie ich príslušných povinností, ktoré sú v nej stanovené, by Komisia, ak to považuje za vhodné, mala vykonať určité podporné činnosti zamerané na uľahčenie plnenia týchto povinností. Pri poskytovaní podpory členským štátom a kritickým subjektom pri plnení povinností podľa tejto smernice by Komisia mala vychádzať z existujúcich štruktúr a nástrojov, ako sú napríklad štruktúry a nástroje v rámci mechanizmu Únie v oblasti civilnej ochrany a Európskej referenčnej siete na ochranu kritickej infraštruktúry.

(30) Členské štáty by mali zabezpečiť, aby ich príslušné orgány mali určité osobitné právomoci na riadne uplatňovanie a presadzovanie tejto smernice vo vzťahu ku kritickým subjektom, ak tieto subjekty patria do ich jurisdikcie, ako sa uvádza v tejto smernici. Tieto právomoci by mali zahŕňať najmä právomoc vykonávať inšpekcie, dohľad a audity, vyžadovať od kritických subjektov, aby poskytovali informácie a dôkazy týkajúce sa opatrení, ktoré prijali na splnenie svojich povinností, a v prípade potreby vydávať príkazy na nápravu zistených porušení. Pri vydávaní takýchto príkazov by členské štáty nemali vyžadovať opatrenia, ktoré presahujú rámec toho, čo je nevyhnutné a primerané toho, aby dotknutý kritický subjekt dodržiaval povinnosti podľa tejto smernice, a to najmä so zreteľom na závažnosť porušenia a hospodársku kapacitu kritického subjektu. Všeobecnejšie by tieto právomoci mali byť sprevádzané

primeranými a účinnými zárukami, ktoré sa stanovia vo vnútroštátnom práve, v súlade s požiadavkami vyplývajúcimi z Charty základných práv Európskej únie. Pri posudzovaní toho, či kritický subjekt dodržiava svoje povinnosti podľa tejto smernice by príslušné orgány určené podľa tejto smernice mali mať možnosť požiadať príslušné orgány určené podľa smernice o kybernetickej bezpečnosti o posúdenie kybernetickej bezpečnosti týchto subjektov. Uvedené príslušné orgány by mali na tento účel spolupracovať a vymieňať si informácie.

(31) V záujme zohľadnenia nových rizík, technologického vývoja alebo osobitostí jedného alebo viacerých odvetví by sa mala na Komisiu delegovať právomoc prijímať akty v súlade s článkom 290 Zmluvy o fungovaní Európskej únie, aby mohla dopĺňať opatrenia na zabezpečenie odolnosti, ktoré majú kritické subjekty prijať, ďalším vymedzením niektorých alebo všetkých týchto opatrení. Je osobitne dôležité, aby Komisia počas prípravných prác uskutočnila príslušné konzultácie, a to aj na úrovni odborníkov, a aby tieto konzultácie vykonávala v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva[32]. Predovšetkým, v záujme rovnakého zastúpenia pri príprave delegovaných aktov, sa všetky dokumenty doručujú Európskemu parlamentu a Rade v rovnakom čase ako odborníkom z členských štátov, a odborníci Európskeho parlamentu a Rady majú systematický prístup na zasadnutia skupín odborníkov Komisie, ktoré sa zaoberajú prípravou delegovaných aktov.

(32) S cieľom zabezpečiť jednotné podmienky vykonávania tejto smernice by sa mali na Komisiu preniesť vykonávacie právomoci. Uvedené právomoci by sa mali vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 182/2011[33].

(33) Keďže ciele tejto smernice, a to zabezpečenie poskytovania služieb nevyhnutných na zachovanie životne dôležitých spoločenských funkcií alebo hospodárskych činností na vnútornom trhu a zvýšenie odolnosti kritických subjektov poskytujúcich takéto služby, nie je možné uspokojivo dosiahnuť na úrovni členských štátov, ale z dôvodu účinku tohto opatrenia ich možno lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o Európskej únii. V súlade so zásadou proporcionality podľa uvedeného článku 5 táto smernica neprekračuje rámec nevyhnutný na dosiahnutie týchto cieľov.

(34) Smernica 2008/114/ES by sa preto mala zrušiť,

PRIJALI TÚTO SMERNICU:

---

32 Ú. v. EÚ L 123, 12.5.2016, s. 1.

33 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 182/2011 zo 16. februára 2011, ktorým sa ustanovujú pravidlá a všeobecné zásady mechanizmu, na základe ktorého členské štáty kontrolujú vykonávanie vykonávacích právomocí Komisie (Ú. v. EÚ L 55, 28.2.2011, s. 13).

KAPITOLA I
PREDMET ÚPRAVY, ROZSAH PÔSOBNOSTI A VYMEDZENIE POJMOV

Článok 1
Predmet úpravy a rozsah pôsobnosti

1. Táto smernica:

   a) stanovuje pre členské štáty povinnosť prijať určité opatrenia zamerané na zabezpečenie poskytovania služieb na vnútornom trhu, ktoré sú nevyhnutné na zachovanie životne dôležitých spoločenských funkcií alebo hospodárskych činností, najmä s cieľom identifikovať kritické subjekty a subjekty, s ktorými sa má v určitých ohľadoch zaobchádzať ako s rovnocennými, a umožniť im plniť si povinnosti;

   b) stanovuje pre kritické subjekty povinnosti zamerané na zvýšenie ich odolnosti a zlepšenie ich schopnosti poskytovať tieto služby na vnútornom trhu;

   c) stanovuje pravidlá dohľadu nad kritickými subjektmi a ich presadzovania a osobitný dohľad nad kritickými subjektmi, ktoré sa považujú za subjekty osobitného európskeho významu.

2. Bez toho, aby bol dotknutý článok 7 sa táto smernica nevzťahuje na záležitosti, na ktoré sa vzťahuje smernica (EÚ) XX/YY [navrhovaná smernica o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii; (ďalej len „smernica o kybernetickej bezpečnosti“)].

3. Ak sa v ustanoveniach odvetvových aktov práva Únie vyžaduje, aby kritické subjekty prijali opatrenia stanovené v kapitole III, a ak sú tieto požiadavky aspoň rovnocenné s povinnosťami stanovenými v tejto smernici, príslušné ustanovenia tejto smernice vrátane ustanovení o dohľade a presadzovaní uvedených v kapitole VI sa neuplatňujú.

4. Bez toho, aby bol dotknutý článok 346 ZFEÚ, informácie, ktoré sú dôverné podľa predpisov Únie a vnútroštátnych predpisov, ako napríklad predpisov o obchodnom tajomstve, sa vymieňajú s Komisiou a inými príslušnými orgánmi len v prípade, ak je táto výmena potrebná na účely uplatňovania tejto smernice. Vymieňané informácie sa obmedzujú na tie informácie, ktoré sú relevantné a primerané účelu tejto výmeny. Pri takejto výmene informácií sa zachováva ich dôvernosť a chránia sa bezpečnostné a obchodné záujmy kritických subjektov.

Článok 2
Vymedzenie pojmov

Na účely tejto smernice sa uplatňuje toto vymedzenie pojmov:

1. „kritický subjekt“ je verejný alebo súkromný subjekt typu uvedeného v prílohe, ktorý bol ako taký identifikovaný členským štátom v súlade s článkom 5;

2. „odolnosť“ je schopnosť predchádzať incidentu, ktorý narúša alebo môže narušiť prevádzku kritického subjektu, odolávať tomuto incidentu, zmierňovať ho, absorbovať ho, prispôsobiť sa mu a zotaviť sa z neho;

3. „incident“ je každá udalosť, ktorá môže narušiť alebo ktorá narúša prevádzku kritického subjektu;

4. „infraštruktúra“ je zložka, systém alebo jeho časť, ktoré sú potrebné na poskytovanie základnej služby;

5. „základná služba“ je služba, ktorá má zásadný význam z hľadiska zachovania životne dôležitých spoločenských alebo hospodárskych činností;

6. „riziko“ je akákoľvek okolnosť alebo udalosť, ktorá môže mať nepriaznivý vplyv na odolnosť kritických subjektov;

7. „posúdenie rizika“ je metodika na určenie povahy a rozsahu rizika prostredníctvom analýzy potenciálnych hrozieb a nebezpečenstiev a hodnotenia existujúcich podmienok zraniteľnosti, ktoré by mohli narušiť prevádzku kritického subjektu.

KAPITOLA II
VNÚTROŠTÁTNE RÁMCE V OBLASTI ODOLNOSTI KRITICKÝCH SUBJEKTOV

Článok 3
Stratégia v oblasti odolnosti kritických subjektov

1. Každý členský štát prijme do [troch rokov od nadobudnutia účinnosti tejto smernice] stratégiu na posilnenie odolnosti kritických subjektov. V tejto stratégii sa stanovia strategické ciele a politické opatrenia s cieľom dosiahnuť a udržať vysokú úroveň odolnosti týchto kritických subjektov a pokryť aspoň odvetvia uvedené v prílohe.

2. Stratégia obsahuje minimálne tieto prvky:

   a) strategické ciele a priority na účely zvýšenia celkovej odolnosti kritických subjektov s prihliadnutím na cezhraničné a medziodvetvové vzájomné závislosti;

   b) rámec riadenia na dosiahnutie strategických cieľov a priorít vrátane opisu úloh a zodpovedností rôznych orgánov, kritických subjektov a iných strán zapojených do vykonávania stratégie;

   c) opis opatrení potrebných na zvýšenie celkovej odolnosti kritických subjektov vrátane vnútroštátneho posúdenia rizika, identifikácie kritických subjektov a subjektov rovnocenných kritickým subjektom a opatrení na podporu kritických subjektov prijatých v súlade s touto kapitolou;

d) politický rámec pre posilnenú koordináciu medzi príslušnými orgánmi určenými podľa článku 8 tejto smernice a podľa [smernice o kybernetickej bezpečnosti] na účely výmeny informácií o incidentoch a kybernetických hrozbách a vykonávania úloh dohľadu.

Stratégia sa aktualizuje v prípade potreby a aspoň každé štyri roky.

3. Členské štáty oznámia Komisii svoje stratégie a akékoľvek ich aktualizácie do troch mesiacov od ich prijatia.

Článok 4
Posúdenie rizika členskými štátmi

1. Príslušné orgány určené podľa článku 8 vypracujú zoznam základných služieb v odvetviach uvedených v prílohe. Do [troch rokov od nadobudnutia účinnosti tejto smernice] a následne v prípade potreby a aspoň každé štyri roky vykonajú posúdenie všetkých relevantných rizík, ktoré môžu ovplyvniť poskytovanie týchto základných služieb, s cieľom identifikovať kritické subjekty v súlade s článkom 5 ods. 1 a pomôcť týmto kritickým subjektom prijať opatrenia podľa článku 11.

   V posúdení rizika sa zohľadňujú všetky relevantné prírodné riziká a riziká spôsobené ľudskou činnosťou vrátane nehôd, prírodných katastrof, ohrozenia verejného zdravia, antagonistických hrozieb vrátane trestných činov terorizmu podľa smernice Európskeho parlamentu a Rady (EÚ) 2017/541[34].

2. Pri vykonávaní posúdenia rizika členské štáty zohľadňujú aspoň:

   a) všeobecné posúdenie rizika vykonané podľa článku 6 ods. 1 rozhodnutia Európskeho parlamentu a Rady č. 1313/2013/EÚ[35];

   b) iné relevantné posúdenia rizík vykonané v súlade s požiadavkami príslušných odvetvových aktov práva Únie vrátane nariadenia Európskeho parlamentu a Rady (EÚ) 2019/941[36] a nariadenia Európskeho parlamentu a Rady (EÚ) 2017/1938[37];

   c) akékoľvek riziká vyplývajúce zo závislostí medzi odvetviami uvedenými v prílohe, a to aj z iných členských štátov a tretích krajín, a vplyv, ktorý môže mať narušenie v jednom odvetví na iné odvetvia;

   d) akékoľvek informácie o incidentoch oznámených v súlade s článkom 13.

---

34 Smernica Európskeho parlamentu a Rady (EÚ) 2017/541 z 15. marca 2017 o boji proti terorizmu, ktorou sa nahrádza rámcové rozhodnutie Rady 2002/475/SVV a mení rozhodnutie Rady 2005/671/SVV (Ú. v. EÚ L 88, 31.3.2017, s. 6).

35 Rozhodnutie Európskeho parlamentu a Rady č. 1313/2013/EÚ zo 17. decembra 2013 o mechanizme Únie v oblasti civilnej ochrany (Ú. v. EÚ L 347, 20.12.2013, s. 924).

36 Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/941 z 5. júna 2019 o pripravenosti na riziká v sektore elektrickej energie a o zrušení smernice 2005/89/ES (Ú. v. EÚ L 158, 14.6.2019, s. 1).

37 Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/1938 z 25. októbra 2017 o opatreniach na zaistenie bezpečnosti dodávok plynu a o zrušení nariadenia (EÚ) č. 994/2010 (Ú. v. EÚ L 280, 28.10.2017, s. 1).

Na účely prvého pododseku písm. c) členské štáty podľa potreby spolupracujú s príslušnými orgánmi iných členských štátov a tretích krajín.

3. Členské štáty sprístupnia relevantné prvky posúdenia rizika uvedeného v odseku 1 kritickým subjektom, ktoré identifikovali v súlade s článkom 5, s cieľom pomôcť im pri vykonávaní ich posúdenia rizika podľa článku 10 a pri prijímaní opatrení na zabezpečenie ich odolnosti podľa článku 11.

4. Každý členský štát poskytne Komisii údaje o typoch zistených rizík a výsledkoch posúdení rizík podľa odvetví a pododvetví uvedených v prílohe do [troch rokov od nadobudnutia účinnosti tejto smernice] a následne v prípade potreby a aspoň každé štyri roky.

5. Komisia môže v spolupráci s členskými štátmi vypracovať dobrovoľný spoločný vzor na podávanie správ na účely dosiahnutia súladu s odsekom 4.

Článok 5
Identifikácia kritických subjektov

1. Do [troch rokov a troch mesiacov od nadobudnutia účinnosti tejto smernice] členské štáty identifikujú kritické subjekty pre každé odvetvie a pododvetvie uvedené v prílohe, okrem tých, ktoré sú uvedené v bodoch 3, 4 a 8 prílohy.

2. Pri identifikácii kritických subjektov podľa odseku 1 členské štáty zohľadňujú výsledky posúdenia rizika podľa článku 4 a uplatňujú tieto kritériá:

   a) subjekt poskytuje jednu alebo viac základných služieb;

   b) poskytovanie tejto služby závisí od infraštruktúry nachádzajúcej sa v členskom štáte a

   c) incident by mal závažný rušivý vplyv na poskytovanie služby alebo iných základných služieb v odvetviach uvedených v prílohe, ktoré závisia od služby.

3. Každý členský štát zostaví zoznam identifikovaných kritických subjektov a zabezpečí, aby bolo týmto kritickým subjektom oznámené, že boli identifikované ako kritické subjekty do jedného mesiaca od tejto identifikácie, pričom ich informuje o ich povinnostiach podľa kapitol II a III a o dni, od ktorého sa na ne vzťahujú ustanovenia uvedených kapitol.

   Ustanovenia tejto kapitoly sa na dotknuté kritické subjekty uplatňujú odo dňa oznámenia a ustanovenia kapitoly III sa na ne začnú uplatňovať šesť mesiacov po tomto dni.

4. Členské štáty zabezpečia, aby ich príslušné orgány určené podľa článku 8 tejto smernice oznámili príslušným orgánom, ktoré členské štáty určili v súlade s článkom 8 [smernice o kybernetickej bezpečnosti], totožnosť subjektov identifikovaných ako kritické subjekty podľa tohto článku, a to do jedného mesiaca od tejto identifikácie.

5. Po oznámení uvedenom v odseku 3 členské štáty zabezpečia, aby kritické subjekty poskytovali svojim príslušným orgánom určeným podľa článku 8 tejto smernice

informácie o tom, či boli identifikované ako kritický subjekt v jednom alebo vo viacerých iných členských štátoch. Ak dva alebo viaceré členské štáty identifikovali subjekt ako kritický, tieto členské štáty navzájom konzultujú s cieľom znížiť zaťaženie kritického subjektu, pokiaľ ide o povinnosti podľa kapitoly III.

6. Na účely kapitoly IV členské štáty zabezpečia, aby kritické subjekty po oznámení uvedenom v odseku 3 poskytovali svojim príslušným orgánom určeným podľa článku 8 tejto smernice informácie o tom, či poskytujú základné služby do viac ako tretiny členských štátov, resp. vo viac ako tretine členských štátov. V takom prípade dotknutý členský štát bez zbytočného odkladu oznámi Komisii totožnosť týchto kritických subjektov.

7. Členské štáty v prípade potreby a v každom prípade aspoň každé štyri roky preskúmajú a v náležitých prípadoch aktualizujú zoznam identifikovaných kritických subjektov.

Ak tieto aktualizácie vedú k identifikácii ďalších kritických subjektov, uplatňujú sa odseky 3, 4, 5 a 6. Členské štáty okrem toho zabezpečia, aby subjektom, ktoré už nie sú identifikované ako kritické subjekty podľa ktorejkoľvek takejto aktualizácie, bola táto skutočnosť oznámená a aby boli informované o tom, že od prijatia takejto informácie už nepodliehajú povinnostiam podľa kapitoly III.

Článok 6
Závažný rušivý vplyv

1. Pri určovaní závažnosti rušivého vplyvu uvedeného v článku 5 ods. 2 písm. c) členské štáty zohľadňujú tieto kritériá:

a) počet používateľov využívajúcich službu, ktorú poskytuje subjekt;

b) závislosť iných odvetví uvedených v prílohe od tejto služby;

c) vplyv, ktorý by mohli mať incidenty z hľadiska rozsahu a trvania na hospodárske a spoločenské činnosti, životné prostredie a verejnú bezpečnosť;

d) trhový podiel subjektu na trhu s takýmito službami;

e) geografická oblasť, ktorú by incident mohol ovplyvniť, vrátane akýchkoľvek cezhraničných vplyvov;

f) význam subjektu z hľadiska zachovania dostatočnej úrovne služby berúc do úvahy dostupnosť alternatívnych spôsobov poskytovania danej služby.

2. Členské štáty predložia Komisii do [troch rokov a troch mesiacov od nadobudnutia účinnosti tejto smernice] tieto informácie:

a) zoznam služieb uvedený v článku 4 ods. 1;

b) počet kritických subjektov identifikovaných pre každé odvetvie a pododvetvie uvedené v prílohe a službu alebo služby podľa článku 4 ods. 1, ktoré každý subjekt poskytuje;

c) akékoľvek prahové hodnoty použité na určenie jedného alebo viacerých kritérií uvedených v odseku 1.

Následne tieto informácie poskytujú v prípade potreby a aspoň každé štyri roky.

3. Komisia môže po konzultácii so skupinou pre odolnosť kritických subjektov prijať usmernenia na uľahčenie uplatňovania kritérií uvedených v odseku 1, pričom zohľadní informácie uvedené v odseku 2.

Článok 7
Subjekty rovnocenné kritickým subjektom podľa tejto kapitoly

1. Pokiaľ ide o odvetvia uvedené v bodoch 3, 4 a 8 prílohy, členské štáty do [troch rokov a troch mesiacov od nadobudnutia účinnosti tejto smernice] identifikujú subjekty, s ktorými sa na účely tejto kapitoly zaobchádza ako s rovnocennými kritickým subjektom. Vo vzťahu k týmto subjektom uplatňujú ustanovenia článkov 3, 4, článku 5 ods. 1 až 4 a 7 a článku 9.

2. Pokiaľ ide o subjekty v odvetviach uvedených v bodoch 3 a 4 prílohy, identifikované podľa odseku 1, členské štáty zabezpečia, aby na účely uplatňovania článku 8 ods. 1 boli za príslušné orgány určené tie orgány, ktoré boli za príslušné orgány určené podľa článku 41 [nariadenia DORA].

3. Členské štáty zabezpečia, aby subjekty uvedené v odseku 1 boli bez zbytočného odkladu informované o ich identifikácii ako subjektov uvedených v tomto článku.

Článok 8
Príslušné orgány a miesto jednotného kontaktu

1. Každý členský štát určí jeden alebo viac príslušných orgánov zodpovedných za správne uplatňovanie a v prípade potreby presadzovanie pravidiel tejto smernice na vnútroštátnej úrovni (ďalej len „príslušný orgán“). Členské štáty môžu určiť existujúci orgán alebo orgány.

Ak určia viac ako jeden orgán, jasne stanovia príslušné úlohy dotknutých orgánov a zabezpečia účinnú spoluprácu týchto orgánov pri plnení ich úloh podľa tejto smernice, a to aj pokiaľ ide o určenie a činnosti miesta jednotného kontaktu uvedeného v odseku 2.

2. Každý členský štát určí v rámci príslušného orgánu miesto jednotného kontaktu na plnenie styčnej funkcie s cieľom zabezpečiť cezhraničnú spoluprácu s príslušnými orgánmi iných členských štátov a so skupinou pre odolnosť kritických subjektov uvedenou v článku 16 (ďalej len „miesto jednotného kontaktu“).

3. Do [troch rokov a šiestich mesiacov od nadobudnutia účinnosti tejto smernice] a potom každý rok predložia miesta jednotného kontaktu Komisii a skupine pre odolnosť kritických subjektov súhrnnú správu o prijatých oznámeniach vrátane počtu

oznámení, povahy oznámených incidentov a opatrení prijatých v súlade s článkom 13 ods. 3.

4. Každý členský štát zabezpečí, aby príslušný orgán vrátane miesta jednotného kontaktu, ktoré je v rámci neho určené, mal právomoci a primerané finančné, ľudské a technické zdroje na účinné a efektívne vykonávanie úloh, ktoré mu boli zverené.

5. Členské štáty zabezpečia, aby ich príslušné orgány vždy, keď je to vhodné a v súlade s právom Únie a vnútroštátnym právom, konzultovali a spolupracovali s inými príslušnými vnútroštátnymi orgánmi, najmä tými, ktoré sú zodpovedné za civilnú ochranu, presadzovanie práva a ochranu osobných údajov, ako aj s príslušnými zainteresovanými stranami vrátane kritických subjektov.

6. Členské štáty zabezpečia, aby ich príslušné orgány určené podľa tohto článku spolupracovali s príslušnými orgánmi určenými podľa [smernice o kybernetickej bezpečnosti] v oblasti kybernetických rizík a kybernetických incidentov ovplyvňujúcich kritické subjekty, ako aj pokiaľ ide o opatrenia prijaté príslušnými orgánmi určenými podľa [smernice o kybernetickej bezpečnosti] relevantné pre kritické subjekty.

7. Každý členský štát oznámi Komisii určenie príslušného orgánu a miesta jednotného kontaktu do troch mesiacov od tohto určenia vrátane ich presných úloh a zodpovedností podľa tejto smernice, ich kontaktných údajov a všetkých ich následných zmien. Každý členský štát zverejní určenie príslušného orgánu a miesta jednotného kontaktu.

8. Komisia uverejní zoznam miest jednotného kontaktu členských štátov.

Článok 9
Podpora členských štátov pre kritické subjekty

1. Členské štáty podporujú kritické subjekty pri zvyšovaní ich odolnosti. Táto podpora môže zahŕňať vypracúvanie poradenského materiálu a metodiky, podporu v súvislosti s organizovaním cvičení na testovanie ich odolnosti a poskytovanie odbornej prípravy zamestnancom kritických subjektov.

2. Členské štáty zabezpečia, aby príslušné orgány spolupracovali a vymieňali si informácie a osvedčené postupy s kritickými subjektmi pôsobiacimi v odvetviach uvedených v prílohe.

3. Členské štáty zavedú nástroje na výmenu informácií na podporu dobrovoľnej výmeny informácií medzi kritickými subjektmi v súvislosti so záležitosťami, na ktoré sa vzťahuje táto smernica, a to v súlade s právom Únie a vnútroštátnym právom týkajúcim sa najmä hospodárskej súťaže a ochrany osobných údajov.

KAPITOLA III
ODOLNOSŤ KRITICKÝCH SUBJEKTOV

Článok 10
Posúdenie rizika kritickými subjektmi

Členské štáty zabezpečia, aby kritické subjekty posúdili do šiestich mesiacov od prijatia oznámenia uvedeného v článku 5 ods. 3 a následne v prípade potreby a aspoň každé štyri roky na základe posúdenia rizík členských štátov a iných relevantných informačných zdrojov všetky relevantné riziká, ktoré môžu narušiť prevádzku kritických subjektov.

V posúdení rizika sa zohľadňujú všetky relevantné riziká uvedené v článku 4 ods. 1, ktoré by mohli viesť k narušeniu poskytovania základných služieb. Zohľadní sa v ňom akákoľvek závislosť iných odvetví uvedených v prílohe od základnej služby, ktorú poskytuje kritický subjekt, a to v prípade potreby aj v susedných členských štátoch a tretích krajinách, a vplyv, ktorý môže mať narušenie poskytovania základných služieb v jednom alebo vo viacerých z týchto odvetví na základnú službu poskytovanú kritickým subjektom.

Článok 11
Opatrenia kritických subjektov na zabezpečenie odolnosti

1. Členské štáty zabezpečia, aby kritické subjekty prijali vhodné a primerané technické a organizačné opatrenia na zabezpečenie svojej odolnosti vrátane opatrení potrebných na:

   a) predchádzanie vzniku incidentov, a to aj prostredníctvom opatrení na znižovanie rizika katastrof a adaptáciu na zmenu klímy;

   b) zabezpečenie primeranej fyzickej ochrany citlivých oblastí, zariadení a inej infraštruktúry vrátane oplotenia, bariér, nástrojov a postupov monitorovania bezpečnostnej zóny, ako aj detekčného vybavenia a kontrol prístupu;

   c) odolávanie incidentom a zmierňovanie ich následkov vrátane vykonávania postupov a protokolov riadenia rizík a krízového riadenia a postupov spojených s bezpečnostnými varovaniami;

   d) zotavenie sa z incidentov vrátane opatrení na zabezpečenie kontinuity činností a identifikácie alternatívnych dodávateľských reťazcov;

   e) zabezpečenie primeraného riadenia bezpečnosti zamestnancov, a to aj stanovením kategórií pracovníkov vykonávajúcich kritické funkcie, stanovením prístupových práv k citlivým oblastiam, zariadeniam a inej infraštruktúre a k citlivým informáciám, ako aj určením osobitných kategórií zamestnancov so zreteľom na článok 12;

   f) zvyšovanie informovanosti príslušných pracovníkov o opatreniach uvedených v písmenách a) až e).

2. Členské štáty zabezpečia, aby kritické subjekty mali zavedený a uplatňovali plán odolnosti alebo rovnocenný dokument či dokumenty, v ktorých podrobne opíšu opatrenia podľa odseku 1. Ak kritické subjekty prijali opatrenia v súlade s povinnosťami obsiahnutými v iných aktoch práva Únie, ktoré sú relevantné aj pre opatrenia uvedené v odseku 1, opíšu tieto opatrenia aj v pláne odolnosti alebo v rovnocennom dokumente či dokumentoch.

3. Komisia na žiadosť členského štátu, ktorý identifikoval kritický subjekt, a so súhlasom dotknutého kritického subjektu organizuje poradné misie v súlade s mechanizmami stanovenými v článku 15 ods. 4, 5, 7 a 8 s cieľom poskytovať poradenstvo dotknutému kritickému subjektu pri plnení jeho povinností podľa kapitoly III. Poradná misia podáva správy o svojich zisteniach Komisii, uvedenému členskému štátu a dotknutému kritickému subjektu.

4. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 21, ktorými sa dopĺňa odsek 1, a to stanovením podrobných pravidiel spresňujúcich niektoré alebo všetky opatrenia, ktoré sa majú prijať podľa uvedeného odseku. Tieto delegované akty prijme, pokiaľ je to potrebné na účinné a konzistentné uplatňovanie uvedeného odseku v súlade s cieľmi tejto smernice, pričom zohľadní akýkoľvek relevantný vývoj v oblasti rizík, technológií alebo poskytovania dotknutých služieb, ako aj všetky osobitosti týkajúce sa konkrétnych odvetví a typov subjektov.

5. Komisia prijme vykonávacie akty s cieľom stanoviť potrebné technické a metodické špecifikácie týkajúce sa uplatňovania opatrení uvedených v odseku 1. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 20 ods. 2.

Článok 12
Previerky osôb

1. Členské štáty zabezpečia, aby kritické subjekty mohli predkladať žiadosti o previerku osôb, ktoré patria do určitých osobitných kategórií ich zamestnancov, vrátane osôb, u ktorých sa zvažuje prijatie do zamestnanie na pozície patriace do týchto kategórií, a aby tieto žiadosti urýchlene posúdili orgány príslušné na vykonávanie takýchto previerok osôb.

2. V súlade s uplatniteľným právom Únie a vnútroštátnym právom vrátane nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 [38]sa previerka osôb uvedená v odseku 1 zameria na:

   a) potvrdenie totožnosti osoby na základe listinného dôkazu;

   b) na všetky záznamy vedené v registri trestov za najmenej päť predchádzajúcich rokov a najviac desať rokov, a to o trestných činoch relevantných pre prijatie do zamestnania na konkrétnu pozíciu v členskom štáte alebo členských štátoch, ktorých je osoba štátnym príslušníkom, a v ktoromkoľvek členskom štáte alebo tretej krajine pobytu počas tohto obdobia;

[38] Ú. v. EÚ L 119, 4.5.2016, s. 1.

c) predchádzajúce zamestnania, vzdelávanie a akékoľvek medzery vo vzdelávaní alebo zamestnaní v životopise osoby, a to aspoň počas predchádzajúcich piatich rokov a najviac desiatich rokov.

Pokiaľ ide o prvý pododsek písm. b), členské štáty zabezpečia, aby ich orgány príslušné na vykonávanie previerok osôb získali prostredníctvom systému ECRIS informácie o záznamoch vedených v registroch trestov od iných členských štátov v súlade s postupmi stanovenými v rámcovom rozhodnutí Rady 2009/315/SVV a prípadne v nariadení Európskeho parlamentu a Rady (EÚ) 2019/816[39]. Ústredné orgány uvedené v článku 3 uvedeného rámcového rozhodnutia a v článku 3 ods. 5 uvedeného nariadenia poskytnú odpovede na žiadosti o takéto informácie do 10 pracovných dní odo dňa prijatia žiadosti.

3. V súlade s uplatniteľným právom Únie a vnútroštátnym právom vrátane nariadenia (EÚ) 2016/679 každý členský štát zabezpečí, aby sa na základe riadne odôvodnenej žiadosti kritického subjektu mohla rozšíriť previerka osoby uvedená v odseku 1 aj tak, aby sa využili spravodajské informácie a akékoľvek iné objektívne dostupné informácie, ktoré môžu byť potrebné na určenie vhodnosti dotknutej osoby pracovať na pozícii, v súvislosti s ktorou kritický subjekt požiadal o rozšírenú previerku osoby.

Článok 13
Oznamovanie incidentov

1. Členské štáty zabezpečia, aby kritické subjekty bez zbytočného odkladu oznamovali príslušnému orgánu incidenty, ktoré významne narúšajú alebo môžu významne narušiť ich prevádzku. Oznámenia obsahujú všetky dostupné informácie potrebné na to, aby príslušný orgán mohol pochopiť povahu, príčinu a možné dôsledky incidentu, a to aj s cieľom určiť prípadný cezhraničný vplyv incidentu. Takéto oznámenie nesmie mať pre kritický subjekt za následok vyššiu zodpovednosť.

2. S cieľom určiť závažnosť narušenia alebo potenciálneho narušenia prevádzky kritického subjektu vyplývajúceho z incidentu sa zohľadňujú najmä tieto parametre:

   a) počet používateľov postihnutých narušením alebo potenciálnym narušením;

   b) trvanie narušenia alebo predpokladané trvanie potenciálneho narušenia;

   c) geografické územie ovplyvnené narušením alebo potenciálnym narušením.

3. Na základe informácií poskytnutých v oznámení kritickým subjektom príslušný orgán prostredníctvom svojho miesta jednotného kontaktu informuje miesta jednotného kontaktu ostatných dotknutých členských štátov, ak incident má alebo môže mať významný vplyv na kritické subjekty a kontinuitu poskytovania základných služieb v jednom alebo vo viacerých iných členských štátoch.

   Miesta jednotného kontaktu pritom v súlade s právom Únie alebo vnútroštátnymi právnymi predpismi, ktoré sú v súlade s právom Únie, zaobchádzajú s informáciami

[39] Ú. v. EÚ L 135, 22.5.2019, s. 1.

spôsobom, ktorý rešpektuje ich dôvernosť a chráni bezpečnosť a obchodné záujmy dotknutého kritického subjektu.

4. Príslušný orgán čo najskôr po oznámení v súlade s odsekom 1 poskytne oznamujúcemu kritickému subjektu relevantné informácie týkajúce sa následných opatrení v nadväznosti na jeho oznámenie vrátane informácií, ktoré by mohli podporiť účinnú reakciu kritického subjektu na incident.

KAPITOLA IV
OSOBITNÝ DOHĽAD NAD KRITICKÝMI SUBJEKTMI OSOBITNÉHO EURÓPSKEHO VÝZNAMU

Článok 14
Kritické subjekty osobitného európskeho významu

1. Kritické subjekty osobitného európskeho významu podliehajú osobitnému dohľadu v súlade s touto kapitolou.

2. Subjekt sa považuje za kritický subjekt osobitného európskeho významu, ak bol identifikovaný ako kritický subjekt a poskytuje základné služby do viac ako tretiny členských štátov, resp. vo viac ako tretine členských štátov, a bol ako taký oznámený Komisii podľa článku 5 ods. 1 a 6.

3. Komisia po prijatí oznámenia podľa článku 5 ods. 6 bez zbytočného odkladu oznámi dotknutému subjektu, že sa považuje za kritický subjekt osobitného európskeho významu, a informuje tento subjekt o jeho povinnostiach podľa tejto kapitoly a o dni, od ktorého sa na neho tieto povinnosti vzťahujú.

Ustanovenia tejto kapitoly sa uplatňujú na kritický subjekt osobitného európskeho významu odo dňa prijatia uvedeného oznámenia.

Článok 15
Osobitný dohľad

1. Na žiadosť jedného alebo viacerých členských štátov alebo Komisie členský štát, v ktorom sa nachádza infraštruktúra kritického subjektu osobitného európskeho významu, informuje spolu s týmto subjektom Komisiu a skupinu pre odolnosť kritických subjektov o výsledku posúdenia rizika vykonaného podľa článku 10 a o opatreniach prijatých v súlade s článkom 11.

Uvedený členský štát rovnako bez zbytočného odkladu informuje Komisiu a skupinu pre odolnosť kritických subjektov o akýchkoľvek opatreniach v oblasti dohľadu alebo presadzovania vrátane všetkých posúdení dodržiavania povinností podľa tejto povinnosti alebo vydaných príkazov, ktoré jeho príslušný orgán realizoval v súvislosti s týmto subjektom podľa článkov 18 a 19.

2. Komisia na žiadosť jedného alebo viacerých členských štátov, resp. z vlastného podnetu, a na základe dohody s členským štátom, v ktorom sa nachádza infraštruktúra kritického subjektu osobitného európskeho významu, zorganizuje poradnú misiu s cieľom posúdiť opatrenia zavedené týmto subjektom na účely splnenia jeho povinností podľa kapitoly III. Poradné misie môžu v prípade potreby požiadať o osobitnú expertízu v oblasti riadenia rizika katastrof prostredníctvom Koordinačného centra pre reakcie na núdzové situácie.

3. Poradná misia oznámi svoje zistenia Komisii, skupine pre odolnosť kritických subjektov a kritickému subjektu osobitného európskeho významu do troch mesiacov od ukončenia poradnej misie.

   Skupina pre odolnosť kritických subjektov analyzuje správu a v prípade potreby poskytuje Komisii poradenstvo o tom, či si príslušný kritický subjekt osobitného európskeho významu plní svoje povinnosti podľa kapitoly III, a ak je to vhodné, aké opatrenia by sa mohli prijať na zlepšenie odolnosti tohto subjektu.

   Komisia na základe uvedeného odporúčania oznámi svoje stanoviská členskému štátu, v ktorom sa nachádza infraštruktúra tohto subjektu, skupine pre odolnosť kritických subjektov a predmetnému subjektu k tomu, či si tento subjekt plní svoje povinnosti podľa kapitoly III, a ak je to vhodné, aké opatrenia by sa mohli prijať na zlepšenie odolnosti tohto subjektu.

   Uvedený členský štát náležite zohľadní tieto stanoviská a poskytne Komisii a skupine pre odolnosť kritických subjektov informácie o všetkých opatreniach, ktoré prijal na základe predmetného oznámenia.

4. Každá poradná misia pozostáva z expertov z členských štátov a zo zástupcov Komisie. Členské štáty môžu navrhnúť kandidátov, ktorí majú byť súčasťou poradnej misie. Komisia vyberá a vymenúva členov každej poradnej misie podľa ich odbornej spôsobilosti a zabezpečuje geograficky vyvážené zastúpenie medzi členskými štátmi. Komisia znáša náklady spojené s účasťou na poradnej misii.

   Komisia organizuje program poradnej misie po porade s členmi konkrétnej poradnej misie a po dohode s členským štátom, v ktorom sa nachádza infraštruktúra kritického subjektu alebo kritického subjektu európskeho významu.

5. Komisia prijme vykonávací akt, v ktorom stanoví pravidlá týkajúce sa procedurálnych mechanizmov na účely realizácie poradných misií a podávania správ o týchto misiách. Tento vykonávací akt sa prijme v súlade s postupom preskúmania uvedeným v článku 20 ods. 2.

6. Členské štáty zabezpečia, aby príslušný kritický subjekt osobitného európskeho významu poskytol poradnej misii prístup ku všetkým informáciám, systémom a zariadeniam súvisiacim s poskytovaním jeho základných služieb potrebných na plnenie jeho úloh.

7. Poradná misia sa vykonáva v súlade s uplatniteľným vnútroštátnym právom členského štátu, v ktorom sa táto infraštruktúra nachádza.

8. Pri organizovaní poradných misií Komisia zohľadní správy o všetkých inšpekciách vykonaných Komisiou podľa nariadenia (ES) č. 300/2008 a nariadenia (ES)

č. 725/2004 a správy o akomkoľvek monitorovaní vykonanom Komisiou podľa smernice 2005/65/ES, pokiaľ ide o kritický subjekt alebo kritický subjekt osobitného európskeho významu.

KAPITOLA V
SPOLUPRÁCA A PODÁVANIE SPRÁV

Článok 16
Skupina pre odolnosť kritických subjektov

1. Skupina pre odolnosť kritických subjektov sa zriaďuje s účinnosťou od [šiestich mesiacov po nadobudnutí účinnosti tejto smernice]. Podporuje Komisiu a uľahčuje strategickú spoluprácu a výmenu informácií o otázkach týkajúcich sa tejto smernice.

2. Skupina pre odolnosť kritických subjektov sa skladá zo zástupcov členských štátov a Komisie. Ak je to relevantné pre plnenie jej úloh, skupina pre odolnosť kritických subjektov môže vyzvať zástupcov zainteresovaných strán, aby sa zúčastnili na jej práci.

   Skupine pre odolnosť kritických subjektov predsedá zástupca Komisie.

3. Skupina pre odolnosť kritických subjektov má tieto úlohy:

   a) podporovať Komisiu v rámci pomoci členským štátom pri posilňovaní ich schopnosti prispievať k zabezpečeniu odolnosti kritických subjektov v súlade s touto smernicou;

   b) hodnotiť stratégie v oblasti odolnosti kritických subjektov uvedené v článku 3 a určiť najlepšie postupy v súvislosti s týmito stratégiami;

   c) uľahčiť výmenu najlepších postupov, pokiaľ ide o identifikáciu kritických subjektov členskými štátmi v súlade s článkom 5, a to aj pokiaľ ide o cezhraničné závislosti a riziká a incidenty;

   d) prispievať na požiadanie k príprave usmernení uvedených v článku 6 ods. 3 a akýchkoľvek delegovaných a vykonávacích aktov podľa tejto smernice;

   e) každoročne preskúmavať súhrnné správy uvedené v článku 8 ods. 3;

   f) uskutočňovať výmenu najlepších postupov v oblasti výmeny informácií týkajúcich sa oznamovania incidentov uvedených v článku 13;

   g) analyzovať správy poradných misií a poskytovať k nim poradenstvo v súlade s článkom 15 ods. 3;

   h) uskutočňovať výmenu informácií a najlepších postupov v oblasti výskumu a vývoja v súvislosti s odolnosťou kritických subjektov v súlade s touto smernicou;

i) vo vhodných prípadoch uskutočňovať výmenu informácií v otázkach týkajúcich sa odolnosti kritických subjektov s príslušnými inštitúciami, orgánmi, úradmi a agentúrami Únie.

4. Skupina pre odolnosť kritických subjektov do [24 mesiacov od nadobudnutia účinnosti tejto smernice] a potom každé dva roky vypracuje pracovný program obsahujúci opatrenia, ktoré sa majú realizovať na účely vykonávania jej cieľov a úloh, a ktorý musí byť v súlade s požiadavkami a cieľmi tejto smernice.

5. Skupina pre odolnosť kritických subjektov zasadá pravidelne a aspoň raz ročne sa schádza so skupinou pre spoluprácu zriadenou podľa [smernice o kybernetickej bezpečnosti] s cieľom podporiť strategickú spoluprácu a výmenu informácií.

6. Komisia môže prijať vykonávacie akty stanovujúce procesné mechanizmy potrebné na fungovanie skupiny pre odolnosť kritických subjektov. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 20 ods. 2.

7. Komisia poskytne skupine pre odolnosť kritických subjektov súhrnnú správu o informáciách poskytnutých členskými štátmi podľa článku 3 ods. 3 a článku 4 ods. 4 do [troch rokov a šiestich mesiacov po nadobudnutí účinnosti tejto smernice] a následne v prípade potreby a aspoň každé štyri roky.

Článok 17
Podpora Komisie príslušným orgánom a kritickým subjektom

1. Komisia tam, kde je to vhodné, podporuje členské štáty a kritické subjekty pri plnení ich povinností podľa tejto smernice, a to najmä vypracovaním prehľadu cezhraničných a medziodvetvových rizík spojených s poskytovaním základných služieb na úrovni Únie, organizovaním poradných misií uvedených v článku 11 ods. 3 a článku 15 ods. 3 a uľahčovaním výmeny informácií medzi expertmi v celej Únii.

2. Komisia dopĺňa činnosti členských štátov uvedené v článku 9 vypracovaním najlepších postupov a metodík a rozvojom cezhraničných činností a cvičení odbornej prípravy s cieľom otestovať odolnosť kritických subjektov.

KAPITOLA VI
DOHĽAD A PRESADZOVANIE

Článok 18
Vykonávanie a presadzovanie

1. Členské štáty s cieľom posúdiť, či subjekty nimi identifikované ako kritické subjekty podľa článku 5 dodržiavajú povinnosti podľa tejto smernice, zabezpečia, aby príslušné orgány mali právomoci a prostriedky na:

a) uskutočňovanie kontrol na mieste v priestoroch, ktoré kritický subjekt využíva na poskytovanie svojich základných služieb, a na dohľad na diaľku nad opatreniami kritických subjektov podľa článku 11;

b) vykonávanie alebo nariaďovanie auditov vo vzťahu k týmto subjektom.

2. Členské štáty zabezpečia, aby príslušné orgány mali právomoci a prostriedky, ktoré im umožnia požadovať, ak je to potrebné na plnenie ich úloh podľa tejto smernice, aby subjekty, ktoré identifikovali ako kritické subjekty podľa odseku 5, v primeranej lehote stanovenej týmito orgánmi poskytli:

a) informácie potrebné na posúdenie toho, či opatrenia prijaté týmito subjektmi na zabezpečenie ich odolnosti spĺňajú požiadavky článku 11;

b) dôkaz o účinnom vykonávaní týchto opatrení vrátane výsledkov auditu vykonaného nezávislým a kvalifikovaným audítorom vybraným týmto subjektom a vykonaným na jeho náklady.

Pri požadovaní týchto informácií príslušný orgán uvedie účel požiadavky a druh informácií, ktoré sa požadujú.

3. Bez toho, aby bola dotknutá možnosť uložiť sankcie v súlade s článkom 19, príslušné orgány môžu na základe opatrení dohľadu uvedených v odseku 1 alebo na základe posúdenia informácií uvedených v odseku 2 nariadiť dotknutým kritickým subjektom, aby v primeranej lehote stanovenej týmito orgánmi prijali potrebné a primerané opatrenia na nápravu akéhokoľvek zisteného porušenia tejto smernice a aby týmto orgánom poskytli informácie o prijatých opatreniach. V týchto príkazoch sa zohľadní najmä závažnosť porušenia.

4. Členský štát zabezpečí, aby sa právomoci stanovené v odsekoch 1, 2 a 3 mohli vykonávať len pod podmienkou primeraných záruk. Tieto záruky zaručujú najmä to, aby sa vykonávanie právomocí uskutočňovalo objektívnym, transparentným a primeraným spôsobom a aby boli riadne chránené práva a oprávnené záujmy dotknutých kritických subjektov vrátane ich práva na vypočutie, obhajobu a účinný prostriedok nápravy pred nezávislým súdom.

5. Členské štáty zabezpečia, že keď príslušný orgán posudzuje podľa tohto článku, či kritický subjekt dodržiava povinnosti podľa tejto smernice, informuje o tom príslušné orgány dotknutého členského štátu určené podľa [smernice o kybernetickej bezpečnosti] a že tieto orgány môže požiadať o posúdenie kybernetickej bezpečnosti takéhoto subjektu, ako aj o to, aby na tento účel spolupracovali a vymieňali si informácie.

Článok 19
Sankcie

Členské štáty stanovia pravidlá, pokiaľ ide o sankcie uplatniteľné pri porušení vnútroštátnych ustanovení prijatých podľa tejto smernice, a prijmú všetky opatrenia potrebné na zabezpečenie ich uplatňovania. Stanovené sankcie musia byť účinné, primerané a odrádzajúce. Členské štáty oznámia tieto ustanovenia Komisii najneskôr do [dvoch rokov

od nadobudnutia účinnosti tejto smernice] a bezodkladne jej oznámia každú nasledujúcu zmenu, ktorá sa ich dotkne.

KAPITOLA VII
ZÁVEREČNÉ USTANOVENIA

Článok 20
Postup výboru

1. Komisii pomáha výbor. Uvedený výbor je výborom v zmysle nariadenia (EÚ) č. 182/2011.

2. Ak sa odkazuje na tento odsek, uplatňuje sa článok 5 nariadenia (EÚ) č. 182/2011.

Článok 21
Vykonávanie delegovania právomoci

1. Komisii sa udeľuje právomoc prijímať delegované akty za podmienok stanovených v tomto článku.

2. Právomoc prijímať delegované akty uvedené v článku 11 ods. 4 sa Komisii udeľuje na obdobie piatich rokov od dátumu nadobudnutia účinnosti tejto smernice alebo akéhokoľvek iného dátumu stanoveného spoluzákonodarcami.

3. Delegovanie právomocí uvedené v článku 11 ods. 4 môže Európsky parlament alebo Rada kedykoľvek odvolať. Rozhodnutím o odvolaní sa ukončuje delegovanie právomoci, ktorá sa v ňom uvádza. Rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie* alebo k neskoršiemu dátumu, ktorý je v ňom určený. Nie je ním dotknutá platnosť delegovaných aktov, ktoré už nadobudli účinnosť.

4. Komisia pred prijatím delegovaného aktu konzultuje s odborníkmi určenými jednotlivými členskými štátmi v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva.

5. Komisia oznamuje delegovaný akt hneď po prijatí súčasne Európskemu parlamentu a Rade.

6. Delegovaný akt prijatý podľa článku 11 ods. 4 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote dvoch mesiacov odo dňa oznámenia uvedeného aktu Európskemu parlamentu a Rade alebo ak pred uplynutím uvedenej lehoty Európsky parlament a Rada informovali Komisiu o svojom rozhodnutí nevzniesť námietku. Na podnet Európskeho parlamentu alebo Rady sa táto lehota predĺži o dva mesiace.

Článok 22
Podávanie správ a preskúmanie

Komisia do [54 mesiacov po nadobudnutí účinnosti tejto smernice] predloží Európskemu parlamentu a Rade správu, v ktorej sa posúdi rozsah, v akom členské štáty prijali potrebné opatrenia na dosiahnutie súladu s touto smernicou.

Komisia pravidelne skúma fungovanie tejto smernice a podáva o tom správu Európskemu parlamentu a Rade. V správe sa posúdi najmä vplyv a pridaná hodnota tejto smernice na zabezpečenie odolnosti kritických subjektov a to, či by sa rozsah pôsobnosti smernice nemal rozšíriť tak, aby sa vzťahoval aj na iné odvetvia alebo pododvetvia. Prvá správa sa predloží do [šiestich rokov od nadobudnutia účinnosti tejto smernice] a posúdi sa v nej najmä to, či by sa rozsah pôsobnosti smernice nemal rozšíriť tak, aby zahŕňal odvetvie výroby, spracovania a distribúcie potravín.

Článok 23
Zrušenie smernice 2008/114/ES

Smernica 2008/114/ES sa týmto zrušuje s účinnosťou odo [dňa nadobudnutia účinnosti tejto smernice].

Článok 24
Transpozícia

1. Členské štáty prijmú a uverejnia zákony, iné právne predpisy a správne opatrenia potrebné na dosiahnutie súladu s touto smernicou najneskôr do [18 mesiacov po nadobudnutí účinnosti tejto smernice]. Komisii bezodkladne oznámia znenie týchto ustanovení.

   Tieto ustanovenia začnú uplatňovať po uplynutí [dvoch rokov a jedného dňa od nadobudnutia účinnosti tejto smernice].

   Členské štáty uvedú priamo v prijatých ustanoveniach alebo pri ich úradnom uverejnení odkaz na túto smernicu. Podrobnosti o odkaze upravia členské štáty.

2. Členské štáty oznámia Komisii znenie hlavných ustanovení vnútroštátnych právnych predpisov, ktoré prijmú v oblasti pôsobnosti tejto smernice.

Článok 25
Nadobudnutie účinnosti

Táto smernica nadobúda účinnosť dvadsiatym dňom po jej uverejnení v *Úradnom vestníku Európskej únie*.

Článok 26
Adresáti

Táto smernica je určená členským štátom.

V Bruseli

Za Európsky parlament
predseda

Za Radu
predseda

LEGISLATÍVNY FINANČNÝ VÝKAZ

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

SMERNICA EURÓPSKEHO PARLAMENTU A RADY

o odolnosti kritických subjektov

1.2. Príslušné oblasti politiky

Bezpečnosť

1.3. Návrh/iniciatíva sa týka:

☐ **novej akcie**

☐ **novej akcie, ktorá nadväzuje na pilotný projekt/prípravnú akciu**[40]

☑ **predĺženia trvania existujúcej akcie**

☐ **zlúčenia jednej alebo viacerých akcií do ďalšej/novej akcie alebo presmerovania jednej alebo viacerých akcií na ďalšiu/novú akciu**

1.4. Ciele

1.4.1. Všeobecné ciele

Prevádzkovatelia kritickej infraštruktúry poskytujú služby vo viacerých odvetviach (ako je doprava, energetika, zdravotníctvo, vodné hospodárstvo atď.), ktoré sú nevyhnutné pre životne dôležité spoločenské funkcie a hospodárske činnosti. Prevádzkovatelia preto musia byť odolní, t. j. dobre chránení, ale takisto schopní rýchlo obnoviť prevádzku v prípade narušenia.

Všeobecným cieľom návrhu je zvýšiť odolnosť týchto prevádzkovateľov (ďalej len „kritické subjekty“) voči celej škále prírodných a ľudskou činnosťou zapríčinených, úmyselných či neúmyselných rizík.

1.4.2. Špecifické ciele

Cieľom iniciatívy je zamerať sa na štyri špecifické ciele:

– zabezpečiť lepšie pochopenie rizík a vzájomných závislostí, ktorým čelia kritické subjekty, ako aj prostriedky na ich riešenie,

– zabezpečiť, aby orgány členských štátov označili všetky príslušné subjekty ako „kritické subjekty“,

[40] Podľa článku 58 ods. 2 písm. a) alebo b) nariadenia o rozpočtových pravidlách.

– zabezpečiť, aby sa do verejných politík a prevádzkovej praxe zahrnulo celé spektrum činností na zvýšenie odolnosti,

– posilniť kapacity a zlepšiť spoluprácu a komunikáciu medzi zainteresovanými stranami.

Tieto ciele prispejú k dosiahnutiu všeobecného cieľa iniciatívy.

1.4.3. Očakávané výsledky a vplyv

Uveďte, aký vplyv by mal mať návrh/iniciatíva na prijímateľov/cieľové skupiny.

Očakáva sa, že iniciatíva bude mať pozitívny vplyv na bezpečnosť kritických subjektov, ktoré by sa mali stať odolnejšími voči rizikám a narušeniam. Mali by byť schopné lepšie zmierňovať riziká, riešiť potenciálne narušenia a minimalizovať negatívne vplyvy v prípadoch, keď dôjde k incidentu.

Lepšia odolnosť kritických subjektov takisto znamená, že ich prevádzka bude spoľahlivejšia a ich služby v mnohých životne dôležitých odvetviach budú poskytované konzistentným spôsobom, čo prispeje k bezproblémovému fungovaniu vnútorného trhu. To bude mať zase pozitívny vplyv na širokú verejnosť a podniky, keďže sa na tieto služby spoliehajú pri svojej každodennej činnosti.

Bezproblémové fungovanie kľúčových hospodárskych činností a nepretržité poskytovanie základných služieb občanom by malo predstavovať prínos aj pre verejné orgány.

1.4.4. Ukazovatele výkonnosti

Uveďte ukazovatele na monitorovanie pokroku a dosiahnutých výsledkov.

Ukazovatele na monitorovanie pokroku a dosiahnutých výsledkov budú prepojené so špecifickými cieľmi iniciatívy:

– počet a rozsah posúdení rizík vykonaných orgánmi a kritickými subjektmi bude ukazovateľom lepšieho pochopenia rizík zo strany kľúčových aktérov,

– počet „kritických subjektov“ identifikovaných členskými štátmi bude odrážať komplexnosť pokrytia politík kritickej infraštruktúry,

– začleňovanie odolnosti do verejných politík a prevádzkovej praxe sa odrazí v národných stratégiách a opatreniach kritických subjektov na zabezpečenie odolnosti,

– zlepšenia, pokiaľ ide o kapacity a spoluprácu, sa budú posudzovať na základe činností zameraných na budovanie kapacít a vyvinutých iniciatív spolupráce.

1.5. Dôvody návrhu/iniciatívy

1.5.1. Potreby, ktoré sa majú uspokojiť v krátkodobom alebo dlhodobom horizonte vrátane podrobného harmonogramu prvotnej fázy vykonávania iniciatívy

Aby členské štáty splnili požiadavky iniciatívy, budú musieť v krátkodobom až strednodobom horizonte vypracovať stratégiu v oblasti odolnosti kritických subjektov, vykonať vnútroštátne posúdenie rizík a na základe výsledkov posúdenia rizík a konkrétnych kritérií identifikovať, ktorí prevádzkovatelia sú „kritickými subjektmi“. Tieto činnosti sa budú vykonávať pravidelne podľa potreby a aspoň raz za štyri roky. Členské štáty budú musieť takisto vytvoriť mechanizmy spolupráce medzi príslušnými zainteresovanými stranami.

Od prevádzkovateľov označených ako „kritické subjekty“ by sa malo vyžadovať, aby v krátkodobom až strednodobom horizonte vykonali vlastné posúdenie rizík, prijali vhodné a primerané technické a organizačné opatrenia na zabezpečenie ich odolnosti a aby informovali príslušné orgány o incidentoch.

1.5.2. Prínos zapojenia Únie (môže byť výsledkom rôznych faktorov, napr. lepšej koordinácie, právnej istoty, väčšej účinnosti alebo komplementárnosti). Na účely tohto bodu je „prínos zapojenia Únie“ hodnota vyplývajúca zo zásahu Únie, ktorá dopĺňa hodnotu, ktorú by inak vytvorili len samotné členské štáty.

Dôvody na akciu na európskej úrovni (ex-ante):

Cieľom tejto iniciatívy je zvýšiť odolnosť kritických subjektov voči rôznym rizikám. Tento cieľ nemožno uspokojivo dosiahnuť na úrovni členských štátov: opatrenie EÚ je odôvodnené spoločnou povahou rizík, ktorým čelia kritické subjekty, nadnárodným charakterom služieb, ktoré poskytujú, a vzájomnou závislosťou a prepojením medzi nimi (naprieč odvetviami a hranicami). Znamená to, že zraniteľnosť alebo narušenie jednej štruktúry má potenciál spôsobiť narušenie naprieč odvetviami a hranicami.

Očakávaný prínos vytvorený Úniou (ex-post):

V porovnaní so súčasnou situáciou prinesie navrhovaná iniciatíva pridanú hodnotu, a to najmä:

– vytvorením všeobecného rámca, ktorý by podporil lepšie zosúladenie politík členských štátov (konzistentný rozsah pôsobnosti naprieč odvetviami, kritériá na označenie kritických subjektov, spoločné požiadavky, pokiaľ ide o posudzovanie rizík),

– zaistením toho, že kritické subjekty prijmú primerané opatrenia na zabezpečenie odolnosti,

– spájaním poznatkov a odborných znalostí z celej EÚ, ktoré by mali optimalizovať reakciu kritických subjektov a orgánov,

– znížením rozdielov medzi členskými štátmi a zvýšením odolnosti kritických subjektov v celej Európskej únii.

1.5.3. Poznatky získané z podobných skúseností v minulosti

Návrh vychádza zo skúseností získaných pri vykonávaní smernice o európskych kritických infraštruktúrach (smernica 2008/114/ES) a jej hodnotenia [SWD(2019) 308].

1.5.4. Zlučiteľnosť s viacročným finančným rámcom a možná synergia s inými vhodnými nástrojmi

Tento návrh je jedným zo základných prvkov novej Stratégie EÚ pre bezpečnostnú úniu zameranej na dosiahnutie nadčasového bezpečnostného prostredia.

Je možné vytvoriť synergie s mechanizmom Únie v oblasti civilnej ochrany, pokiaľ ide o predchádzanie katastrofám, ich zmierňovanie a riadenie.

1.6. Trvanie a finančný vplyv návrhu/iniciatívy

☐ **obmedzené trvanie**

☐ v platnosti od [DD/MM]RRRR do [DD/MM]RRRR

☐ Finančný vplyv na viazané rozpočtové prostriedky od RRRR do RRRR a na platobné rozpočtové prostriedky od RRRR do RRRR.

☑ **neobmedzené trvanie**

- Počiatočná fáza vykonávania bude trvať od roku 2021 do roku 2027,
- a potom bude implementácia pokračovať v plnom rozsahu.

1.7. Plánovaný spôsob riadenia[41]

☑ **Priame riadenie** na úrovni Komisie

☑ prostredníctvom jej útvarov vrátane zamestnancov v delegáciách Únie

☐ prostredníctvom výkonných agentúr

☑ **Zdieľané riadenie** s členskými štátmi

☐ **Nepriame riadenie**, pri ktorom sa plnením rozpočtu poveria:

☐ tretie krajiny alebo subjekty, ktoré tieto krajiny určili,

☐ medzinárodné organizácie a ich agentúry (uveďte),

☐ Európska investičná banka (EIB) a Európsky investičný fond,

☐ subjekty uvedené v článkoch 70 a 71 nariadenia o rozpočtových pravidlách,

☐ verejnoprávne subjekty,

☐ súkromnoprávne subjekty poverené vykonávaním verejnej služby, pokiaľ tieto subjekty poskytujú dostatočné finančné záruky,

☐ súkromnoprávne subjekty spravované právom členského štátu, ktoré sú poverené vykonávaním verejno-súkromného partnerstva a ktoré poskytujú dostatočné finančné záruky,

☐ osoby poverené vykonávaním osobitných činností v oblasti SZBP podľa hlavy V Zmluvy o Európskej únii a určené v príslušnom základnom akte.

V prípade viacerých spôsobov riadenia uveďte v oddiele „Poznámky“ presnejšie vysvetlenie.

---

41 Vysvetlenie spôsobov riadenia a odkazy na nariadenie o rozpočtových pravidlách sú k dispozícii na webovej stránke BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Poznámky:

Priame riadenie bude v prvom rade zahŕňať: administratívne výdavky Generálneho riaditeľstva pre migráciu a vnútorné záležitosti (ďalej len „GR HOME“), administratívnu dohodu so Spoločným výskumným centrom, granty riadené Komisiou.

Zdieľané riadenie bude zahŕňať: Projekty v rámci zdieľaného riadenia: Členské štáty budú musieť vypracovať stratégiu a posúdenie rizík a na tieto účely môžu použiť svoje vnútroštátne finančné balíky.

2. OPATRENIA V OBLASTI RIADENIA

2.1. Opatrenia týkajúce sa monitorovania a predkladania správ

Uveďte časový interval a podmienky, ktoré sa vzťahujú na tieto opatrenia.

Podľa návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa ako súčasť Fondu pre vnútornú bezpečnosť zriaďuje nástroj Únie určený pre oblasť bezpečnosti [COM(2018) 472 final]:

Zdieľané riadenie:

Každý členský štát zavedie pre svoj program systémy riadenia a kontroly a zabezpečí kvalitu a spoľahlivosť monitorovacieho systému a údajov o ukazovateľoch v súlade s nariadením o spoločných ustanoveniach (NSU). S cieľom uľahčiť rýchle začatie vykonávania je možné „previesť“ existujúce dobre fungujúce systémy riadenia a kontroly do ďalšieho programového obdobia.

V tejto súvislosti budú členské štáty požiadané o zriadenie monitorovacieho výboru, v ktorom bude Komisia zastávať poradnú funkciu. Monitorovací výbor sa stretne najmenej jedenkrát ročne. Bude preskúmavať všetky otázky, ktoré majú vplyv na pokrok programu smerom k dosiahnutiu jeho cieľov.

Členské štáty zašlú výročnú správu o výkonnosti, v ktorej by mali uviesť informácie o pokroku pri vykonávaní programu a dosahovaní cieľov a zámerov. Správa by mala takisto poukázať na akékoľvek problémy, ktoré ovplyvňujú výkonnosť programu, a opísať opatrenia prijaté na ich riešenie.

Na konci obdobia každý členský štát predloží záverečnú správu o výkonnosti. Záverečná správa by sa mala zamerať na pokrok dosiahnutý pri plnení cieľov programu a mala by poskytnúť prehľad o kľúčových problémoch, ktoré ovplyvnili výkonnosť programu, opatreniach prijatých na riešenie týchto problémov a hodnotení účinnosti týchto opatrení. Okrem toho by mala uvádzať príspevok programu k riešeniu výziev uvedených v príslušných odporúčaniach EÚ adresovaných členskému štátu, pokrok pri dosahovaní cieľov stanovených vo výkonnostnom rámci, zistenia príslušných hodnotení a následné opatrenia prijaté v nadväznosti na tieto zistenia a výsledky komunikačných opatrení.

Podľa návrhu všeobecného nariadenia členské štáty každoročne zasielajú balík uisťujúcich dokumentov, ktorý zahŕňa ročnú účtovnú závierku, vyhlásenie riadiaceho subjektu a stanoviská orgánu auditu k účtovnej závierke, k výročnej kontrolnej správe v zmysle článku 92 ods. 1 písm. d) všeobecného nariadenia, k systému riadenia a kontroly a k zákonnosti a správnosti výdavkov deklarovaných v ročnej účtovnej závierke. Komisia použije tento balík uisťujúcich dokumentov na určenie sumy hradenej z fondu za účtovný rok.

Každé dva roky sa zorganizuje hodnotiace stretnutie medzi Komisiou a každým členským štátom s cieľom preskúmať výkonnosť jednotlivých programov.

Členské štáty zasielajú šesťkrát za rok údaje za každý program rozčlenené podľa špecifických cieľov. Tieto údaje sa týkajú nákladov na operácie a hodnôt spoločných ukazovateľov výstupov a výsledkov.

Vo všeobecnosti:

Komisia vykoná hodnotenie v polovici trvania a spätné hodnotenie akcií implementovaných v rámci tohto fondu v súlade s nariadením o spoločných ustanoveniach. Hodnotenie v polovici trvania by malo byť založené najmä na hodnotení programov v polovici trvania, ktoré členské štáty predložia Komisii do 31. decembra 2024.

2.2. Systémy riadenia a kontroly

2.2.1. Opodstatnenie navrhovaných spôsobov riadenia, mechanizmov vykonávania financovania, spôsobov platby a stratégie kontroly

Podľa návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa ako súčasť Fondu pre vnútornú bezpečnosť zriaďuje nástroj Únie určený pre oblasť bezpečnosti [COM(2018) 472 final]:

Z *ex-post* hodnotení týkajúcich sa fondov GR HOME na obdobie 2007 – 2013, ako aj z priebežných hodnotení súčasných fondov GR HOME, vyplýva, že kombinácia spôsobov čerpania fondov v oblasti migrácie a vnútorných záležitostí umožnila vytvoriť účinný postup, ako dosiahnuť ciele fondov. Ucelený návrh mechanizmov plnenia sa zachováva a zahŕňa zdieľané, priame a nepriame riadenie.

Prostredníctvom zdieľaného riadenia členské štáty realizujú programy, ktoré prispievajú k cieľom politiky Únie, ktoré sú prispôsobené ich vnútroštátnemu kontextu. Zdieľané riadenie zabezpečuje, že finančná podpora je k dispozícii vo všetkých zúčastnených štátoch. Zdieľané riadenie okrem toho umožňuje predvídať financovanie a členským štátom, ktoré sú najlepšie oboznámené s výzvami, ktorým čelia, umožňuje, aby zodpovedajúcim spôsobom plánovali svoje dlhodobé príspevky. Novým prvkom je, že z fondu sa môže poskytovať okrem priameho a nepriameho riadenia aj núdzová pomoc prostredníctvom zdieľaného riadenia.

Prostredníctvom priameho riadenia Komisia podporuje ďalšie akcie, ktoré prispievajú k spoločným cieľom politiky Únie. Vďaka týmto akciám možno poskytovať prispôsobenú podporu pre naliehavé a osobitné potreby v jednotlivých členských štátoch („núdzovú pomoc“), podporovať nadnárodné siete a činnosti, testovať inovatívne činnosti, ktoré by sa mohli rozšíriť v rámci národných programov, a uskutočňovať štúdie v záujme Únie ako celku („akcie Únie“).

Prostredníctvom nepriameho riadenia si fond ponecháva možnosť delegovať úlohy súvisiace s plnením rozpočtu okrem iného na medzinárodné organizácie a agentúry pre vnútorné záležitosti na osobitné účely.

Vzhľadom na rôzne ciele a potreby sa v rámci fondu navrhuje tematický nástroj, aby sa zabezpečila rovnováha medzi predvídateľnosťou viacročného prideľovania finančných prostriedkov pre národné programy a flexibilitou pravidelného vyplácania finančných prostriedkov na akcie s vysokou pridanou hodnotou pre Úniu.

Tematický nástroj sa použije na konkrétne akcie v členských štátoch a naprieč nimi, akcie Únie a núdzovú pomoc. Zabezpečí sa ním, aby sa finančné prostriedky mohli prideľovať a presúvať medzi rôznymi uvedenými spôsobmi riadenia na základe dvojročného programovania.

Spôsoby platby v rámci zdieľaného riadenia sú opísané v návrhu všeobecného nariadenia, v ktorom sa stanovuje ročná zálohová platba, po ktorej nasledujú maximálne štyri priebežné platby na program a rok na základe žiadostí o platbu, ktoré členské štáty predložili počas účtovného roka. Podľa návrhu všeobecného nariadenia sa zálohová platba zúčtuje v rámci posledného účtovného roka programov.

Stratégia kontrol bude vychádzať z nového nariadenia o rozpočtových pravidlách a zo všeobecného nariadenia. Novým nariadením o rozpočtových pravidlách a návrhom všeobecného nariadenia by sa malo rozšíriť využívanie zjednodušených foriem grantov, ako sú napríklad jednorazové platby, paušálne sadzby a jednotkové náklady. Namiesto nákladov sa zavádzajú aj nové formy platieb na základe dosiahnutých výsledkov. Prijímatelia budú môcť získať fixnú sumu prostriedkov, ak preukážu, že sa uskutočnili určité akcie, ako napr. odborná príprava alebo poskytnutie humanitárnej pomoci. Očakáva sa, že sa tým zjednoduší zaťaženie spojenej s kontrolami, a to na úrovni prijímateľov aj na úrovni členských štátov (napr. kontrola nákladov vykazovaných na faktúrach a potvrdenkách).

Pokiaľ ide o zdieľané riadenie, návrh všeobecného nariadenia vychádza zo stratégie riadenia a kontroly zavedenej v programovom období 2014 – 2020, ale zavádzajú sa ním niektoré opatrenia zamerané na zjednodušenie vykonávania a zníženie záťaže spojenej s kontrolami na úrovni prijímateľov aj členských štátov. Tieto nové prvky zahŕňajú:

– odstránenie postupu označovania (čo by malo umožniť urýchlenie vykonávania programov),

– overovanie zo strany riadiaceho orgánu (administratívne kontroly a kontroly na mieste), ktoré má vykonať riadiaci orgán na základe rizík (v porovnaní so 100 % administratívnych kontrol požadovaných v programovom období 2014 – 2020). Riadiace orgány môžu navyše za určitých podmienok uplatňovať primerané kontrolné opatrenia v súlade s vnútroštátnymi postupmi,

– podmienky na zabránenie viacnásobným auditom tej istej operácie/výdavkov.

Programové orgány predložia Komisii žiadosti o priebežné platby založené na výdavkoch, ktoré vynaložili prijímatelia. Návrh všeobecného nariadenia umožňuje riadiacim orgánom vykonávať overovanie zo strany riadiaceho orgánu na základe rizík a stanovujú sa v ňom aj osobitné kontroly (napr. kontroly na mieste zo strany riadiaceho orgánu a audity operácií/výdavkov zo strany orgánu auditu) po tom, čo boli súvisiace výdavky vykázané Komisii v žiadostiach o priebežnú platbu. S cieľom znížiť riziko úhrady neoprávnených výdavkov sa v návrhu všeobecného nariadenia stanovuje limit pre priebežné platby Komisie vo výške 90 %, keďže v tejto chvíli sa vykonala iba časť vnútroštátnych kontrol. Komisia uhradí zvyšný zostatok po schválení účtov a po doručení balíka uisťujúcich dokumentov od orgánov zodpovedných za programy. Akékoľvek nezrovnalosti zistené Komisiou

alebo Európskym dvorom audítorov po postúpení ročného balíka uisťujúcich dokumentov môžu viesť k čistej finančnej oprave.

V prípade časti vykonávanej prostredníctvom **priameho riadenia** v rámci tematického nástroja bude systém riadenia a kontroly vychádzať zo skúseností získaných v rokoch 2014 – 2020 v rámci akcií Únie aj núdzovej pomoci Únie. Vytvorí sa zjednodušená schéma, ktorá umožní rýchle spracovanie žiadostí o financovanie a súčasne zníži riziko chýb: oprávnenými žiadateľmi budú len členské štáty a medzinárodné organizácie, financovanie bude založené na zjednodušenom vykazovaní nákladov, vytvoria sa štandardné vzory pre žiadosti o financovanie, dohody o grantoch/príspevkoch a predkladanie správ a stály hodnotiaci výbor bude posudzovať žiadosti hneď po ich doručení.

2.2.2. Informácie o zistených rizikách a systémoch vnútornej kontroly zavedených na ich zmierňovanie

Generálne riaditeľstvo pre migráciu a vnútorné záležitosti sa vo svojich výdavkových programoch nestretlo so závažnými rizikami chybovosti. Potvrdzuje to aj opakujúca absencia významných zistení vo výročných správach Dvora audítorov.

V rámci zdieľaného riadenia sa všeobecné riziká v súvislosti s vykonávaním súčasných programov týkajú nedostatočného čerpania prostriedkov z fondu členskými štátmi a možných chýb vyplývajúcich zo zložitosti pravidiel a nedostatkov v systémoch riadenia a kontroly. Návrh všeobecného nariadenia zjednodušuje regulačný rámec tým, že sa ním harmonizujú pravidlá a systémy riadenia a kontroly rôznych fondov, z ktorých sa čerpajú finančné prostriedky v rámci zdieľaného riadenia. Takisto sa ním zjednodušujú požiadavky na kontrolu (napr. overovanie zo strany riadiaceho orgánu na základe rizík, možnosť primeraných kontrolných mechanizmov založených na vnútroštátnych postupoch, obmedzenia audítorskej činnosti z hľadiska načasovania a/alebo konkrétnych operácií).

2.2.3. Odhad a opodstatnenie nákladovej účinnosti kontrol (pomer medzi nákladmi na kontroly a hodnotou súvisiacich riadených finančných prostriedkov) a posúdenie očakávaných úrovní rizika chyby (pri platbe a uzavretí)

Komisia uvádza pomer medzi „nákladmi na kontroly a hodnotou súvisiacich riadených finančných prostriedkov“. Vo výročnej správe o činnosti GR HOME za rok 2019 sa uvádza pomer 0,72 %, pokiaľ ide o zdieľané riadenie, 1,31 %, pokiaľ ide o granty v rámci priameho riadenia a 6,05 %, pokiaľ ide o verejné obstarávanie v rámci priameho riadenia. Pokiaľ ide o zdieľané riadenie, tento percentuálny podiel sa zvyčajne časom so zvýšením efektívnosti pri vykonávaní programov a zvýšením platieb členským štátom znižuje.

Predpokladá sa, že s prístupom k riadeniu a kontrolám založeným na rizikách, ktorý sa zavádza v návrhu všeobecného nariadenia, spolu so zvýšeným úsilím o prijímanie zjednodušených možností vykazovania nákladov, sa náklady na kontroly pre členské štáty budú naďalej znižovať.

Vo výročnej správe o činnosti za rok 2019 sa uvádza kumulatívna zvyšková chybovosť vo výške 1,57 % v prípade národných programov AMIF/ISF

a kumulatívna zvyšková chybovosť vo výške 4,11 % v prípade grantov nesúvisiacich s výskumom v rámci priameho riadenia.

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

Uveďte existujúce a plánované preventívne a ochranné opatrenia, napr. zo stratégie na boj proti podvodom.

Generálne riaditeľstvo pre migráciu a vnútorné záležitosti bude pokračovať v uplatňovaní svojej stratégie pre boj proti podvodom v súlade so stratégiou Komisie pre boj proti podvodom, aby okrem iného zabezpečilo, že jeho vnútorné kontroly súvisiace s bojom proti podvodom sú v plnom súlade so stratégiou Komisie pre boj proti podvodom a že jeho prístup k riadeniu rizík v oblasti boja proti podvodom je zameraný na identifikáciu oblastí, v ktorých existuje riziko podvodu, a na primerané reakcie.

Pokiaľ ide o zdieľané riadenie, členské štáty zabezpečia zákonnosť a správnosť výdavkov uvedených v účtovných závierkach, ktoré predkladajú Komisii. V tejto súvislosti členské štáty prijmú všetky potrebné opatrenia na predchádzanie nezrovnalostiam, ich odhaľovanie a nápravu. Podobne ako v súčasnom programovom cykle 2014 – 2020 sú členské štáty povinné zaviesť postupy na odhaľovanie nezrovnalostí a na boj proti podvodom v spojení s osobitným delegovaným nariadením Komisie o oznamovaní nezrovnalostí. Opatrenia na boj proti podvodom budú pre členské štáty naďalej prierezovou zásadou a povinnosťou.

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

1. Nové rozpočtové riadky

V poradí, v akom za sebou nasledujú okruhy viacročného finančného rámca a rozpočtové riadky.

Okruh viacročného finančného rámca	Rozpočtový riadok	Druh výdavkov	Príspevky			
	Okruh č. 5: Odolnosť, bezpečnosť a obrana	DRP/NRP [42]	krajín EZVO[43]	kandidátskych krajín[44]	tretích krajín	v zmysle článku 21 ods. 2 písm. b) nariadenia o rozpočtových pravidlách
5	12 02 01 – „Fond pre vnútornú bezpečnosť“	DRP	NIE	NIE	ÁNO	NIE
5	12 01 01 – Podporné výdavky pre „Fond pre vnútornú bezpečnosť“	NRP	NIE	NIE	ÁNO	NIE

Poznámka:

Treba poznamenať, že operačné rozpočtové prostriedky požadované v súvislosti s návrhom sú pokryté rozpočtovými prostriedkami, ktoré sú už stanovené vo VZPS, z ktorého vychádza nariadenie o Fonde pre vnútornú bezpečnosť.

V kontexte tohto legislatívneho návrhu sa požadujú dodatočné ľudské zdroje.

42 DRP = diferencované rozpočtové prostriedky / NRP = nediferencované rozpočtové prostriedky.
43 EZVO: Európske združenie voľného obchodu.
44 Kandidátske krajiny a prípadne potenciálni kandidáti zo západného Balkánu.

3.2. Odhadovaný finančný vplyv návrhu na rozpočtové prostriedky

3.2.1. Zhrnutie odhadovaného vplyvu na operačné rozpočtové prostriedky

☐ Návrh/iniciatíva si nevyžaduje použitie operačných rozpočtových prostriedkov.

☑ Návrh/iniciatíva si vyžaduje použitie operačných rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Okruh viacročného finančného rámca	5	Odolnosť, bezpečnosť a obrana

GR: HOME			2021	2022	2023	2024	2025	2026	2027	**Po roku 2027**	**SPOLU**
• Operačné rozpočtové prostriedky											
Rozpočtový riadok 12 02 01 Fond pre vnútornú bezpečnosť	Záväzky	(1a)	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Platby	(2a)	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822
Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov[45]											
Rozpočtový riadok		(3)									
Rozpočtové prostriedky pre GR HOME **SPOLU**	Záväzky	= 1a + 1b + 3	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Platby	= 2a + 2b	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822

[45] Technická a/alebo administratívna pomoc a výdavky určené na financovanie vykonávania programov a/alebo akcií Európskej únie (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

		+3									

• Operačné rozpočtové prostriedky SPOLU	Záväzky	(4)									
	Platby	(5)									
• Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov SPOLU		(6)									
Rozpočtové prostriedky OKRUHU 5 viacročného finančného rámca **SPOLU**	Záväzky	= 4 + 6	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Platby	= 5 + 6	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822

Ak má návrh/iniciatíva vplyv na viaceré operačné okruhy, zopakujte oddiel uvedený vyššie:

• Operačné rozpočtové prostriedky SPOLU (všetky operačné okruhy)	Záväzky	(4)									
	Platby	(5)									
Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov SPOLU (všetky operačné okruhy)		(6)									
Rozpočtové prostriedky OKRUHOV 1 až 6 viacročného finančného rámca **SPOLU** (referenčná suma)	Záväzky	= 4 + 6	0,124	4,348	5,570	6,720	7,020	7,020	7,020		37,822
	Platby	= 5 + 6	0,540	4,323	5,357	5,403	5,403	5,403	5,403	5,989	37,822

Okruh viacročného finančného rámca	**7**	„Administratívne výdavky“

Tento oddiel sa vyplní s použitím rozpočtových údajov administratívnej povahy, ktoré budú po prvýkrát uvedené v prílohe k legislatívnemu finančnému výkazu (príloha V k interným predpisom), ktorá je nahraná do DECIDE na účely medziútvarovej konzultácie.

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		2021	2022	2023	2024	2025	2026	2027	**SPOLU**
GR: HOME									
• Ľudské zdroje		0,152	0,228	0,499	0,813	0,932	0,932	0,932	**4,488**
• Ostatné administratívne výdavky		0,033	0,085	0,109	0,109	0,109	0,109	0,109	**0,663**
GR HOME **SPOLU**	Rozpočtové prostriedky	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,151**

Rozpočtové prostriedky OKRUHU 7 viacročného finančného rámca **SPOLU**	(Záväzky spolu = Platby spolu)	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,151**

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		2021	2022	2023	2024	2025	2026	2027	**Po roku 2027**	**SPOLU**
Rozpočtové prostriedky OKRUHOV 1 až 7 viacročného finančného rámca **SPOLU**	Záväzky	**0,309**	**4,661**	**6,178**	**7,642**	**8,061**	**8,061**	**8,061**	**-**	**42,973**
	Platby	**0,725**	**4,636**	**5,965**	**6,325**	**6,444**	**6,444**	**6,444**	**5,989**	**42,973**

3.2.2. Odhadované výsledky financované z operačných rozpočtových prostriedkov

viazané rozpočtové prostriedky v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Uveďte ciele a výstupy ⇩	Druh	Priemerné náklady	Rok 2021		Rok 2022		Rok 2023		Rok 2024		Rok 2025		Rok 2026		Rok 2027		SPOLU	
			Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady
ŠPECIFICKÝ CIEĽ č. 1: Podpora Komisie pre príslušné orgány a kritické subjekty																		
Výstup	Rozvíjanie a udržiavanie poznatkov a podpornej kapacity					2,000		2,000				2,000		2,000		2,000		12,000
Výstup	Podpora príslušných orgánov podporovaním výmeny osvedčených postupov a informácií a vykonávaním posúdení rizík (finančné náklady pokryté ďalej uvedenými štúdiami) a vykonávaním hodnotení úloh																	
Výstup	Podpora príslušných orgánov a kritických subjektov (t. j. prevádzkovateľov) vypracovaním poradenských materiálov a metodík, podporovaním organizácie cvičení, ktoré simulujú scenáre incidentov v reálnom čase, a poskytovaním odbornej prípravy					0,500		0,850		1,200		1,500		1,500		1,500		7,050
Výstup	Projekty na rôzne témy súvisiace s uvedenými podpornými činnosťami (metodiky posudzovania rizík, simulácia scenárov incidentov v reálnom čase)	**0,400**			3	1,200	5	2,000	7	2,800		2,800	7	2,800	7		36	14,400
Výstup	Štúdie (posúdenia rizík) a konzultácie (súvisiace s vykonávaním smernice)	**0,100**			4	0,400	4	0,400	4	0,400	4	0,400	4	0,400	4	0,400	24	2,400
Výstup	Iné stretnutia a konferencie	**0,031**		0,124	8	0,248	8	0,248	8	0,248	8	0,248	8	0,248	8	0,248	52	1,612
Špecifický cieľ č. 1 medzisúčet				0,124		4,348		5,498		6,648		6,948		6,948		6,948		37,462
SPECIFICKY CIEĽ č. 2: Poradné tímy pre odolnosť																		
Výstup	Organizácia poradných tímov pre odolnosť (členovia: zástupcovia členských štátov). Komisia zorganizuje výzvu na účely náboru členov (pre účastnícke členské štáty)																	
Výstup	Komisia zorganizuje program a poradné misie Komisia poskytne poradným misiám podstatné vstupy (usmernenia a dohľad nad kritickými subjektmi európskeho významu – spolu s členskými štátmi) Každodenná koordinácia poradných tímov pre odolnosť							0,072		0,072		0,072		0,072		0,072		0,360
Špecifický cieľ č. 2 medzisúčet								0,072		0,072		0,072		0,072		0,072		0,360
Ciele 1 až 2 SPOLU				**0,124**		**4,348**		**5,570**		**6,720**		**7,020**		**7,020**		**7,020**		**37,822**

3.2.3. Zhrnutie odhadovaného vplyvu na administratívne rozpočtové prostriedky

☐ Návrh/iniciatíva si nevyžaduje použitie administratívnych rozpočtových prostriedkov

☑ Návrh/iniciatíva si vyžaduje použitie administratívnych rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	2021	2022	2023	2024	2025	2026	2027	SPOLU
OKRUH 7 viacročného finančného rámca								
Ľudské zdroje	0,152	0,228	0,499	0,813	0,932	0,932	0,932	4,488
Ostatné administratívne výdavky	0,033	0,085	0,109	0,109	0,109	0,109	0,109	0,663
Medzisúčet OKRUHU 7 viacročného finančného rámca	**0,185**	**0,313**	**0,608**	**0,922**	**1,041**	**1,041**	**1,041**	**5,188**

Mimo OKRUHU 7[46] viacročného finančného rámca								
Ľudské zdroje								
Ostatné administratívne výdavky								
Medzisúčet mimo OKRUHU 7 viacročného finančného rámca								

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

Rozpočtové prostriedky potrebné na ľudské zdroje a na ostatné administratívne výdavky budú pokryté rozpočtovými prostriedkami GR, ktoré už boli pridelené na riadenie akcie a/alebo boli prerozdelené v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu prideľovania zdrojov a v závislosti od rozpočtových obmedzení.

[46] Technická a/alebo administratívna pomoc a výdavky určené na financovanie vykonávania programov a/alebo akcií Európskej únie (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

3.2.3.1. Odhadované potreby ľudských zdrojov

☐ Návrh/iniciatíva si nevyžaduje použitie ľudských zdrojov.

☑ Návrh/iniciatíva si vyžaduje použitie ľudských zdrojov, ako je uvedené v nasledujúcej tabuľke:

odhady sa vyjadrujú v jednotkách ekvivalentu plného pracovného času

		Rok **2021**	Rok **2022**	Rok **2023**	Rok **2024**	2025	2026	2027
• Plán pracovných miest (úradníci a dočasní zamestnanci)								
20 01 02 01 (ústredie a zastúpenia Komisie)		1	2	4	5	5	5	5
XX 01 01 02 (delegácie)								
XX 01 05 01/11/21 (nepriamy výskum)								
10 01 05 01/11 (priamy výskum)								
• Externí zamestnanci (ekvivalent plného pracovného času)[47]								
20 02 01 03 (ZZ, VNE, DAZ z celkového finančného krytia)				1	2	2	2	2
XX 01 02 02 (ZZ, MZ, VNE, DAZ, PED v delegáciách)								
XX 01 04 **yy** [48]	– ústredie							
	– delegácie							
XX 01 05 02/12/22 (ZZ, VNE, DAZ – nepriamy výskum)								
10 01 05 02/12 (ZZ, DAZ, VNE – priamy výskum)								
Iné rozpočtové riadky (uveďte)								
SPOLU		**1**	**2**	**5**	**7**	**7**	**7**	**7**

XX predstavuje príslušnú oblasť politiky alebo rozpočtovú hlavu.

Potreby ľudských zdrojov budú pokryté úradníkmi GR, ktorí už boli pridelení na riadenie akcie a/alebo boli interne prerozdelení v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu prideľovania zdrojov v závislosti od rozpočtových obmedzení.

Opis úloh, ktoré sa majú vykonať:

Úradníci a dočasní zamestnanci	V návrhu sa predpokladá, že na vykonávanie smernice na strane Komisie sa priradia 4 AD a 1 AST, z čoho 1 AD je už interným zamestnancom a zostávajúci ekvivalent plného pracovného času predstavujú dodatočné ľudské zdroje, ktoré je potrebné prijať. V pláne zamestnávania nových pracovníkov sa plánuje prijať: v roku 2022: + 1 AD: odborný referent zodpovedný za vytvorenie vedomostnej kapacity a podporných činností, v roku 2023: + 1 AD (odborný referent zodpovedný za poradné tímy), 1 AST (asistent pre poradné tímy pre odolnosť), v roku 2024: + 1 AD (odborný referent, ktorý prispeje k podporným činnostiam pre orgány a prevádzkovateľov).

47 ZZ = zmluvný zamestnanec; MZ = miestny zamestnanec; VNE = vyslaný národný expert; DAZ = dočasný agentúrny zamestnanec; PED = pomocný expert v delegácii.

48 Čiastkový strop pre externých zamestnancov financovaných z operačných rozpočtových prostriedkov (pôvodné rozpočtové riadky „BA“).

Externí zamestnanci	V návrhu sa predpokladá, že na vykonávanie smernice na strane Komisie sa priradia 2 vyslaní národní experti. V pláne zamestnávania nových pracovníkov sa plánuje prijať: v roku 2023: + 1 VNE (odborník na odolnosť kritickej infraštruktúry, ktorý prispeje k podporným činnostiam pre orgány a prevádzkovateľov), v roku 2024: + 1 VNE (odborník na odolnosť kritickej infraštruktúry, ktorý prispeje k podporným činnostiam pre orgány a prevádzkovateľov).

3.2.4. Súlad s platným viacročným finančným rámcom

Návrh/iniciatíva:

☑ môže byť v plnej miere financovaná prerozdelením v rámci príslušného okruhu viacročného finančného rámca (VFR).

Operačné výdavky pokryté z ISF v rámci VFR na roky 2021 – 2027

☐ si vyžaduje použitie nepridelenej rezervy v rámci príslušného okruhu VFR a/alebo použitie osobitných nástrojov vymedzených v nariadení o VFR.

Vysvetlite potrebu a uveďte príslušné okruhy, rozpočtové riadky, zodpovedajúce sumy a nástroje, ktorých použitie sa navrhuje.

☐ si vyžaduje revíziu VFR.

Vysvetlite potrebu a uveďte príslušné okruhy, rozpočtové riadky a zodpovedajúce sumy.

3.2.5. Príspevky od tretích strán

Návrh/iniciatíva:

☑ nezahŕňa spolufinancovanie tretími stranami

☐ zahŕňa spolufinancovanie tretími stranami, ako je odhadnuté v nasledujúcej tabuľke:

rozpočtové prostriedky v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	Rok **N**[49]	Rok **N + 1**	Rok **N + 2**	Rok **N + 3**	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)			Spolu
Uveďte spolufinancujúci subjekt								
Prostriedky zo spolufinancovania SPOLU								

[49] Rok N je rokom, v ktorom sa návrh/iniciatíva začína vykonávať. Nahraďte „N“ očakávaným prvým rokom vykonávania (napríklad: 2021). To isté urobte aj pri nasledujúcich rokoch.

3.3. Odhadovaný vplyv na príjmy

☑ Návrh/iniciatíva nemá finančný vplyv na príjmy.

☐ Návrh/iniciatíva má finančný vplyv na príjmy, ako je uvedené v nasledujúcej tabuľke:

☐ vplyv na vlastné zdroje

☐ vplyv na iné príjmy

uveďte, či sú príjmy pripísané rozpočtovým riadkom výdavkov ☐

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Rozpočtový riadok príjmov:	Rozpočtové prostriedky k dispozícii v bežnom rozpočtovom roku	Vplyv návrhu/iniciatívy[50]						
		Rok **N**	Rok **N + 1**	Rok **N + 2**	Rok **N + 3**	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)		
Článok …….								

V prípade pripísaných príjmov uveďte príslušné rozpočtové riadky výdavkov.

[…]

Ďalšie poznámky (napr. spôsob/vzorec použitý na výpočet vplyvu na príjmy alebo akékoľvek ďalšie informácie).

[…]

[50] Pokiaľ ide o tradičné vlastné zdroje (clá, odvody z produkcie cukru), uvedené sumy musia predstavovať čisté sumy, t. j. hrubé sumy po odčítaní 20 % na náklady na výber.