EVROPSKA
KOMISIJA

Bruselj, 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Predlog

DIREKTIVA EVROPSKEGA PARLAMENTA IN SVETA

o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148

(Besedilo velja za EGP)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

OBRAZLOŽITVENI MEMORANDUM

1. OZADJE PREDLOGA

• Razlogi za predlog in njegovi cilji

Ta predlog je del svežnja ukrepov za nadaljnje izboljšanje odpornosti javnih in zasebnih subjektov, pristojnih organov in Unije kot celote ter njihovih zmogljivosti za odzivanje na incidente na področju kibernetske varnosti in zaščite kritične infrastrukture. V skladu s prednostnimi nalogami Komisije se mora Evropa prilagoditi digitalni dobi in vzpostaviti gospodarstvo, pripravljeno na prihodnost, ki koristi ljudem. Kibernetska varnost je prednostna naloga pri odzivanju Komisije na krizo zaradi COVID-19. Sveženj vključuje novo strategijo za kibernetsko varnost, namenjeno okrepitvi strateške avtonomije Unije za izboljšanje njene odpornosti in kolektivnega odziva ter vzpostavitev odprtega in globalnega interneta. Nazadnje, sveženj vključuje predlog direktive o odpornosti kritičnih izvajalcev bistvenih storitev, ki je namenjen ublažitvi fizičnih groženj takim izvajalcem.

Ta predlog temelji na Direktivi (EU) 2016/1148 o varnosti omrežij in informacijskih sistemov, ki je prvi zakonodajni akt o kibernetski varnosti, ki se uporablja po vsej EU in določa pravne ukrepe za zvišanje splošne ravni kibernetske varnosti v Uniji, ter jo razveljavlja. Direktiva o varnosti omrežij in informacijskih sistemov je (1) prispevala k izboljšanju zmogljivosti za kibernetsko varnost na nacionalni ravni z zahtevo, naj države članice sprejmejo nacionalne strategije za kibernetsko varnost in imenujejo organe za kibernetsko varnost; (2) povečala sodelovanje med državami članicami na ravni Unije z vzpostavitvijo različnih forumov za olajšanje izmenjave strateških in operativnih informacij ter (3) izboljšala kibernetsko odpornost javnih in zasebnih subjektov v sedmih posebnih sektorjih (energija, promet, bančništvo, infrastrukture finančnih trgov, zdravstveno varstvo, oskrba s pitno vodo in njena distribucija ter digitalne infrastrukture) ter na področju treh digitalnih storitev (spletne tržnice, spletni iskalniki in storitve računalništva v oblaku) z zahtevo, naj države članice zagotovijo, da izvajalci bistvenih storitev in ponudniki digitalnih storitev določijo zahteve glede kibernetske varnosti in poročajo o incidentih.

Predlog posodablja obstoječi pravni okvir ob upoštevanju večje digitalizacije notranjega trga v zadnjih letih in razvijajočega se okolja kibernetskih groženj. Oboje se je od začetka krize zaradi COVID-19 še dodatno okrepilo. Predlog obravnava tudi več pomanjkljivosti, zaradi katerih direktiva o varnosti omrežij in informacijskih sistemov ni mogla v celoti izkoristiti svojega potenciala.

Vendar pa se je za direktivo o varnosti omrežij in informacijskih sistemov, ki je utrla pot do velike spremembe v mišljenju, kar zadeva institucionalni in regulativni pristop h kibernetski varnosti v številnih državah članicah, kljub njenim pomembnim dosežkom izkazalo, da ima omejitve. Z digitalno preobrazbo družbe (ki jo je okrepila kriza zaradi COVID-19) se je okolje groženj razširilo in nastajajo novi izzivi, ki zahtevajo prilagojene in inovativne odzive. Število kibernetskih napadov se še naprej povečuje, z vse bolj izpopolnjenimi napadi iz različnih virov znotraj in zunaj EU.

Pri ocenjevanju delovanja direktive o varnosti omrežij in informacijskih sistemov za namene ocene učinka so bile opredeljene naslednje težave: (1) nizka raven kibernetske odpornosti podjetij, ki delujejo v EU; (2) neskladna odpornost po državah članicah in sektorjih ter (3) nizka raven skupnega situacijskega zavedanja in pomanjkanje skupnega odzivanja na krize. Nekatere večje bolnišnice v državi članici na primer ne spadajo na področje uporabe direktive o varnosti omrežij in informacijskih sistemov, zato jim ni treba izvajati varnostnih ukrepov, ki izhajajo iz nje, medtem ko v drugi državi članici za skoraj vse izvajalce zdravstvene dejavnosti v državi veljajo zahteve glede varnosti omrežij in informacijskih sistemov.

Ker je predlog pobuda v okviru programa ustreznosti in uspešnosti predpisov (REFIT), je namenjen zmanjšanju regulativnega bremena pristojnih organov ter stroškov izpolnjevanja obveznosti javnih in zasebnih subjektov. To je mogoče doseči zlasti z odpravo obveznosti, da pristojni organi določijo izvajalce bistvenih storitev, ter povečanjem stopnje harmonizacije varnostnih zahtev in zahtev glede poročanja za olajšanje regulativne skladnosti subjektov, ki opravljajo čezmejne storitve. Hkrati bo pristojnim organom dodeljenih tudi več novih nalog, vključno z nadzorom subjektov v sektorjih, ki za zdaj niso zajeti z direktivo o varnosti omrežij in informacijskih sistemov.

- **Skladnost z veljavnimi predpisi s področja zadevne politike**

Ta predlog je del širšega sklopa obstoječih pravnih instrumentov in prihodnjih pobud na ravni Unije, namenjenih povečanju odpornosti javnih in zasebnih subjektov proti grožnjam.

Na področju kibernetske varnosti sta to zlasti Direktiva (EU) 2018/1972 o Evropskem zakoniku o elektronskih komunikacijah (njene s kibernetsko varnostjo povezane določbe bodo nadomeščene z določbami tega predloga) in predlog uredbe o digitalni operativni odpornosti za finančni sektor (COM(2020) 595 final), ki se bo štel za *lex specialis* k temu predlogu, ko bosta oba akta začela veljati.

Na področju fizične varnosti predlog dopolnjuje predlog direktive o odpornosti kritičnih subjektov, s katerim se revidira Direktiva 2008/114/ES o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe po izboljšanju njene zaščite (direktiva o evropski kritični infrastrukturi), ki vzpostavlja postopek Unije za ugotavljanje in določanje evropskih kritičnih infrastruktur ter določa pristop za izboljšanje njihove zaščite. Komisija je julija 2020 sprejela strategijo EU za varnostno unijo[1], v kateri sta bili priznani vse večja medsebojna povezanost in odvisnost med fizičnimi in digitalnimi infrastrukturami. V njej je bila poudarjena potreba po bolj usklajenem in doslednem pristopu med direktivo o evropski kritični infrastrukturi in Direktivo (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji.

Predlog je zato natančno usklajen s predlogom direktive o odpornosti kritičnih subjektov, ki je namenjena povečanju odpornosti kritičnih subjektov proti fizičnim grožnjam v številnih sektorjih. Namen predloga je zagotoviti, da pristojni organi v skladu z obema pravnima aktoma sprejmejo dopolnilne ukrepe in si po potrebi izmenjajo informacije v zvezi s kibernetsko in nekibernetsko odpornostjo ter da zlasti za kritične izvajalce v sektorjih, ki se v skladu s tem predlogom štejejo za „bistvene“, veljajo tudi splošnejše obveznosti glede povečanja odpornosti s poudarkom na nekibernetskih tveganjih.

- **Skladnost z drugimi politikami Unije**

Kot je navedeno v sporočilu „Oblikovanje digitalne prihodnosti Evrope“[2], je za Evropo ključnega pomena, da v varnih in etičnih okvirih izkoristi priložnosti, ki jih nudi digitalna doba, ter okrepi svoje industrijske in inovacijske zmogljivosti. Evropska strategija za podatke določa štiri stebre – varstvo podatkov, temeljne pravice, varnost in kibernetsko varnost –, ki so ključni predpogoji za družbo, ki izkorišča moč podatkov.

[1] COM(2020) 605 final.
[2] COM(2020) 67 final.

Evropski parlament je v resoluciji z dne 12. marca 2019 pozval „Komisijo naj oceni, ali je treba področje uporabe direktive o varnosti omrežij in informacijskih sistemov dodatno razširiti na druge kritične sektorje in storitve, ki niso zajeti v posebni zakonodaji za sektor“[3]. Svet je v svojih sklepih z dne 9. junija 2020 pozdravil „načrte Komisije, da zagotovi dosledna pravila za udeležence na trgu ter omogoči varno, zanesljivo in ustrezno izmenjavo informacij o grožnjah in incidentih, med drugim z revizijo direktive o varnosti omrežij in informacijskih sistemov, da bi si tako prizadevali za možnosti za večjo kibernetsko odpornost in učinkovitejše odzive na kibernetske napade, zlasti na bistvene gospodarske in družbene dejavnosti, ob spoštovanju pristojnosti držav članic, tudi njihove odgovornosti za nacionalno varnost“[4]. Poleg tega predlagani pravni akt ne posega v uporabo pravil konkurence, določenih v Pogodbi o delovanju Evropske unije (PDEU).

Glede na to, da ima velik del kibernetskih groženj izvor zunaj EU, je potreben usklajen pristop k mednarodnemu sodelovanju. Ta direktiva je referenčni model, ki ga je treba spodbujati v okviru sodelovanja EU s tretjimi državami, zlasti pri zagotavljanju zunanje tehnične pomoči.

2. PRAVNA PODLAGA, SUBSIDIARNOST IN SORAZMERNOST

• Pravna podlaga

Pravna podlaga direktive o varnosti omrežij in informacijskih sistemov je člen 114 Pogodbe o delovanju Evropske unije, katerega cilj je vzpostavitev in delovanje notranjega trga z okrepitvijo ukrepov za približevanje nacionalnih pravil. Kot je Sodišče Evropske unije razsodilo v sodbi v zadevi C-58/08, Vodafone in drugi, je sklicevanje na člen 114 PDEU upravičeno, kadar obstajajo razlike med nacionalnimi pravili, ki imajo neposreden učinek na delovanje notranjega trga. Sodišče je tudi razsodilo, da če so bile z aktom, ki temelji na členu 114 PDEU, že odstranjene vse ovire pri trgovanju na področju, ki ga usklajuje, to zakonodajalcu Unije ne more preprečiti možnosti, da ta akt prilagodi vsem spremembam okoliščin ali razvoju znanja zaradi njegove naloge varovanja splošnih interesov, določenih s Pogodbo. Nazadnje je Sodišče je razsodilo, da so ukrepi za približevanje iz člena 114 PDEU namenjeni omogočanju polja proste presoje glede metode približevanja, ki je najprimernejša za doseganje želenega rezultata, odvisno od splošnega okvira in posebnih okoliščin področja, ki ga je treba uskladiti. S predlaganim pravnim aktom bi se odpravile ovire za ter izboljšala vzpostavitev in delovanje notranjega trga za bistvene in pomembne subjekte z: določitvijo jasnih splošno veljavnih pravil o področju uporabe direktive o varnosti omrežij in informacijskih sistemov ter harmonizacijo pravil, ki se uporabljajo na področju obvladovanja tveganj za kibernetsko varnost in poročanja o incidentih. Sedanje razlike na tem področju, tako na zakonodajni in nadzorni ravni kot tudi na nacionalni ravni in ravni EU, ovirajo notranji trg, ker se subjekti, ki se ukvarjajo s čezmejnimi dejavnostmi, srečujejo z različnimi in po možnosti prekrivajočimi se regulativnimi zahtevami in/ali njihovo uporabo, kar lahko ovira uresničevanje njihovih pravic do ustanavljanja in opravljanja storitev. Različna pravila negativno vplivajo tudi na pogoje konkurence na notranjem trgu, kar zadeva istovrstne subjekte v različnih državah članicah.

[3] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_SL.html.
[4] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/sl/pdf.

- **Subsidiarnost (za neizključno pristojnost)**

Kibernetska odpornost v Uniji ne more biti učinkovita, če se k njej zaradi nacionalnih ali regionalnih omejitev pristopa neenotno. V direktivi o varnosti omrežij in informacijskih sistemov so te pomanjkljivosti deloma obravnavane z določitvijo okvira za varnost omrežij in informacijskih sistemov na nacionalni ravni in ravni Unije. Vendar pa so se z njenim prenosom in izvajanjem pokazale tudi pomanjkljivosti in omejitve nekaterih določb ali pristopov, kot je nejasna razmejitev področja uporabe Direktive, ki vodi do velikih razlik v obsegu in intenzivnosti dejanskega ukrepanja EU na ravni držav članic. Poleg tega je evropsko gospodarstvo od začetka krize zaradi COVID-19 postalo še bolj odvisno od omrežij in informacijskih sistemov kot kdaj koli prej, sektorji in storitve pa so vse bolj medsebojno povezani. Ukrepanje EU, ki presega sedanje ukrepe iz direktive o varnosti omrežij in informacijskih sistemov, je upravičeno zlasti zaradi: (i) vse bolj čezmejne narave groženj in izzivov, povezanih z varnostjo omrežij in informacijskih sistemov; (ii) možnosti, da se z ukrepi Unije izboljšajo in olajšajo učinkovite in usklajene nacionalne politike, ter (iii) prispevka usklajenih in skupnih ukrepov politike k učinkovitemu varstvu podatkov in zasebnosti.

- **Sorazmernost**

Pravila, predlagana v tej direktivi, ne presegajo tistega, kar je potrebno za zadovoljivo doseganje specifičnih ciljev. Predvidena uskladitev in racionalizacija varnostnih ukrepov in obveznosti poročanja se nanašata na zahteve držav članic in podjetij po izboljšanju sedanjega okvira.

Predlog upošteva obstoječe prakse v državah članicah. Višja raven varstva, dosežena s takimi racionaliziranimi in usklajenimi zahtevami, je sorazmerna z vse večjimi tveganji, vključno s tistimi, ki zajemajo čezmejni element; zahteve so razumne in na splošno ustrezajo interesu subjektov, vključenih v zagotavljanje neprekinjenega izvajanja storitev in njihove kakovosti. Stroški zagotavljanja sistematičnega sodelovanja med državami članicami bi bili nizki v primerjavi z gospodarskimi in družbenimi izgubami ter škodo, ki jo povzročijo kibernetski incidenti. Poleg tega posvetovanja z zainteresiranimi stranmi, opravljena v okviru pregleda direktive o varnosti omrežij in informacijskih sistemov, vključno z rezultati odprtega javnega posvetovanja in ciljno usmerjenih raziskav, kažejo podporo reviziji direktive o varnosti omrežij in informacijskih sistemov v skladu z zgoraj navedenim.

- **Izbira instrumenta**

Predlog bo nadalje racionaliziral obveznosti, naložene podjetjem, in zagotovil višjo stopnjo njihove harmonizacije. Hkrati je predlog namenjen zagotovitvi prožnosti za države članice, ki je potrebna za upoštevanje nacionalnih posebnosti (kot je možnost določitve dodatnih bistvenih ali pomembnih subjektov, kar presega izhodiščni okvir, določen s pravnim aktom). Prihodnji pravni instrument bi zato moral biti direktiva, saj ta pravni instrument omogoča ciljno usmerjeno izboljšano harmonizacijo in določeno stopnjo prožnosti za pristojne organe.

3. REZULTATI NAKNADNIH OCEN, POSVETOVANJ Z ZAINTERESIRANIMI STRANMI IN OCEN UČINKA

- **Naknadne ocene/preverjanja primernosti obstoječe zakonodaje**

Komisija je ocenila delovanje direktive o varnosti omrežij in informacijskih sistemov[5]. Analizirala je njeno ustreznost, dodano vrednost EU, skladnost, uspešnost in učinkovitost. Glavne ugotovitve te analize so:

- Področje uporabe direktive o varnosti omrežij in informacijskih sistemov je preveč omejeno, kar zadeva zajete sektorje, zlasti zaradi: (i) večje digitalizacije v zadnjih letih in višje stopnje medsebojne povezanosti ter (ii) dejstva, da področje uporabe direktive o varnosti omrežij in informacijskih sistemov ne odraža več vseh digitaliziranih sektorjev, ki gospodarstvu in družbi kot celoti zagotavljajo ključne storitve.
- Direktiva o varnosti omrežij in informacijskih sistemov ni dovolj jasna, kar zadeva področje uporabe za izvajalce bistvenih storitev, njene določbe pa ne zagotavljajo zadostne jasnosti v zvezi z nacionalno pristojnostjo glede ponudnikov digitalnih storitev. To je privedlo do stanja, v katerem nekatere vrste subjektov niso bile opredeljene v vseh državah članicah, zaradi česar jim ni treba uvesti varnostnih ukrepov in poročati o incidentih.
- Direktiva o varnosti omrežij in informacijskih sistemov je državam članicam omogočila široko diskrecijsko pravico pri določanju zahtev glede varnosti in poročanja o incidentih za izvajalce bistvenih storitev. Ocena kaže, da so države članice v nekaterih primerih te zahteve izvajale na zelo različne načine, s čimer je bilo ustvarjeno dodatno breme za podjetja, ki delujejo v več kot eni državi članici.
- Ureditev nadzora in izvrševanja iz direktive o varnosti omrežij in informacijskih sistemov je neučinkovita. Države članice so na primer zelo nenaklonjene uporabi sankcij za subjekte, ki ne uvedejo varnostnih zahtev ali ne poročajo o incidentih. To ima lahko negativne posledice za kibernetsko odpornost posameznih subjektov.
- Finančni in človeški viri, ki jih države članice namenijo za opravljanje svojih nalog (kot je določitev ali nadzor izvajalcev bistvenih storitev), ter posledično različne stopnje zrelosti pri obravnavanju tveganj za kibernetsko varnost se zelo razlikujejo. To še bolj poglablja razlike v kibernetski odpornosti med državami članicami.
- Države članice si informacij ne izmenjujejo sistematično, kar ima negativne posledice zlasti za učinkovitost ukrepov za kibernetsko varnost in raven skupnega situacijskega zavedanja na ravni EU. To velja tudi za izmenjavo informacij med zasebnimi subjekti ter sodelovanje med strukturami sodelovanja na ravni EU in zasebnimi subjekti.

- **Posvetovanja z zainteresiranimi stranmi**

Komisija se je posvetovala s številnimi zainteresiranimi stranmi. Države članice in zainteresirane strani so bile pozvane, naj sodelujejo pri odprtem javnem posvetovanju ter v raziskavah in na delavnicah, ki so jih organizirali družba Wavestone, Center za evropske politične študije (CEPS) in družba ICF, od katerih je Komisija naročila izvedbo študije v podporo pregledu direktive o varnosti omrežij in informacijskih sistemov. Med zainteresiranimi stranmi, s katerimi so bila opravljena posvetovanja, so bili pristojni organi,

[5] [Priloga 5 ocene učinka].

organi Unije, ki se ukvarjajo s kibernetsko varnostjo, izvajalci bistvenih storitev, ponudniki digitalnih storitev, subjekti, ki opravljajo storitve, ki ne spadajo na področje uporabe sedanje direktive o varnosti omrežij in informacijskih sistemov, trgovinska združenja in potrošniške organizacije ter državljani.

Poleg tega je bila Komisija v stalnem stiku s pristojnimi organi, zadolženimi za izvajanje direktive o varnosti omrežij in informacijskih sistemov. Skupina za sodelovanje je obširno obravnavala različne medsektorske in sektorske vidike izvajanja. Nazadnje, Komisija je med obiski držav v zvezi z varnostjo omrežij in informacijskih sistemov v obdobju 2019–2020 opravila razgovore s 154 javnimi in zasebnimi subjekti ter 117 pristojnimi organi.

- **Zbiranje in uporaba strokovnih mnenj**

Komisija je sklenila pogodbo s konzorcijem, ki ga sestavljajo družba Wavestone, Center za evropske politične študije in družba ICF, da bi ji zagotavljal podporo pri pregledu direktive o varnosti omrežij in informacijskih sistemov[6]. Izvajalec je s ciljno usmerjenimi raziskavami in delavnicami vzpostavil stik z zainteresiranimi stranmi, ki jih direktiva o varnosti omrežij in informacijskih sistemov neposredno zadeva, poleg tega pa se je posvetoval s številnimi strokovnjaki s področja kibernetske varnosti, kot so raziskovalci kibernetske varnosti in strokovnjaki iz panoge kibernetske varnosti.

- **Ocena učinka**

Temu predlogu je priložena ocena učinka[7], ki je bila 23. oktobra 2020 predložena Odboru za regulativni nadzor, ki je 20. novembra 2020 izdal pozitivno mnenje s pripombami. Odbor za regulativni nadzor je priporočil izboljšave na nekaterih področjih, da bi se: (1) bolje odražala vloga čezmejnih prelivanj pri analizi težav; (2) bolje pojasnilo, kaj bi bil uspeh pobude; (3) nadalje utemeljil seznam možnosti politike in (4) podrobneje opredelili stroški predlaganih ukrepov. Ocena učinka je bila prilagojena, da bi se obravnavale te točke in podrobnejše pripombe Odbora za regulativni nadzor. Zdaj vključuje podrobnejše razlage vloge čezmejnih prelivanj na področju kibernetske varnosti, jasnejši pregled možnosti merjenja uspeha, podrobnejšo razlago zasnove in logike, na katerih temeljijo različne možnosti politike in ukrepi, obravnavani v okviru teh možnosti, podrobnejšo razlago vidikov, analiziranih v zvezi s sektorskim področjem uporabe direktive o varnosti omrežij in informacijskih sistemov, in dodatna pojasnila v zvezi s stroški.

Komisija je preučila več možnosti politike za izboljšanje pravnega okvira na področju kibernetske odpornosti in odzivanja na incidente:

- „brez ukrepanja“: direktiva o varnosti omrežij in informacijskih sistemov bi ostala nespremenjena in ne bi se sprejeli nobeni drugi nezakonodajni ukrepi za obravnavanje težav, opredeljenih z oceno direktive o varnosti omrežij in informacij;
- možnost 1: brez sprememb na zakonodajni ravni. Namesto tega bi Komisija izdala priporočila in smernice (na primer o določitvi izvajalcev bistvenih storitev, varnostnih zahtevah, postopkih priglasitve incidentov in nadzoru) po posvetovanju s

[6] Študija v podporo pregledu Direktive (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (direktiva o varnosti omrežij in informacijskih sistemov) – št. 2020-665. Wavestone, CEPS in ICF.

[7] **[Dodati povezavi do končnega dokumenta in povzetka.]**

skupino za sodelovanje, Agencijo EU za kibernetsko varnost (ENISA) in, po potrebi, mrežo skupin za odzivanje na incidente na področju računalniške varnosti (CSIRT);

- možnost 2: ta možnost vključuje ciljno usmerjene spremembe direktive o varnosti omrežij in informacijskih sistemov, vključno z razširitvijo področja uporabe in več drugimi spremembami, ki bi bile namenjene zagotavljanju nekaterih takojšnjih rešitev opredeljenih težav ter večje jasnosti in nadaljnje harmonizacije (kot so določbe za harmonizacijo pragov za določitev). Vendar pa bi se v spremenjeni direktivi o varnosti omrežij in informacijskih sistemov ohranili glavni gradniki, pristop in utemeljitev;
- možnost 3: ta scenarij vključuje sistemske in strukturne spremembe direktive o varnosti omrežij in informacijskih sistemov (z novo direktivo), ki predvidevajo temeljitejšo spremembo pristopa za pokrivanje širšega segmenta gospodarstev v Uniji, vendar z bolj osredotočenim nadzorom, usmerjenim v velike in ključne akterje. Racionalizirane bi bile tudi obveznosti, naložene podjetjem, in zagotovljena višja stopnja njihove harmonizacije, ustvarjeno bi bilo učinkovitejše okolje za operativne vidike in vzpostavljena jasna podlaga za okrepljene deljene obveznosti in odgovornost različnih zainteresiranih strani pri ukrepih za kibernetsko varnost.

V oceni učinka je ugotovljeno, da je prednostna možnost možnost 3 (tj. sistemske in strukturne spremembe okvira za varnost omrežij in informacijskih sistemov. Kar zadeva uspešnost, bi bila s prednostno možnostjo jasno določena področje uporabe direktive o varnosti omrežij in informacijskih sistemov, razširjeno na bolj reprezentativen del gospodarstev in družb EU, ter racionalizacija zahtev, skupaj z bolj opredeljenim okvirom za nadzor in izvrševanje, ki bi bil namenjen zvišanju ravni izpolnjevanja obveznosti. Vključuje tudi ukrepe, namenjene izboljšanju pristopov k oblikovanju politike na ravni držav članic in spremembi njihove paradigme, spodbujanju novih okvirov za obvladovanje tveganja pri odnosih z dobavitelji in usklajenemu razkrivanju šibkih točk. Hkrati prednostna možnost politike vzpostavlja jasno podlago za deljene obveznosti in odgovornost ter predvideva mehanizme, namenjene spodbujanju večjega zaupanja med državami članicami, tako med organi kot tudi industrijo, podpiranju izmenjave informacij in zagotavljanju bolj operativnega pristopa, kot so medsebojna pomoč in mehanizmi medsebojnih strokovnih pregledov. S to možnostjo bi bil tudi določen okvir EU za krizno upravljanje, ki bi temeljil na nedavno vzpostavljeni operativni mreži EU, in zagotovljena večja vključenost agencije ENISA v okviru njenega sedanjega mandata pri izvajanju natančnega pregleda stanja na področju kibernetske varnosti v Uniji.

Kar zadeva učinkovitost, bi prednostna možnost sicer pomenila dodatne stroške za izpolnjevanje obveznosti in izvrševanje za podjetja in države članice, vendar pa bi privedla tudi do učinkovitih kompromisov in sinergij, z največjim potencialom izmed vseh analiziranih možnosti politike za zagotovitev višje in usklajene ravni kibernetske odpornosti ključnih subjektov po vsej Uniji, ki bi na koncu privedla do znižanja stroškov za podjetja in družbo. Ta možnost politike bi ustvarila nekaj dodatnega upravnega bremena in stroškov za izpolnjevanje obveznosti za organe držav članic. Vendar pa bi, gledano v celoti, srednje- in dolgoročno prinesla tudi precejšnje koristi z večjim sodelovanjem med državami članicami, tudi na operativni ravni, ter z medsebojno pomočjo, mehanizmi medsebojnih strokovnih pregledov ter boljšim pregledom ključnih podjetij in sodelovanjem z njimi spodbudila splošno povečanje zmogljivosti za kibernetsko varnost na nacionalni in regionalni ravni. Prednostna možnost politike bi v veliki meri zagotavljala tudi skladnost z drugo zakonodajo, pobudami ali ukrepi politike, vključno s sektorskim *lex specialis*.

Obravnavanje sedanje nezadostne pripravljenosti na področju kibernetske varnosti na ravni držav članic in ravni podjetij ter drugih organizacij bi lahko zagotovilo večjo učinkovitost in znižanje dodatnih stroškov, ki izhajajo iz kibernetskih incidentov.

- Za bistvene in pomembne subjekte bi zvišanje ravni pripravljenosti na področju kibernetske varnosti lahko privedlo do zmanjšanja morebitne izgube prihodkov zaradi motenj – tudi zaradi industrijskega vohunjenja – in znižalo visoke stroške *ad-hoc* zmanjševanja groženj. Takšne koristi bodo verjetno večje od stroškov potrebnih naložb. Z zmanjšanjem razdrobljenosti na notranjem trgu bi se izboljšali tudi enaki konkurenčni pogoji med izvajalci.
- Kar zadeva države članice, bi se lahko dodatno zmanjšalo tveganje naraščanja proračunskih odhodkov za *ad-hoc* zmanjševanje groženj in znižali dodatni stroški v izrednih razmerah, povezanih s kibernetskimi incidenti.
- Kar zadeva državljane, se pričakuje, da se bo z obravnavanjem kibernetskih incidentov zmanjšala izguba dohodka zaradi gospodarskih motenj.

Višje ravni kibernetske varnosti v državah članicah ter sposobnost podjetij in organov, da se hitro odzovejo na incident in ublažijo njegov vpliv, bodo najverjetneje privedle do večjega splošnega zaupanja državljanov v digitalno gospodarstvo, kar bi lahko pozitivno vplivalo na rast in naložbe.

Zviševanje splošne ravni kibernetske varnosti bo verjetno privedlo do večje splošne varnosti in nemotenega neprekinjenega delovanja bistvenih storitev, ki so kritične za družbo. Pobuda lahko prispeva tudi k drugim družbenim učinkom, kot so nižje ravni kibernetske kriminalitete in terorizma ter večja civilna zaščita. Zviševanje ravni kibernetske pripravljenosti za podjetja in druge organizacije lahko prepreči morebitne finančne izgube zaradi kibernetskih napadov in s tem potrebo po odpuščanju zaposlenih.

Zviševanje splošne ravni kibernetske varnosti bi lahko tudi preprečilo okoljska tveganja ali okoljsko škodo v primeru napada na bistveno storitev. To bi lahko veljalo zlasti za energetski in prometni sektor ter sektor oskrbe z vodo in njene distribucije. Pobuda bi lahko z okrepitvijo zmogljivosti za kibernetsko varnost zagotovila večjo uporabo infrastruktur in storitev IKT zadnje generacije, ki so tudi okoljsko bolj trajnostne, ter zamenjavo neučinkovitih in manj varnih obstoječih infrastruktur. To naj bi prispevalo tudi k zmanjšanju števila dragih kibernetskih incidentov in sprostitvi virov, ki so na voljo za trajnostne naložbe.

- **Primernost in poenostavitev ureditve**

Predlog predvideva splošno izključitev mikro in malih subjektov s področja uporabe okvira za varnost omrežij in informacijskih sistemov in manj strogo ureditev naknadnega nadzora, ki se uporablja za številne nove subjekte, ki spadajo na revidirano področje uporabe (tako imenovani pomembni subjekti). Ti ukrepi so namenjeni zmanjšanju in uravnoteženju bremena podjetij in javnih uprav. Poleg tega predlog nadomešča zapleten sistem določanja izvajalcev bistvenih storitev s splošno veljavno obveznostjo ter uvaja višjo stopnjo harmonizacije obveznosti glede varnosti in poročanja, s katero bi se zmanjšalo breme glede skladnosti, zlasti za subjekte, ki opravljajo čezmejne storitve.

Predlog znižuje stroške izpolnjevanja obveznosti za MSP, saj morajo subjekti sprejeti le tiste ukrepe, ki so potrebni za zagotavljanje ravni varnosti omrežij in informacijskih sistemov, ki ustreza obstoječemu tveganju.

- **Temeljne pravice**

EU je zavezana zagotavljanju visokih standardov varstva temeljnih pravic. Vsi dogovori o prostovoljni izmenjavi informacij med subjekti, ki jih spodbuja ta direktiva, bi se izvajali v zaupanja vrednih okoljih ob popolnem spoštovanju pravil Unije o varstvu podatkov, zlasti Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta[8].

4. PRORAČUNSKE POSLEDICE

Glej oceno finančnih posledic.

5. DRUGI ELEMENTI

- **Načrti za izvedbo ter ureditev spremljanja, ocenjevanja in poročanja**

Predlog vključuje splošni načrt za spremljanje in ocenjevanje učinka na specifične cilje, pri čemer se zahteva, da Komisija opravi revizijo vsaj [54 mesecev] po datumu začetka veljavnosti ter o svojih glavnih ugotovitvah poroča Evropskemu parlamentu in Svetu.

Revizijo je treba izvesti v skladu s smernicami Komisije za boljše pravno urejanje.

- **Natančnejša pojasnitev posameznih določb predloga**

Predlog temelji na več glavnih področjih politike, ki so medsebojno povezana in namenjena zvišanju ravni kibernetske varnosti v Uniji.

Predmet urejanja in področje uporabe (člena 1 in 2)

Direktiva zlasti (a) določa obveznosti držav članic, da sprejmejo nacionalno strategijo za kibernetsko varnost, imenujejo pristojne nacionalne organe, enotne kontaktne točke in skupine CSIRT; (b) določa, da države članice določijo obveznosti glede obvladovanja tveganj za kibernetsko varnost in poročanja za subjekte, ki se v skladu s Prilogo I štejejo za bistvene subjekte in v skladu s Prilogo II za pomembne subjekte; (c) določa, da države članice določijo obveznosti glede izmenjave informacij o kibernetski varnosti.

Uporablja se za nekatere javne ali zasebne bistvene subjekte, ki delujejo v sektorjih, navedenih v Prilogi I (energija, promet, bančništvo, infrastrukture finančnega trga, zdravje, pitna voda, odpadna voda, digitalna infrastruktura, javna uprava in vesolje), in nekatere pomembne subjekte, ki delujejo v sektorjih, navedenih v Prilogi II (poštne in kurirske storitve, ravnanje z odpadki, proizvodnja, izdelava in distribucija kemikalij, proizvodnja, predelava in distribucija živil, proizvodnja in ponudniki digitalnih storitev). Mikro in mali subjekti v smislu Priporočila Komisije 2003/361/ES z dne 6. maja 2003 so izključeni s področja uporabe Direktive, razen ponudnikov elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, ponudnikov storitev zaupanja, registrov vrhnjih domenskih imen in javnih uprav ter nekaterih drugih subjektov, kot je edini ponudnik storitve v državi članici.

Nacionalni okviri kibernetske varnosti (členi 5 do 11)

[8] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

Države članice morajo sprejeti nacionalno strategijo za kibernetsko varnost, v kateri so opredeljeni strateški cilji ter ustrezni ukrepi politike in regulativni ukrepi za doseganje in ohranjanje visoke ravni kibernetske varnosti.

Direktiva vzpostavlja tudi okvir za usklajeno razkrivanje šibkih točk in zahteva, da države članice imenujejo skupine CSIRT, ki bodo delovale kot zaupanja vredni posredniki ter olajševale sodelovanje med poročajočimi subjekti in proizvajalci ali ponudniki proizvodov in storitev IKT. Agencija ENISA mora razviti in vzdrževati evropski register ugotovljenih šibkih točk.

Države članice morajo vzpostaviti nacionalne okvire za krizno upravljanje kibernetske varnosti, med drugim z imenovanjem pristojnih nacionalnih organov, odgovornih za upravljanje velikih kibernetskih incidentov in kriz.

Države članice morajo imenovati tudi enega ali več pristojnih nacionalnih organov za kibernetsko varnost za nadzorne naloge po tej direktivi ter nacionalno enotno kontaktno točko za kibernetsko varnost za opravljanje povezovalne vloge, da se zagotovi čezmejno sodelovanje organov držav članic. Države članice morajo imenovati tudi skupine CSIRT.

Sodelovanje (členi 12 do 16)

Direktiva vzpostavlja skupino za sodelovanje, ki podpira in olajšuje strateško sodelovanje in izmenjavo informacij med državami članicami ter krepi zaupanje med njimi. Vzpostavlja tudi mrežo skupin CSIRT, ki prispeva h krepitvi zaupanja med državami članicami ter spodbuja hitro in učinkovito operativno sodelovanje.

Evropska organizacijska mreža za povezovanje v kibernetski krizi (EU-CyCLONe) je vzpostavljena za podpiranje usklajenega upravljanja velikih kibernetskih incidentov in kriz ter zagotavljanje redne izmenjave informacij med državami članicami in institucijami EU.

Agencija ENISA mora v sodelovanju s Komisijo izdati dvoletno poročilo o stanju kibernetske varnosti v Uniji.

Komisija mora vzpostaviti sistem medsebojnih strokovnih pregledov, ki bo omogočal redne medsebojne strokovne preglede uspešnosti politik kibernetske varnosti držav članic.

Obveznosti glede obvladovanja tveganj za kibernetsko varnost in poročanja (členi 17 do 23)

Direktiva določa, da morajo države članice zagotoviti, da upravni organi vseh subjektov, ki spadajo na področje uporabe, odobrijo ukrepe za obvladovanje tveganj za kibernetsko varnost, ki jih sprejmejo zadevni subjekti, in se udeležijo posebnega usposabljanja v zvezi s kibernetsko varnostjo.

Države članice morajo zagotoviti, da subjekti, ki spadajo na področje uporabe, sprejmejo ustrezne in sorazmerne tehnične in organizacijske ukrepe za obvladovanje tveganj za kibernetsko varnost omrežij in informacijskih sistemov. Poleg tega morajo zagotoviti, da subjekti priglasijo pristojnim nacionalnim organom ali skupinam CSIRT vse kibernetske incidente, ki bistveno vplivajo na storitev, ki jo opravljajo.

Registri vrhnjih domen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene, zbirajo ter vzdržujejo točne in popolne podatke o registraciji domenskih imen.

Poleg tega morajo taki subjekti zagotavljati učinkovit dostop do podatkov o registraciji domen za osebe, ki imajo upravičen razlog za dostop.

Sodna pristojnost in registracija (člena 24 in 25)

Praviloma se za bistvene in pomembne subjekte šteje, da spadajo v sodno pristojnost države članice, kjer opravljajo svoje storitve. Vendar se za nekatere vrste subjektov (ponudniki storitev sistema domenskih imen, registri vrhnjih domenskih imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnih centrov in ponudniki omrežij za dostavo vsebine ter nekateri ponudniki digitalnih storitev) šteje, da spadajo v sodno pristojnost države članice, v kateri imajo glavni sedež v Uniji. Namen tega je zagotoviti, da se taki subjekti ne soočajo s številnimi različnimi pravnimi zahtevami, saj opravljajo čezmejne storitve v zelo velikem obsegu. Agencija ENISA mora vzpostaviti in vzdrževati register te vrste subjektov.

Izmenjava informacij (člena 26 in 27)

Države članice določijo pravila, ki subjektom omogočajo, da sodelujejo pri izmenjavi informacij, povezanih s kibernetsko varnostjo, v okviru posebnih dogovorov o izmenjavi informacij o kibernetski varnosti v skladu s členom 101 PDEU. Poleg tega države članice omogočijo subjektom, ki ne spadajo na področje uporabe te direktive, da prostovoljno poročajo o pomembnih incidentih, kibernetskih grožnjah ali skorajšnjih dogodkih.

Nadzor in izvrševanje (členi 28 do 34)

Pristojni organi morajo nadzorovati subjekte, ki spadajo na področje uporabe Direktive, in zlasti zagotoviti, da izpolnjujejo zahteve glede varnosti in priglasitve incidentov. Direktiva razlikuje med ureditvijo predhodnega nadzora za bistvene subjekte in ureditvijo naknadnega nadzora za pomembne subjekte, pri čemer slednja od pristojnih organov zahteva, da ukrepajo na podlagi dokazov ali znakov, da pomembni subjekt ne izpolnjuje zahtev glede varnosti in priglasitve incidentov.

Direktiva od držav članic tudi zahteva, da bistvenim in pomembnim subjektom naložijo upravne globe, ter določa nekatere najvišje globe.

Države članice morajo sodelovati in si po potrebi pomagati, če subjekti opravljajo storitve v več kot eni državi članici ali če je glavni sedež subjekta ali njegov predstavnik v eni državi članici, njegovo omrežje in informacijski sistemi pa v eni ali več drugih državah članicah.

2020/0359 (COD)

Predlog

DIREKTIVA EVROPSKEGA PARLAMENTA IN SVETA

o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148

(Besedilo velja za EGP)

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 114 Pogodbe,

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora[9],

ob upoštevanju mnenja Odbora regij[10],

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

(1) Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta[11] je bila namenjena razvoju zmogljivosti za kibernetsko varnost po vsej Uniji, ublažitvi groženj za omrežja in informacijske sisteme, ki se uporabljajo za opravljanje bistvenih storitev v ključnih sektorjih, ter zagotovitvi neprekinjenega izvajanja takih storitev pri spoprijemanju s kibernetskimi incidenti, s čimer naj bi prispevala k učinkovitemu delovanju gospodarstva in družbe Unije.

(2) Od začetka veljavnosti Direktive (EU) 2016/1148 je bil dosežen velik napredek pri zviševanju ravni kibernetske odpornosti v Uniji. Pregled navedene direktive je pokazal, da se je uporabljala kot katalizator za institucionalni in regulativni pristop h kibernetski varnosti v Uniji, s čimer je utrla pot do velike spremembe v mišljenju. Direktiva je zagotovila dokončanje nacionalnih okvirov z opredelitvijo nacionalnih strategij za kibernetsko varnost, vzpostavitvijo nacionalnih zmogljivosti in izvajanjem regulativnih ukrepov, ki so zajemali bistvene infrastrukture in akterje, ki so jih določile posamezne države članice. Prispevala je tudi k sodelovanju na ravni Unije z ustanovitvijo skupine za sodelovanje[12] in mreže nacionalnih skupin za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: mreža skupin CSIRT)[13]. Kljub navedenim dosežkom pa so bile pri pregledu Direktive (EU) 2016/1148 razkrite pomanjkljivosti, zaradi katerih z navedeno direktivo ni mogoče

---

9 UL C , , str. .

10 UL C , , str. .

11 Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

12 Člen 11 Direktive (EU) 2016/1148.

13 Člen 12 Direktive (EU) 2016/1148.

učinkovito obravnavati sedanjih in nastajajočih izzivov na področju kibernetske varnosti.

(3) Omrežja in informacijski sistemi so se razvili v osrednjo značilnost vsakdanjega življenja s hitro digitalno preobrazbo in medsebojno povezanostjo družbe, vključno s čezmejnimi izmenjavami. Ta razvoj je privedel do razširitve okolja kibernetskih groženj, s čimer so se pojavili novi izzivi, ki zahtevajo prilagojene, usklajene in inovativne odzive v vseh državah članicah. Število, obseg, izpopolnjenost, pogostost in vpliv kibernetskih incidentov so vse večji ter pomenijo veliko grožnjo delovanju omrežij in informacijskih sistemov. Posledično lahko kibernetski incidenti ovirajo gospodarske dejavnosti na notranjem trgu, ustvarjajo finančne izgube, slabijo zaupanje uporabnikov ter povzročajo veliko škodo gospodarstvu in družbi Unije. Pripravljenost in učinkovitost na področju kibernetske varnosti sta zato zdaj pomembnejši za ustrezno delovanje notranjega trga kot kdaj koli prej.

(4) Pravna podlaga Direktive (EU) 2016/1148 je bil člen 114 Pogodbe o delovanju Evropske unije (PDEU), katerega cilj je vzpostavitev in delovanje notranjega trga z okrepitvijo ukrepov za približevanje nacionalnih pravil. Zahteve glede kibernetske varnosti, ki jih morajo izpolnjevati subjekti, ki opravljajo storitve ali gospodarsko pomembne dejavnosti, se med državami članicami močno razlikujejo v smislu vrste zahtev, njihove ravni podrobnosti in metode nadzora. Te razlike povzročajo dodatne stroške in ustvarjajo težave za podjetja, ki ponujajo blago ali storitve čezmejno. Zahteve, ki jih naloži ena država članica in ki se razlikujejo od zahtev, ki jih naloži druga država članica, ali so celo v nasprotju z njimi, lahko bistveno vplivajo na takšne čezmejne dejavnosti. Poleg tega bo možnost neoptimalnega oblikovanja ali izvajanja standardov kibernetske varnosti v eni državi članici verjetno vplivala na raven kibernetske varnosti drugih držav članic, zlasti glede na intenzivne čezmejne izmenjave. Pregled Direktive (EU) 2016/1148 je pokazal velike razlike v njenem izvajanju v državah članicah, tudi v zvezi z njenim področjem uporabe, katerega razmejitev je bila v zelo veliki meri prepuščena presoji držav članic. Direktiva (EU) 2016/1148 je državam članicam zagotovila tudi zelo široko polje proste presoje, kar zadeva izvajanje obveznosti glede varnosti in poročanja o incidentih, določenih v Direktivi. Te obveznosti so se zato na nacionalni ravni izpolnjevale na zelo različne načine. Podobne razlike pri izvajanju so se pojavile tudi v zvezi z določbami Direktive o nadzoru in izvrševanju.

(5) Vse te razlike povzročajo razdrobljenost notranjega trga in lahko škodljivo učinkujejo na njegovo delovanje, kar vpliva zlasti na čezmejno opravljanje storitev in raven kibernetske odpornosti zaradi uporabe različnih standardov. Ta direktiva je namenjena odpravi tako velikih razlik med državami članicami, zlasti z določitvijo minimalnih pravil v zvezi z delovanjem usklajenega regulativnega okvira, določitvijo mehanizmov za učinkovito sodelovanje med pristojnimi organi v posameznih državah članicah, posodobitvijo seznama sektorjev in dejavnosti, za katere veljajo obveznosti glede kibernetske varnosti, ter določitvijo učinkovitih pravnih sredstev in sankcij, ki so ključni za učinkovito izvrševanje navedenih obveznosti. Zato bi bilo treba Direktivo (EU) 2016/1148 razveljaviti in nadomestiti s to direktivo.

(6) Ta direktiva ne vpliva na zmožnost držav članic, da sprejmejo potrebne ukrepe, s katerimi zaščitijo bistvene interese svoje varnosti, javni red in javno varnost ter omogočijo preiskovanje, odkrivanje in pregon kaznivih dejanj v skladu s pravom Unije. V skladu s členom 346 PDEU nobena država članica ni dolžna dajati informacij, katerih razkritje bi bilo v nasprotju z bistvenimi interesi njene javne varnosti. V tem smislu so pomembni nacionalna pravila in pravila Unije za varovanje

tajnih podatkov, sporazumi o nerazkritju informacij ali neuradni sporazumi o nerazkritju informacij, kot je semaforski protokol (Traffic Light Protocol)[14].

(7) Z razveljavitvijo Direktive (EU) 2016/1148 bi bilo treba področje uporabe po sektorjih razširiti na večji del gospodarstva, ob upoštevanju premislekov iz uvodnih izjav 4 do 6. Sektorje, zajete z Direktivo (EU) 2016/1148, bi bilo torej treba razširiti, da bi se zagotovila celovita pokritost sektorjev in storitev, ki so bistvenega pomena za ključne družbene in gospodarske dejavnosti na notranjem trgu. Pravila se ne bi smela razlikovati glede na to, ali so subjekti izvajalci bistvenih storitev ali ponudniki digitalnih storitev. Takšno razlikovanje se je izkazalo za zastarelo, saj ne odraža dejanskega pomena sektorjev ali storitev za družbene in gospodarske dejavnosti na notranjem trgu.

(8) V skladu z Direktivo (EU) 2016/1148 so bile države članice odgovorne za določanje, kateri subjekti izpolnjujejo merila, v skladu s katerimi se štejejo za izvajalce bistvenih storitev („postopek določitve“). Za odpravo velikih razlik med državami članicami v zvezi s tem in zagotovitev pravne varnosti za zahteve glede obvladovanja tveganj in obveznosti poročanja za vse ustrezne subjekte bi bilo treba določiti enotno merilo, ki bi določalo, kateri subjekti spadajo na področje uporabe te direktive. Navedeno merilo bi moralo vključevati uporabo pravila omejitve velikosti, v skladu s katerim na področje uporabe te direktive spadajo vsa srednja in velika podjetja, kot so opredeljena v Priporočilu Komisije 2003/361/ES[15], ki delujejo v sektorjih ali opravljajo vrsto storitev, zajetih s to direktivo. Od držav članice se ne bi smelo zahtevati, naj pripravijo seznam subjektov, ki izpolnjujejo to splošno veljavno merilo, povezano v velikostjo.

(9) Vendar bi morali biti s to direktivo zajeti tudi mali ali mikro subjekti, ki izpolnjujejo nekatera merila, ki kažejo ključno vlogo za gospodarstvo ali družbo držav članic ali za določene sektorje ali vrste storitev. Države članice bi morale biti odgovorne za pripravo seznama takih subjektov in ga predložiti Komisiji.

(10) Komisija lahko v sodelovanju s skupino za sodelovanje izda smernice o izvajanju meril, ki se uporabljajo za mikro in mala podjetja.

(11) Glede na sektor, v katerem delujejo, ali vrsto storitve, ki jo opravljajo, bi morali biti subjekti, ki spadajo na področje uporabe te direktive, razvrščeni v dve kategoriji: bistvene in pomembne. Pri takšni kategorizaciji bi bilo treba upoštevati stopnjo kritičnosti sektorja ali vrste storitve ter stopnjo odvisnosti od drugih sektorjev ali vrst storitev. Za bistvene in pomembne subjekte bi morale veljati enake zahteve glede obvladovanja tveganj in obveznosti poročanja. Pri teh dveh kategorijah subjektov bi bilo treba razlikovati med ureditvijo nadzora in ureditvijo kazni, da bi se zagotovilo ustrezno ravnovesje med zahtevami in obveznostmi na eni strani ter upravnim bremenom, ki izhaja iz nadzora nad izpolnjevanjem zahtev in obveznosti, na drugi strani.

(12) Sektorska zakonodaja in sektorski instrumenti lahko prispevajo k zagotavljanju visokih ravni kibernetske varnosti, ob polnem upoštevanju posebnosti in kompleksnosti zadevnih sektorjev. Če sektorski pravni akt Unije določa, da morajo bistveni in pomembni subjekti sprejeti ukrepe za obvladovanje tveganj za kibernetsko

[14] Semaforski protokol je sredstvo, s katerim nekdo, ki izmenjuje informacije, obvesti svoje ciljne skupine o morebitnih omejitvah pri nadaljnjem širjenju teh informacij. Uporablja se v skoraj vseh skupnostih CSIRT ter nekaterih centrih za izmenjavo in analizo informacij.

[15] Priporočilo Komisije 2003/361/ES z dne 6. maja 2003 o opredelitvi mikro, malih in srednjih podjetij (UL L 124, 20.5.2003, str. 36).

varnost ali priglasiti incidente ali pomembne kibernetske grožnje, ki imajo vsaj enak učinek kot obveznosti, določene v tej direktivi, bi se morale uporabljati navedene sektorske določbe, vključno z določbami o nadzoru in izvrševanju. Komisija lahko izda smernice v zvezi z izvajanjem *lex specialis*. Ta direktiva ne izključuje sprejetja dodatnih sektorskih aktov Unije, ki obravnavajo ukrepe za obvladovanje tveganj za kibernetsko varnost in priglasitve incidentov. Ta direktiva ne posega v obstoječa izvedbena pooblastila, ki so bila podeljena Komisiji v številnih sektorjih, vključno s prometnim in energetskim.

(13) Uredba XXXX/XXXX Evropskega parlamenta in Sveta[16] bi se morala šteti za sektorski pravni akt Unije v zvezi s to direktivo, kar zadeva subjekte finančnega sektorja. Določbe Uredbe XXXX/XXXX v zvezi z ukrepi za obvladovanje tveganj na področju informacijske in komunikacijske tehnologije (IKT), upravljanjem incidentov, povezanih z IKT, in zlasti poročanjem o incidentih, pa tudi testiranjem digitalne operativne odpornosti, dogovori o izmenjavi informacij in tveganjem tretjih oseb na področju IKT bi se morale uporabljali namesto določb te direktive. Države članice zato ne bi smele uporabljati določb te direktive o obvladovanju tveganj za kibernetsko varnost in obveznostih poročanja, izmenjavi informacij ter nadzoru in izvrševanju za finančne subjekte, zajete z Uredbo XXXX/XXXX. Hkrati je pomembno ohranjati tesno povezavo in izmenjavo informacij s finančnim sektorjem na podlagi te direktive. V ta namen Uredba XXXX/XXXX omogoča vsem finančnim nadzornikom, evropskim nadzornim organom za finančni sektor in nacionalnim pristojnim organom iz Uredbe XXXX/XXXX, da sodelujejo v razpravah o strateških politikah in pri tehničnem delu skupine za sodelovanje ter si izmenjujejo informacije in sodelujejo z enotnimi kontaktnimi točkami, imenovanimi v skladu s to direktivo, in z nacionalnimi skupinami CSIRT. Pristojni organi iz Uredbe XXXX/XXXX bi morali podrobnosti o večjih incidentih, povezanih z IKT, posredovati tudi enotnim kontaktnim točkam, imenovanim v skladu s to direktivo. Poleg tega bi morale države članice še naprej vključevati finančni sektor v svoje strategije za kibernetsko varnost, nacionalne skupine CSIRT pa lahko vključijo finančni sektor v svoje dejavnosti.

(14) Glede na medsebojne povezave med kibernetsko varnostjo in fizično varnostjo subjektov bi bilo treba zagotoviti skladen pristop med Direktivo (EU) XXX/XXX Evropskega parlamenta in Sveta[17] in to direktivo. Za dosego tega bi morale države članice zagotoviti, da se kritični subjekti in enakovredni subjekti v skladu z Direktivo (EU) XXX/XXX štejejo za bistvene subjekte po tej direktivi. Države članice bi morale tudi zagotoviti, da njihove strategije za kibernetsko varnost določajo okvir politike za okrepljeno usklajevanje med pristojnim organom iz te direktive in pristojnim organom iz Direktive (EU) XXX/XXX v okviru izmenjave informacij o incidentih in kibernetskih grožnjah ter izvajanja nadzornih nalog. Organi iz obeh direktiv bi morali sodelovati in si izmenjevati informacije, zlasti v zvezi z določanjem kritičnih subjektov, kibernetskimi grožnjami, tveganji za kibernetsko varnost in incidenti, ki vplivajo na kritične subjekte, ter o ukrepih za kibernetsko varnost, ki jih sprejmejo kritični subjekti. Na zahtevo pristojnih organov iz Direktive (EU) XXX/XXX bi moralo biti pristojnim organom iz te direktive omogočeno izvajanje nadzornih in izvršilnih pooblastil v zvezi z bistvenim subjektom, ki je opredeljen kot kritičen. Oboji organi bi morali v ta namen sodelovati in si izmenjevati informacije.

---

16 *[vstaviti polni naslov in sklic na objavo v UL, ko bosta znana]*.

17 *[vstaviti polni naslov in sklic na objavo v UL, ko bosta znana]*.

(15) Podpiranje in ohranjanje zanesljivega, odpornega in varnega sistema domenskih imen (DNS) sta ključna dejavnika pri ohranjanju celovitosti interneta ter bistvena za njegovo neprekinjeno in stabilno delovanje, od katerega sta odvisna digitalno gospodarstvo in družba. Zato bi se morala ta direktiva uporabljati za vse ponudnike storitev sistema domenskih imen vzdolž verige razreševanja DNS, vključno z upravljavci korenskih imenskih strežnikov, vrhnjih domenskih strežnikov, krovnih imenskih strežnikov za domenska imena in rekurzivnih razreševalnikov.

(16) Storitve računalništva v oblaku bi morale zajemati storitve, ki omogočajo upravljanje na zahtevo in širok oddaljeni dostop do prožnega in po obsegu prilagodljivega nabora deljivih in porazdeljenih računalniških virov. Ti računalniški viri obsegajo vire, kot so omrežja, strežniki ali druga infrastruktura, operacijski sistemi, programska oprema, pomnilniki, aplikacije in storitve. Modeli uvajanja računalništva v oblaku bi morali vključevati zasebni, skupnostni, javni in hibridni oblak. Zgoraj navedene storitve in modeli uvajanja imajo enak pomen kot izrazi za storitve in modele uvajanja, opredeljeni v standardu ISO/IEC 17788:2014. Zmožnost uporabnika računalništva v oblaku, da enostransko samostojno zagotavlja računalniške zmogljivosti, kot je čas strežnika ali omrežno shranjevanje, brez kakršne koli človeške interakcije ponudnika računalništva v oblaku, bi bilo mogoče opisati kot upravljanje na zahtevo. Izraz „širok oddaljeni dostop“ se uporablja za opis, da se zmogljivosti oblaka zagotavljajo prek omrežja in da se do njih dostopa z mehanizmi, ki spodbujajo uporabo raznolikih platform tankih in debelih odjemalcev (vključno z mobilnimi telefoni, tablicami, prenosniki in delovnimi postajami). Izraz „prožen“ se nanaša na računalniške vire, ki jih ponudnik storitev v oblaku prilagodljivo dodeljuje, ne glede na geografsko lokacijo virov, da bi se tako lahko odzvali na spremembe v povpraševanju. Izraz „prilagodljiv nabor“ opisuje take računalniške vire, ki se zagotavljajo in sproščajo glede na povpraševanje, da bi se tako število razpoložljivih virov hitro povečalo ali zmanjšalo, odvisno od delovne obremenitve. Izraz „deljivi“ opisuje take računalniške vire, ki se zagotavljajo več uporabnikom, ki imajo skupen dostop do storitve, vendar obdelava poteka ločeno za vsakega uporabnika, čeprav se storitev zagotavlja z isto elektronsko opremo. Izraz „porazdeljeni“ se uporablja za opis računalniških virov, ki so na različnih omrežnih računalnikih ali napravah ter ki medsebojno komunicirajo in se usklajujejo z izmenjevanjem sporočil.

(17) Zaradi pojava inovativnih tehnologij in novih poslovnih modelov se pričakuje, da se bodo na trgu pojavili novi modeli uvajanja in storitev računalništva v oblaku v odziv na razvijajoče se potrebe strank. V tem okviru se lahko storitve računalništva v oblaku zagotavljajo v zelo porazdeljeni obliki, še bližje lokaciji, kjer se podatki pridobivajo ali zbirajo, kar pomeni premik s tradicionalnega modela na zelo porazdeljen model („računalništvo na robu“).

(18) Storitve, ki jih ponujajo ponudniki storitev podatkovnih centrov, se morda ne zagotavljajo vedno v obliki storitve računalništva v oblaku. Zato podatkovni centri morda niso vedno del infrastrukture računalništva v oblaku. Za obvladovanje vseh tveganj za varnost omrežij in informacijskih sistemov bi morala ta direktiva zajemati tudi ponudnike takih storitev podatkovnih centrov, ki niso storitve računalništva v oblaku. V tej direktivi bi moral izraz „storitev podatkovnega centra“ zajemati opravljanje storitve, ki vključuje strukture ali skupine struktur, namenjene centralizirani namestitvi, medsebojnemu povezovanju in delovanju opreme za informacijsko tehnologijo in omrežne opreme, za shranjevanje, obdelavo in prenos podatkov skupaj z vsemi zmogljivostmi in infrastrukturami za distribucijo električne energije in okoljski nadzor. Izraz „storitev podatkovnega centra“ se ne nanaša na

podatkovne centre v podjetjih, ki so v lasti zadevnega subjekta, ki jih upravlja za lastne namene.

(19) Ponudniki poštnih storitev v smislu Direktive 97/67/ES Evropskega parlamenta in Sveta[18] ter ponudniki storitev hitre pošte in kurirskih storitev bi morali biti predmet te direktive, če zagotavljajo vsaj en korak v verigi poštne dostave ter zlasti sprejem, usmerjanje ali dostavo, vključno s storitvami prevzema. Storitve prenosa, ki se ne izvajajo v povezavi z enim od navedenih korakov, ne bi smele spadati v obseg poštnih storitev.

(20) Navedene vse večje medsebojne odvisnosti so rezultat vse bolj čezmejne in medsebojno odvisne mreže opravljanja storitev z uporabo ključnih infrastruktur po vsej Uniji v sektorjih energije, prometa, digitalne infrastrukture, pitne in odpadne vode, zdravja, nekaterih vidikov javne uprave in vesolja, kar zadeva opravljanje nekaterih storitev, ki so odvisne od talne infrastrukture, ki jih imajo v lasti, jih upravljajo in vodijo bodisi države članice bodisi zasebni subjekti, s čimer torej niso zajete infrastrukture, ki jih ima v lasti, jih upravlja ali vodi Unija ali ki so v lasti, se upravljajo ali vodijo v imenu Unije v okviru njenih vesoljskih programov. Te medsebojne odvisnosti pomenijo, da ima lahko kakršna koli motnja, tudi takšna, ki je prvotno omejena na en subjekt ali en sektor, širše kaskadne učinke, ki imajo lahko daljnosežne in dolgotrajne negativne učinke na opravljanje storitev na notranjem trgu. Pandemija COVID-19 je razkrila šibko točko naših vse bolj medsebojno odvisnih družb zaradi tveganj z majhno verjetnostjo.

(21) Glede na razlike v nacionalnih strukturah upravljanja in zaradi varovanja že obstoječih sektorskih dogovorov ali nadzornih in regulativnih organov Unije bi morale imeti države članice možnost imenovati več kot en pristojni nacionalni organ, odgovoren za izvajanje nalog, povezanih z varnostjo omrežij in informacijskih sistemov bistvenih in pomembnih subjektov po tej direktivi. Države članice bi morale imeti možnost, da to vlogo dodelijo obstoječemu organu.

(22) Za zagotavljanje lažjega čezmejnega sodelovanja in komunikacije med organi ter za učinkovito izvajanje te direktive je nujno, da vsaka država članica imenuje nacionalno enotno kontaktno točko, odgovorno za usklajevanje vprašanj v zvezi z varnostjo omrežij in informacijskih sistemov ter za čezmejno sodelovanje na ravni Unije.

(23) Pristojni organi ali skupine CSIRT bi morali od subjektov učinkovito in uspešno prejeti priglasitve incidentov. Enotne kontaktne točke bi morale biti zadolžene za posredovanje priglasitev incidentov enotnim kontaktnim točkam drugih prizadetih držav članic. Da bi se zagotovila ena enotna vstopna točka v vsaki državi članici, bi morale enotne kontaktne točke na ravni organov držav članic tudi prejemati ustrezne informacije o incidentih v zvezi s subjekti finančnega sektorja od pristojnih organov iz Uredbe XXXX/XXXX, ki bi jih morale biti sposobne posredovati, če je ustrezno, ustreznim pristojnim nacionalnim organom ali skupinam CSIRT po tej direktivi.

(24) Države članice bi morale imeti ustrezne tehnične in organizacijske zmogljivosti za preprečevanje, odkrivanje in ublažitev incidentov in tveganj v omrežjih in informacijskih sistemih ter za odzivanje nanje. Zato bi morale države članice zagotoviti, da imajo dobro delujoče skupine CSIRT, znane tudi kot skupine za

[18] Direktiva 97/67/ES Evropskega parlamenta in Sveta z dne 15. decembra 1997 o skupnih pravilih za razvoj notranjega trga poštnih storitev v Skupnosti in za izboljšanje kakovosti storitve (UL L 15, 21.1.1998, str. 14).

odzivanje na računalniške grožnje (v nadaljnjem besedilu: skupine CERT), ki izpolnjujejo osnovne zahteve, da bi se tako zagotovile učinkovite in združljive zmogljivosti za obvladovanje incidentov in tveganj ter zagotovilo učinkovito sodelovanje na ravni Unije. Za okrepitev odnosa zaupanja med subjekti in skupinami CSIRT v primerih, ko je skupina CSIRT del pristojnega organa, bi morale države članice razmisliti o funkcionalnem ločevanju med operativnimi nalogami, ki jih opravljajo skupine CSIRT, zlasti v zvezi z izmenjavo informacij in podporo subjektom, in nadzornimi dejavnostmi pristojnih organov.

(25) Kar zadeva osebne podatke, bi moralo biti skupinam CSIRT omogočeno, da v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta[19] v imenu in na zahtevo subjekta po tej direktivi zagotovijo proaktvini pregled omrežij in informacijskih sistemov, ki se uporabljajo za opravljanje storitev subjektov. Države članice bi si morale prizadevati za zagotovitev enake ravni tehničnih zmogljivosti za vse sektorske skupine CSIRT. Države članice lahko pri oblikovanju nacionalnih skupin CSIRT zaprosijo za pomoč Agencijo Evropske unije za kibernetsko varnost (ENISA).

(26) Mednarodno sodelovanje na področju kibernetske varnosti je pomembno, zato bi morali skupinam CSIRT poleg sodelovanja v mreži skupin CSIRT, vzpostavljeni s to direktivo, omogočiti sodelovanje tudi v mrežah mednarodnega sodelovanja.

(27) V skladu s Prilogo k Priporočilu Komisije (EU) 2017/1548 o usklajenem odzivu na velike kibernetske incidente in krize („načrt“)[20] bi moral velik incident pomeniti incident, ki ima velik vpliv na vsaj dve državi članici ali ki povzroči motnje, ki presegajo zmožnost države članice za odziv nanje. Glede na njihov vzrok in vpliv se lahko veliki incidenti stopnjujejo in sprevržejo v popolno krizo, ki ne omogoča ustreznega delovanja notranjega trga. Glede na velik obseg in večinoma čezmejno naravo takih incidentov bi morali države članice ter ustrezne institucije, organi in agencije Unije sodelovati na tehnični, operativni in politični ravni za ustrezno usklajevanje odziva po vsej Uniji.

(28) Ker lahko izkoriščanje šibkih točk v omrežjih in informacijskih sistemih povzroči hude motnje in škodo, sta hitro odkrivanje in odpravljanje takih šibkih točk pomemben dejavnik pri zmanjševanju tveganj za kibernetsko varnost. Subjekti, ki razvijajo take sisteme, bi morali zato vzpostaviti ustrezne postopke za obravnavanje šibkih točk, ko jih odkrijejo. Ker šibke točke pogosto odkrijejo in o njih poročajo (jih razkrijejo) tretje osebe (poročajoči subjekti), bi moral proizvajalec ali ponudnik proizvodov ali storitev IKT vzpostaviti tudi potrebne postopke za prejemanje informacij o šibkih točkah od tretjih oseb. V zvezi s tem mednarodna standarda ISO/IEC 30111 in ISO/IEC 29417 določata smernice o obravnavanju oziroma razkrivanju šibkih točk. Kar zadeva razkrivanje šibkih točk, je pomembno zlasti usklajevanje med poročajočimi subjekti in proizvajalci ali ponudniki proizvodov ali storitev IKT. Usklajeno razkrivanje šibkih točk določa strukturiran postopek, s katerim se šibke točke organizacijam sporočijo tako, da lahko organizacija diagnosticira in odpravi šibko točko, preden se podrobne informacije o šibki točki razkrijejo tretji osebi ali javnosti. Usklajeno razkrivanje šibkih točk bi moralo vključevati tudi usklajevanje med poročajočim subjektom in organizacijo v zvezi s časovnim okvirom za odpravo in objavo šibkih točk.

---

[19] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

[20] Priporočilo Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize (UL L 239, 19.9.2017, str. 36).

(29) Države članice bi morale zato sprejeti ukrepe za olajšanje usklajenega razkrivanja šibkih točk z vzpostavitvijo ustrezne nacionalne politike. V zvezi s tem bi morale države članice imenovati skupino CSIRT, ki bi prevzela vlogo „koordinatorke“ in ki bi po potrebi delovala kot posrednica med poročajočimi subjekti in proizvajalci ali ponudniki proizvodov ali storitev IKT. Naloge skupine CSIRT koordinatorke bi morale vključevati zlasti opredelitev zadevnih subjektov in vzpostavitev stika z njimi, podpiranje poročajočih subjektov, pogajanja o časovnicah razkrivanja in upravljanje razkrivanja šibkih točk, ki vplivajo na več organizacij (razkrivanje šibkih točk več strani). Če šibke točke vplivajo na več proizvajalcev ali ponudnikov proizvodov ali storitev IKT s sedežem v več državah članicah, bi morale imenovane skupine CSIRT iz vsake od prizadetih držav članic sodelovati v okviru mreže skupin CSIRT.

(30) Dostop do točnih in pravočasnih informacij o šibkih točkah, ki vplivajo na proizvode in storitve IKT, prispeva k okrepljenemu obvladovanju tveganj za kibernetsko varnost. V zvezi s tem so viri javno dostopnih informacij o šibkih točkah pomembno orodje za subjekte in njihove uporabnike, pa tudi za pristojne nacionalne organe in skupine CSIRT. Zato bi morala agencija ENISA vzpostaviti register šibkih točk, kjer bi bistveni in pomembni subjekti ter njihovi dobavitelji, pa tudi subjekti, ki ne spadajo na področje uporabe te direktive, lahko prostovoljno razkrivali šibke točke in zagotavljali informacije o šibkih točkah, ki bi uporabnikom omogočale sprejetje ustreznih blažilnih ukrepov.

(31) Čeprav podobni registri ali zbirke podatkov o šibkih točk obstajajo, te upravljajo in vzdržujejo subjekti, ki nimajo sedeža v Uniji. Evropski register šibkih točk, ki bi ga vzdrževala agencija ENISA, bi zagotovil večjo preglednost v zvezi s postopkom objave pred uradnim razkritjem šibke točke in odpornost v primerih motenj ali prekinitev pri opravljanju podobnih storitev. Da bi preprečila podvajanje prizadevanj in poskušala zagotoviti čim večje dopolnjevanje, bi morala agencija ENISA preučiti možnost sklenitve sporazumov o strukturnem sodelovanju s podobnimi registri v jurisdikcijah tretjih držav.

(32) Skupina za sodelovanje bi morala vsaki dve leti pripraviti delovni program, ki bi vključeval ukrepe, ki bi jih skupina sprejela za izvajanje svojih ciljev in nalog. Časovni okvir prvega programa, sprejetega v skladu s to direktivo, bi moral biti usklajen s časovnim okvirom zadnjega programa, sprejetega v skladu z Direktivo (EU) 2016/1148, da bi se preprečile morebitne motnje pri delu skupine.

(33) Skupina za sodelovanje bi morala pri pripravi smernic dosledno: evidentirati nacionalne rešitve in izkušnje, oceniti vpliv svojih dosežkov na nacionalne pristope, razpravljati o izzivih v zvezi z izvajanjem in oblikovati posebna priporočila, ki bi se obravnavala z boljšim izvajanjem obstoječih pravil.

(34) Skupina za sodelovanje bi morala ostati prilagodljiv forum in biti sposobna odzivati se na spreminjajoče se in nove prednostne naloge politike in izzive, ob upoštevanju razpoložljivosti virov. Organizirati bi morala redne skupne sestanke z ustreznimi zasebnimi zainteresiranimi stranmi iz vse Unije, na katerih bi se razpravljalo o dejavnostih, ki jih izvaja skupina, in zbirale informacije o nastajajočih izzivih politike. Za okrepitev sodelovanja na ravni Unije bi morala skupina razmisliti o tem, da bi k sodelovanju pri svojem delu povabila organe in agencije Unije, vključene v politiko na področju kibernetske varnosti, kot so Evropski center za boj proti kibernetski kriminaliteti (EC3), Agencija Evropske unije za varnost v letalstvu (EASA) in Agencija Evropske unije za vesoljski program (EUSPA).

(35) Pristojni organi in skupine CSIRT bi morali biti pooblaščeni za sodelovanje v programih izmenjave uradnikov iz drugih držav članic, da bi izboljšali sodelovanje. Pristojni organi bi morali sprejeti potrebne ukrepe, s katerimi bi uradnikom iz drugih držav članic omogočili učinkovito sodelovanje v dejavnostih pristojnega organa gostitelja.

(36) Unija bi morala, kjer je ustrezno, v skladu s členom 218 PDEU skleniti mednarodne sporazume s tretjimi državami ali mednarodnimi organizacijami, ki bi omogočali in urejali njihovo sodelovanje pri nekaterih dejavnostih skupine za sodelovanje in mreže skupin CSIRT. Taki sporazumi bi morali zagotoviti ustrezno varstvo podatkov.

(37) Države članice bi morale prispevati k vzpostavitvi okvira EU za odzivanje na krize na področju kibernetske varnosti, določenega v Priporočilu (EU) 2017/1584, z obstoječimi mrežami za sodelovanje, zlasti organizacijsko mrežo za povezovanje v kibernetski krizi (EU-CyCLONe), mrežo skupin CSIRT in skupino za sodelovanje. Mreža EU-CyCLONe in mreža skupin CSIRT bi morali sodelovati na podlagi postopkovnih ureditev, v katerih so opredeljeni načini navedenega sodelovanja. V poslovniku mreže EU-CyCLONe bi morali biti podrobneje opredeljeni načini delovanja mreže, med drugim z vlogami, načini sodelovanja, stiki z drugimi ustreznimi akterji in predlogami za izmenjavo informacij ter sredstvi komuniciranja. Za obvladovanje krize na ravni Unije bi se morale ustrezne strani zanašati na enotne ureditve za politično odzivanje na krize (IPCR). Komisija bi morala v ta namen uporabljati postopek medsektorskega kriznega usklajevanja na visoki ravni v okviru sistema ARGUS. Če bo imela kriza znaten vpliv na zunanjo ali skupno varnostno in obrambno politiko (SVOP), bi bilo treba sprožiti mehanizem Evropske službe za zunanje delovanje (ESZD) za krizno odzivanje.

(38) V tej direktivi bi se moral izraz „tveganje“ nanašati na možnost izgube ali motnje, ki jo povzroči kibernetski incident, ter bi moral biti izražen kot kombinacija razsežnosti take izgube ali motnje in verjetnosti pojava navedenega incidenta.

(39) V tej direktivi bi se moral izraz „skorajšnji dogodek“ nanašati na dogodek, ki bi lahko povzročil škodo, vendar se je uspešno preprečilo, da bi se v celoti uresničil.

(40) Med ukrepe za obvladovanje tveganj bi morali spadati ukrepi za prepoznavanje tveganj incidentov, preprečevanje, odkrivanje in obvladovanje incidentov ter ublažitev njihovega vpliva. Varnost omrežij in informacijskih sistemov bi morala obsegati varnost shranjenih, prenesenih in obdelanih podatkov.

(41) Da bistvenim in pomembnim subjektom ne bi bilo naloženo nesorazmerno finančno in upravno breme, bi morale biti zahteve glede obvladovanja tveganj za kibernetsko varnost sorazmerne s tveganjem, ki ga pomenita zadevno omrežje in informacijski sistem, pri čemer bi bilo treba upoštevati dovršenost takih ukrepov.

(42) Bistveni in pomembni subjekti bi morali zagotoviti varnost omrežij in informacijskih sistemov, ki jih uporabljajo pri svojih dejavnostih. To so predvsem zasebna omrežja in informacijski sistemi, ki jih upravlja njihovo notranje osebje za IT ali za varnost katerih skrbi zunanji izvajalec. Zahteve glede obvladovanja tveganj za kibernetsko varnost in poročanja v skladu s to direktivo bi se morale uporabljati za ustrezne bistvene in pomembne subjekte ne glede na to, ali vzdrževanje svojih omrežij in informacijskih sistemov izvajajo notranje ali ga oddajajo zunanjim izvajalcem.

(43) Obravnavanje tveganj za kibernetsko varnost, ki izhajajo iz dobavne verige subjekta in njegovega razmerja z njegovimi dobavitelji, je še zlasti pomembno glede na razširjenost incidentov, v katerih so bili subjekti žrtve kibernetskih napadov in v

katerih so bili zlonamerni akterji sposobni ogroziti varnost omrežij in informacijskih sistemov subjekta z izkoriščanjem šibkih točk, ki vplivajo na proizvode in storitve tretje osebe. Subjekti bi morali zato oceniti in upoštevati splošno kakovost proizvodov ter praks svojih dobaviteljev in ponudnikov storitev na področju kibernetske varnosti, vključno z njihovimi varnimi razvojnimi postopki.

(44) Med ponudniki storitev imajo ponudniki upravljanih varnostnih storitev na področjih, kot so odzivanje na incidente, penetracijsko testiranje, varnostne presoje in svetovanje, še posebno pomembno vlogo pri zagotavljanju pomoči subjektom pri njihovih prizadevanjih za odkrivanje incidentov in odzivanje nanje. Vendar pa so bili takšni ponudniki upravljanih varnostnih storitev tudi sami tarče kibernetskih napadov in zaradi svoje tesne vključenosti v delovanje izvajalcev pomenijo posebno tveganje za kibernetsko varnost. Subjekti bi morali biti zato še bolj skrbni pri izbiri ponudnika upravljanih varnostnih storitev.

(45) Subjekti bi morali obravnavati tudi tveganja za kibernetsko varnost, ki izhajajo iz njihovih stikov in odnosov z drugimi zainteresiranimi stranmi v okviru širšega ekosistema. Subjekti bi morali zlasti sprejeti ustrezne ukrepe za zagotovitev, da njihovo sodelovanje z akademskimi in raziskovalnimi ustanovami poteka v skladu z njihovimi politikami na področju kibernetske varnosti, ob upoštevanju dobrih praks v zvezi z varnim dostopom in razširjanjem informacij na splošno ter še posebno z varstvom intelektualne lastnine. Podobno bi morali subjekti glede na pomen in vrednost podatkov za dejavnosti subjektov pri uporabi storitev pretvorbe podatkov in podatkovne analitike, ki jih opravljajo tretje osebe, sprejeti vse ustrezne ukrepe za kibernetsko varnost.

(46) Za nadaljnje obravnavanje ključnih tveganj za dobavno verigo ter zagotavljanje pomoči subjektom, ki delujejo v sektorjih, zajetih s to direktivo, pri ustreznem obvladovanju tveganj za kibernetsko varnost, povezanih z dobavno verigo in dobavitelji, bi morala skupina za sodelovanje, ki vključuje ustrezne nacionalne organe, v sodelovanju s Komisijo in agencijo ENISA izvesti usklajene sektorske ocene tveganj v zvezi z dobavno verigo, kot je že storila za omrežja 5G na podlagi Priporočila (EU) 2019/534 o kibernetski varnosti omrežij 5G[21], da bi opredelila kritične storitve, sisteme ali proizvode IKT, zadevne grožnje in šibke točke za posamezne sektorje.

(47) Pri ocenah tveganj v zvezi z dobavno verigo bi bilo treba glede na značilnosti zadevnega sektorja upoštevati tehnične in, kjer je ustrezno, netehnične dejavnike, vključno z dejavniki, opredeljenimi v Priporočilu (EU) 2019/534, iz usklajene ocene tveganj za varnost omrežij 5G na ravni EU in nabora orodij EU za kibernetsko varnost omrežij 5G, o katerem se je dogovorila skupina za sodelovanje. Za opredelitev dobavnih verig, ki bi morale biti predmet usklajene ocene tveganja, bi bilo treba upoštevati naslednja merila: (i) obseg, v katerem bistveni in pomembni subjekti uporabljajo določene kritične storitve, sisteme ali proizvode IKT in se zanašajo nanje; (ii) pomembnost določenih kritičnih storitev, sistemov ali proizvodov IKT za izvajanje kritičnih ali občutljivih funkcij, vključno z obdelavo osebnih podatkov; (iii) razpoložljivost alternativnih storitev, sistemov ali proizvodov IKT; (iv) odpornost celotne dobavne verige storitev, sistemov ali proizvodov IKT proti dogodkom, ki povzročajo motnje v delovanju, in (v) morebiten prihodnji pomen nastajajočih storitev, sistemov ali proizvodov IKT za dejavnosti subjektov.

[21] Priporočilo Komisije (EU) 2019/534 z dne 26. marca 2019 – Kibernetska varnost omrežij 5G (UL L 88, 29.3.2019, str. 42).

(48) Za racionalizacijo pravnih obveznosti, naloženih ponudnikom javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev in ponudnikom storitev zaupanja, povezanih z varnostjo njihovih omrežij in informacijskih sistemov, ter za omogočanje zadevnim subjektom in njihovim ustreznim pristojnim organom, da izkoristijo pravni okvir, vzpostavljen s to direktivo (vključno z imenovanjem skupine CSIRT, odgovorne za obvladovanje tveganj in incidentov, sodelovanje pristojnih organov pri delu skupine za sodelovanje in mreže skupin CSIRT), bi jih bilo treba vključiti na področje uporabe te direktive. Zato bi bilo treba razveljaviti ustrezne določbe iz Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta[22] ter Direktive (EU) 2018/1972 Evropskega parlamenta in Sveta[23], ki se nanašajo na uvedbo zahteve glede varnosti in priglasitve za tovrstne subjekte. Pravila o obveznostih poročanja ne bi smela vplivati na Uredbo (EU) 2016/679 in Direktivo 2002/58/ES Evropskega parlamenta in Sveta[24].

(49) Kjer je ustrezno in za preprečitev nepotrebnih motenj, bi morali pristojni organi, zadolženi za nadzor in izvrševanje za namene te direktive, še naprej uporabljati obstoječe nacionalne smernice in nacionalno zakonodajo, sprejeto za prenos pravil, povezanih z varnostnimi ukrepi, določenimi v členu 40(1) Direktive (EU) 2018/1972, in zahtev iz člena 40(2) navedene direktive v zvezi s parametri, ki se nanašajo na pomen incidenta.

(50) Glede na vedno večji pomen medosebnih komunikacijskih storitev, neodvisnih od številke, je treba zagotoviti, da se tudi za take storitve uporabljajo ustrezne varnostne zahteve, ob upoštevanju njihove posebne narave in gospodarskega pomena. Ponudniki takih storitev bi torej prav tako morali zagotoviti raven varnosti omrežij in informacijskih sistemov, primerno obstoječemu tveganju. Ker ponudniki medosebnih komunikacijskih storitev, neodvisnih od številke, običajno nimajo dejanskega nadzora nad prenosom signalov prek omrežja, je mogoče raven tveganja za take storitve v nekaterih pogledih šteti za manjšo kot pri tradicionalnih elektronskih komunikacijskih storitvah. Enako velja za medosebne komunikacijske storitve, ki uporabljajo številke in nimajo dejanskega nadzora nad prenosom signalov.

(51) Notranji trg je bolj odvisen od delovanja interneta kot kdaj koli prej. Storitve praktično vseh bistvenih in pomembnih subjektov so odvisne od storitev, ki se opravljajo prek interneta. Za zagotovitev nemotenega opravljanja storitev bistvenih in pomembnih subjektov je pomembno, da imajo javna elektronska komunikacijska omrežja, kot so na primer hrbtenična internetna omrežja ali podmorski komunikacijski kabli, vzpostavljene ustrezne ukrepe za kibernetsko varnost in da poročajo o incidentih v zvezi z njo.

(52) Kjer je ustrezno, bi morali subjekti obvestiti prejemnike storitev o specifičnih in pomembnih grožnjah ter ukrepih, ki jih lahko sprejmejo za ublažitev posledičnega tveganja za njih same. Zahteva glede obveščanja zadevnih prejemnikov o takih grožnjah subjektov ne bi smela odvezati obveznosti, da na svoje stroške sprejmejo

---

[22] Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (UL L 257, 28.8.2014, str. 73).

[23] Direktiva (EU) 2018/1972 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah (UL L 321, 17.12.2018, str. 36).

[24] Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

ustrezne in takojšnje ukrepe za preprečevanje ali odpravo vseh kibernetskih groženj in ponovno vzpostavitev običajne ravni varnosti storitve. Zagotavljanje takih informacij o varnostnih grožnjah prejemnikom bi moralo biti brezplačno.

(53) Zlasti bi morali ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev prejemnike storitve obvestiti o specifičnih in pomembnih kibernetskih grožnjah ter ukrepih, ki jih lahko sprejmejo za zagotovitev varnosti svojih komunikacij, na primer z uporabo posebnih vrst programske opreme ali tehnologij šifriranja.

(54) Za zaščito varnosti elektronskih komunikacijskih omrežij in storitev bi bilo treba spodbujati uporabo šifriranja, zlasti šifriranja od konca do konca, ki bi morala biti po potrebi obvezna za ponudnike takih storitev in omrežij v skladu z načeloma privzete in vgrajene varnosti ter zasebnosti za namene člena 18. Uporabo šifriranja od konca do konca bi bilo treba uskladiti s pooblastili države članice, da zagotovi zaščito svojih bistvenih varnostnih interesov in javne varnosti ter dovoli preiskovanje, odkrivanje in pregon kaznivih dejanj v skladu s pravom Unije. Pri rešitvah za zakonit dostop do informacij v komunikacijah, šifriranih od konca do konca, bi se morala ohraniti učinkovitost šifriranja pri varovanju zasebnosti in varnosti komunikacij ter hkrati zagotoviti učinkovit odziv na kazniva dejanja.

(55) Direktiva določa dvostopenjski pristop k poročanju o incidentih za vzpostavitev ustreznega ravnovesja med, na eni strani, hitrim poročanjem, ki pomaga blažiti morebitno širjenje incidentov in omogoča subjektom, da zaprosijo za podporo, ter, na drugi strani, podrobnim poročanjem, pri katerem se pridobivajo dragocene izkušnje iz posameznih incidentov ter sčasoma poveča odpornost posameznih podjetij in celotnega sektorja proti kibernetskim grožnjam. Kadar se subjekti seznanijo z incidentom, bi se moralo od njih zahtevati, da v 24 urah predložijo začetno priglasitev, ki ji najpozneje čez en mesec sledi končno poročilo. Začetna priglasitev bi morala vključevati le informacije, ki so nujno potrebne za seznanitev pristojnih organov z incidentom in ki subjektu omogočajo, da po potrebi zaprosi za pomoč. V taki priglasitvi bi moralo biti, kjer je ustrezno, navedeno, ali je bil incident domnevno povzročen z nezakonitim ali zlonamernim dejanjem. Države članice bi morale zagotoviti, da se z zahtevo po predložitvi začetne priglasitve viri poročajočega subjekta ne preusmerijo z dejavnosti, povezanih z obvladovanjem incidentov, ki bi moralo biti prednostna naloga. Da bi države članice nadalje preprečile, da bi se zaradi obveznosti poročanja o incidentih bodisi viri preusmerili z upravljanja odzivov na incidente bodisi kako drugače ogrozila prizadevanja subjektov v zvezi s tem, bi morale tudi zagotoviti, da lahko zadevni subjekt v ustrezno utemeljenih primerih in v dogovoru s pristojnimi organi ali skupino CSIRT odstopa od rokov, tj. 24 ur za začetno priglasitev in enega meseca za končno poročilo.

(56) Bistveni in pomembni subjekti so pogosto v položaju, ko je treba zaradi obveznosti priglasitve, vključenih v različne pravne instrumente, o določenem incidentu zaradi njegovih značilnosti poročati različnim organom. Taki primeri ustvarjajo dodatna bremena in lahko tudi privedejo do negotovosti v zvezi z obliko in postopki takih priglasitev. Glede na navedeno in za poenostavitev poročanja o varnostnih incidentih bi morale države članice vzpostaviti *enotno vstopno točko* za vse priglasitve, ki se zahtevajo v skladu s to direktivo in tudi drugo zakonodajo Unije, kot sta Uredba (EU) 2016/679 in Direktiva 2002/58/ES. Agencija ENISA bi morala v sodelovanju s skupino za sodelovanje s smernicami oblikovati skupne predloge za priglasitev, s katerimi bi se poenostavile in racionalizirale informacije za poročanje, ki se zahtevajo s pravom Unije, ter zmanjšala bremena za podjetja.

(57) V primeru suma, da je incident povezan s hudimi kaznivimi dejanji po pravu Unije ali nacionalnem pravu, bi morale države članice bistvene in pomembne subjekte na podlagi veljavnih pravil o kazenskem postopku v skladu s pravom Unije spodbujati, da incident, za katerega sumijo, da je hudo kaznivo dejanje, prijavijo ustreznim organom kazenskega pregona. Kjer je ustrezno in brez poseganja v pravila o varstvu osebnih podatkov, ki se uporabljajo za Europol, je zaželeno, da Evropski center za boj proti kibernetski kriminaliteti (EC3) in agencija ENISA olajšata usklajevanje med pristojnimi organi in organi kazenskega pregona različnih držav članic.

(58) V številnih primerih je zaradi incidentov ogrožena varnost osebnih podatkov. V tem okviru bi morali pristojni organi v skladu z Direktivo 2002/58/ES sodelovati in si izmenjevati informacije o vseh pomembnih zadevah z organi za varstvo podatkov in nadzornimi organi.

(59) Vzdrževanje točnih in popolnih podatkovnih zbirk domenskih imen in podatkov o registraciji (tako imenovani podatki „WHOIS“) ter omogočanje zakonitega dostopa do takih podatkov sta bistveni za zagotavljanje varnosti, stabilnosti in odpornosti sistema domenskih imen, kar posledično prispeva k višji skupni ravni kibernetske varnosti v Uniji. Če obdelava vključuje osebne podatke, mora biti taka obdelava skladna s pravom Unije o varstvu podatkov.

(60) Razpoložljivost in pravočasna dostopnost teh podatkov za javne organe, vključno s pristojnimi organi po pravu Unije ali nacionalnem pravu za preprečevanje, preiskovanje ali pregon kaznivih dejanj, skupine CERT in CSIRT ter, kar zadeva podatke njihovih strank, ponudnike elektronskih komunikacijskih omrežij in storitev ter ponudnike tehnologij in storitev kibernetske varnosti, ki delujejo v imenu zadevnih strank, sta bistveni za preprečevanje zlorab sistema domenskih imena in boj proti njim, zlasti za preprečevanje in odkrivanje kibernetskih incidentov ter odzivanje nanje. Pri takem dostopu bi bilo treba spoštovati pravo Unije o varstvu podatkov, če je povezan z osebnimi podatki.

(61) Da bi zagotovili razpoložljivost točnih in popolnih podatkov o registraciji domenskih imen, bi morali registri vrhnjih domen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene (tako imenovani registratorji), zbirati podatke o registraciji domenskih imen ter zagotavljati njihovo celovitost in razpoložljivost. Zlasti bi morali registri vrhnjih domen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene, vzpostaviti politike in postopke za zbiranje ter vzdrževanje točnih in popolnih podatkov o registraciji ter za preprečevanje in popravljanje netočnih podatkov o registraciji v skladu s pravili Unije o varstvu podatkov.

(62) Registri vrhnjih domen in subjekti, ki zanje opravljajo storitve registracije domenskih imen, bi morali objaviti podatke o registraciji domenskih imen, ki ne spadajo na področje uporabe pravil Unije o varstvu podatkov, kot so podatki, ki se nanašajo na pravne osebe[25]. Registri vrhnjih domen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene, bi morali v skladu s pravom Unije o varstvu podatkov zakonit dostop do podatkov o registraciji posameznih domenskih imen v zvezi s fizičnimi osebami omogočiti tudi osebam, ki imajo upravičen razlog za dostop. Države članice bi morale zagotoviti, da se registri vrhnjih domen in subjekti, ki zanje

[25] Uvodna izjava 14 UREDBE (EU) 2016/679 EVROPSKEGA PARLAMENTA IN SVETA, v skladu s katero „[t]a uredba ne zajema obdelave osebnih podatkov glede pravnih oseb in zlasti družb, ustanovljenih kot pravne osebe, vključno z imenom in obliko ter kontaktnimi podatki pravne osebe“.

opravljajo storitve registracije domenskih imen, brez nepotrebnega odlašanja odzovejo na zahteve oseb, ki imajo upravičen razlog za dostop, glede razkritja podatkov o registraciji domenskih imen. Registri vrhnjih domen in subjekti, ki zanje opravljajo storitve registracije domenskih imen, bi morali vzpostaviti politike in postopke za objavo in razkritje podatkov o registraciji, vključno s sporazumi o ravni storitve, za obravnavanje zahtev oseb za dostop, ki imajo upravičen razlog za dostop. Postopek dostopa lahko vključuje tudi uporabo vmesnika, portala ali drugih tehničnih orodij za zagotovitev učinkovitega sistema za predložitev zahtev in dostopanje do podatkov o registraciji. Komisija lahko za spodbujanje usklajenih praks na notranjem trgu sprejme smernice o takih postopkih brez poseganja v pristojnosti Evropskega odbora za varstvo podatkov.

(63) Vsi bistveni in pomembni subjekti na podlagi te direktive bi morali spadati v sodno pristojnost države članice, kjer opravljajo svoje storitve. Če subjekt opravlja storitve v več kot eni državi članici, bi moral spadati v ločeno in sočasno sodno pristojnost vsake od teh držav članic. Pristojni organi teh držav članic bi morali sodelovati, si medsebojno pomagati in, kjer je ustrezno, izvajati skupne nadzorne ukrepe.

(64) Da bi se upoštevala čezmejna narava storitev in postopkov ponudnikov storitev sistema domenskih imen, registrov vrhnjih domenskih imen, ponudnikov omrežij za dostavo vsebine, ponudnikov storitev računalništva v oblaku, ponudnikov storitev podatkovnih centrov in ponudnikov digitalnih storitev, bi morala biti za te subjekte pristojna samo ena država članica. Sodno pristojnost bi bilo treba dodeliti državi članici, v kateri ima zadevni subjekt glavni sedež v Uniji. Merilo sedeža za namene te direktive pomeni dejansko izvajanje dejavnosti na podlagi stabilnih ureditev. Pravna oblika takih ureditev, bodisi prek izpostave bodisi prek podružnice, ki je pravna oseba, v tem pogledu ni odločujoči dejavnik. Izpolnjevanje tega merila ne bi smelo biti odvisno od tega, ali so omrežja in informacijski sistemi fizično locirani na tistem mestu; prisotnost in uporaba teh sistemov sami po sebi ne pomenita tega glavnega sedeža in zato nista odločilni merili za ugotavljanje glavnega sedeža. Glavni sedež bi moral biti kraj, kjer se v Uniji sprejemajo odločitve v zvezi z ukrepi za obvladovanje tveganj za kibernetsko varnost. To običajno ustreza kraju osrednje uprave podjetij v Uniji. Če se take odločitve ne sprejemajo v Uniji, bi bilo treba šteti, da je glavni sedež v državah članicah, kjer ima subjekt sedež z največjim številom zaposlenih v Uniji. Kadar storitve opravljajo povezane družbe, bi bilo treba glavni sedež obvladujoče družbe šteti za glavni sedež povezanih družb.

(65) V primerih, ko ponudnik storitev sistema domenskih imen, register vrhnjih domenskih imen, ponudnik omrežij za dostavo vsebine, ponudnik storitev računalništva v oblaku, ponudnik storitev podatkovnih centrov in ponudnik digitalnih storitev, ki nima sedeža v Uniji, ponuja storitve v Uniji, bi moral imenovati predstavnika. Da bi ugotovili, ali tak subjekt ponuja storitve v Uniji, bi bilo treba preveriti, ali je jasno, da namerava subjekt svoje storitve ponujati posameznikom v eni ali več državah članicah. Sama dostopnost v Uniji spletnega mesta subjekta ali posrednika ali elektronskega naslova in drugih kontaktnih podatkov ali uporaba jezika, ki se običajno uporablja v tretji državi, v kateri ima subjekt sedež, ne zadošča za določitev takšne namere. Vendar se lahko z dejavniki, kot je uporaba jezika ali valute, ki se običajno uporablja v eni ali več državah članicah, z možnostjo naročanja storitev v tem drugem jeziku, ali navedba strank ali uporabnikov, ki so v Uniji, jasno pokaže, da namerava subjekt ponujati storitve v Uniji. Predstavnik bi moral delovati v imenu subjekta, pristojni organi ali skupine CSIRT pa bi morali imeti možnost, da navežejo stik s predstavnikom. Predstavnik bi moral biti izrecno imenovan s pisnim pooblastilom subjekta, da v

njegovem imenu izvaja njegove obveznosti na podlagi te direktive, vključno s poročanjem o incidentih.

(66) Če se podatki, ki se v skladu z nacionalnim pravom ali pravom Unije štejejo za tajne, izmenjujejo, sporočajo ali drugače souporabljajo v skladu z določbami te direktive, bi se morala uporabljati ustrezna posebna pravila o ravnanju s tajnimi podatki.

(67) Ker so kibernetske grožnje vse bolj zapletene in izpopolnjene, so dobri ukrepi za odkrivanje in preprečevanje večinoma odvisni od redne izmenjave obveščevalnih podatkov o grožnjah in šibkih točkah med subjekti. Izmenjava informacij prispeva k večji ozaveščenosti o kibernetskih grožnjah, kar posledično krepi sposobnost subjektov za preprečevanje, da bi se grožnje spremenile v dejanske incidente, in subjektom omogoča, da bolje omejijo učinke incidentov in si učinkoviteje opomorejo. Videti je, da ob odsotnosti smernic na ravni Unije več dejavnikov ovira tako izmenjavo obveščevalnih podatkov, zlasti negotovost glede združljivosti s pravili o konkurenci in odgovornosti.

(68) Subjekte bi bilo zato treba spodbuditi, naj skupaj izkoristijo svoje individualno znanje in praktične izkušnje na strateški, taktični in operativni ravni, da bi tako okrepili svoje zmogljivosti za ustrezno ocenjevanje in spremljanje kibernetskih groženj, zaščito pred njimi in odzivanje nanje. Zato je treba omogočiti, da se na ravni Unije vzpostavijo mehanizmi za prostovoljne dogovore o izmenjavi informacij. V ta namen bi morale države članice dejavno podpirati in spodbujati tudi ustrezne subjekte, ki niso zajeti v področje uporabe te direktive, naj sodelujejo v takih mehanizmih za izmenjavo informacij. Taki mehanizmi bi se morali izvajati ob polnem spoštovanju pravil Unije o konkurenci in pravil prava Unije o varstvu podatkov.

(69) Obdelava osebnih podatkov v obsegu, nujno potrebnem in sorazmernem za zagotovitev varnosti omrežja in informacij, ki jo izvajajo subjekti, javni organi, skupine CERT in CSIRT ter ponudniki varnostnih tehnologij in storitev, bi morala pomeniti zakoniti interes zadevnega upravljavca podatkov, kot je navedeno v Uredbi (EU) 2016/679. To bi moralo vključevati ukrepe, povezane s preprečevanjem, odkrivanjem in analizo incidentov ter odzivanjem nanje, ukrepe za ozaveščanje v zvezi s posebnimi kibernetskimi grožnjami, izmenjavo informacij v okviru odpravljanja in usklajenega razkrivanja šibkih točk ter prostovoljno izmenjavo informacij o takih incidentih, pa tudi o kibernetskih grožnjah in šibkih točkah, kazalnikih ogroženosti, taktikah, tehnikah in postopkih, opozorilih glede kibernetske varnosti in orodjih za konfiguracijo. Taki ukrepi lahko zahtevajo obdelavo naslednjih vrst osebnih podatkov: naslovov IP, enotnih naslovov vira (URL), domenskih imen in elektronskih naslovov.

(70) Za okrepitev nadzornih pooblastil in ukrepov, ki pomagajo zagotavljati dejansko izpolnjevanje zahtev, bi bilo treba v tej direktivi določiti minimalni seznam nadzornih ukrepov in sredstev, s katerimi lahko pristojni organi nadzorujejo bistvene in pomembne subjekte. Poleg tega bi bilo treba s to direktivo vzpostaviti razlikovanje nadzorne ureditve med bistvenimi in pomembnimi subjekti, da bi se zagotovilo ustrezno ravnovesje med obveznostmi subjektov in pristojnih organov. Tako bi morala za bistvene subjekte veljati celovita ureditev nadzora (predhodni in naknadni nadzor), medtem ko bi morala za pomembne subjekte veljati manj stroga ureditev nadzora, to je le naknadni nadzor. Za te vrste subjektov to pomeni, da pomembnim subjektom ne bi bilo treba sistematično dokumentirati izpolnjevanja zahtev glede obvladovanja tveganj za kibernetsko varnost, pristojni organi pa bi morali uporabljati reaktivni naknadni

pristop k nadzoru in tako zanje ne bi veljala splošna obveznost nadzorovanja teh subjektov.

(71) Da bi bilo izvrševanje učinkovito, bi bilo treba določiti minimalni seznam upravnih sankcij za kršitve obveznosti glede obvladovanja tveganj za kibernetsko varnost in poročanja iz te direktive ter vzpostaviti jasen in skladen okvir za take sankcije po vsej Uniji. Ustrezno bi bilo treba upoštevati naravo, težo in trajanje kršitve, dejansko povzročeno škodo ali nastale izgube ali morebitno škodo ali izgube, ki bi lahko nastale, ali je kršitev namerna ali posledica malomarnosti, ukrepe, sprejete za preprečevanje ali omilitev nastale škode in/ali izgub, stopnjo odgovornosti ali vse zadevne predhodne kršitve, stopnjo sodelovanja s pristojnim organom in morebitne druge oteževalne ali olajševalne dejavnike. Za naložitev sankcij, vključno z upravnimi globami, bi morali veljati ustrezni postopkovni zaščitni ukrepi v skladu s splošnimi načeli prava Unije in Listine Evropske unije o temeljnih pravicah, vključno z učinkovitim sodnim varstvom in ustreznimi postopki.

(72) Za zagotovitev učinkovitega izvrševanja obveznosti, določenih v tej direktivi, bi morali biti vsi pristojni organi pooblaščeni, da naložijo ali zahtevajo naložitev upravnih glob.

(73) Kadar se upravne globe naložijo podjetjem, bi se podjetje v te namene moralo razumeti kot podjetje v skladu s členoma 101 in 102 PDEU. Kadar se upravne globe naložijo osebam, ki niso podjetje, bi moral nadzorni organ pri določanju ustreznega zneska globe upoštevati splošno raven dohodka v državi članici in ekonomski položaj osebe. Države članice bi morale določiti, ali bi se morale upravne globe uporabljati tudi za javne organe in v kakšnem obsegu. Naložitev upravne globe ne vpliva na uporabo drugih pooblastil pristojnih organov ali drugih sankcij, določenih v nacionalnih pravilih, s katerimi je prenesena ta direktiva.

(74) Državam članicam bi moralo biti omogočeno, da določijo pravila o kazenskih sankcijah za kršitve nacionalnih pravil, s katerimi je prenesena ta direktiva. Naložitev kazenskih sankcij zaradi kršitev takih nacionalnih pravil in z njimi povezanih upravnih kazni pa ne bi smela voditi h kršitvi načela *ne bis in idem,* kakor ga razlaga Sodišče.

(75) Kadar ta direktiva ne zagotavlja harmonizacije upravnih kazni ali po potrebi v drugih primerih, denimo v primerih hudih kršitev obveznosti, določenih v tej direktivi, bi morale države članice uporabiti sistem, ki zagotavlja učinkovite, sorazmerne in odvračilne sankcije. Narava takšnih sankcij, kazenskih ali upravnih, bi morala biti določena s pravom držav članic.

(76) Za nadaljnjo krepitev učinkovitosti in odvračilnosti sankcij, ki se uporabljajo za kršitve obveznosti, določenih v skladu s to direktivo, bi morali biti pristojni organi pooblaščeni za uporabo sankcij, ki vključujejo začasni preklic certifikata ali dovoljenja za del storitev ali vse storitve, ki jih opravlja bistveni subjekt, in začasno prepoved opravljanja vodstvenih funkcij za fizično osebo. Glede na njihovo resnost in vpliv na dejavnosti subjektov ter končno na potrošnike bi se morale take sankcije uporabljati le sorazmerno z resnostjo kršitve in ob upoštevanju posebnih okoliščin posameznega primera, vključno s tem, ali je kršitev namerna ali posledica malomarnosti, ter ukrepi, sprejetimi za preprečevanje ali ublažitev škode in/ali izgub. Take sankcije bi se morale uporabljati le kot *ultima ratio*, kar pomeni šele potem, ko so bili uporabljeni vsi drugi ustrezni izvršilni ukrepi, določeni v tej direktivi, in le dokler subjekti, za katere se uporabijo, ne sprejmejo potrebnih ukrepov za odpravo pomanjkljivosti ali izpolnitev zahtev pristojnega organa, zaradi katerih so bile takšne sankcije naložene. Za uvedbo takšnih sankcij bi morali veljati ustrezni postopkovni zaščitni ukrepi v skladu s

splošnimi načeli prava Unije in Listine Evropske unije o temeljnih pravicah, vključno z učinkovitim sodnim varstvom, ustreznimi postopki, domnevo nedolžnosti in pravico do obrambe.

(77) S to direktivo bi bilo treba določiti pravila sodelovanja med pristojnimi in nadzornimi organi v skladu z Uredbo (EU) 2016/679 za obravnavanje kršitev, povezanih z osebnimi podatki.

(78) Ta direktiva bi morala biti namenjena zagotavljanju visoke ravni odgovornosti za ukrepe za obvladovanje tveganj za kibernetsko varnost in obveznosti poročanja na ravni organizacij. Zato bi morali upravni organi subjektov, ki spadajo na področje uporabe te direktive, odobriti ukrepe za obvladovanje tveganj za kibernetsko varnost in nadzorovati njihovo izvajanje.

(79) Uvesti bi bilo treba mehanizem medsebojnih strokovnih pregledov, ki bi strokovnjakom, ki jih imenujejo države članice, omogočal oceno izvajanja politik na področju kibernetske varnosti, vključno z ravnjo zmogljivosti in razpoložljivih virov držav članic.

(80) Zaradi upoštevanja novih kibernetskih groženj, tehnološkega razvoja ali sektorskih posebnosti bi bilo treba na Komisijo v skladu s členom 290 PDEU prenesti pooblastilo za sprejemanje aktov v zvezi z elementi, ki se nanašajo na ukrepe za obvladovanje tveganj, ki jih zahteva ta direktiva. Na Komisijo bi bilo treba prenesti tudi pooblastilo za sprejetje delegiranih aktov, s katerimi se določi, katere kategorije bistvenih subjektov morajo pridobiti certifikat in na podlagi katerih določenih evropskih certifikacijskih shem za kibernetsko varnost. Zlasti je pomembno, da se Komisija pri svojem pripravljalnem delu ustrezno posvetuje, tudi na ravni strokovnjakov, in da se ta posvetovanja izvedejo v skladu z načeli iz Medinstitucionalnega sporazuma z dne 13. aprila 2016 o boljši pripravi zakonodaje[26]. Da bi se zlasti zagotovilo enakopravno sodelovanje pri pripravi delegiranih aktov, Evropski parlament in Svet vse dokumente prejmeta sočasno s strokovnjaki iz držav članic, njuni strokovnjaki pa se lahko sistematično udeležujejo sestankov strokovnih skupin Komisije, ki zadevajo pripravo delegiranih aktov.

(81) Da bi se zagotovili enotni pogoji za izvajanje ustreznih določb te direktive v zvezi s postopkovnimi ureditvami, potrebnimi za delovanje skupine za sodelovanje, tehničnimi elementi, povezanimi z ukrepi za obvladovanje tveganj, ali vrsto informacij, obliko in postopkom priglasitev incidentov, bi bilo treba na Komisijo prenesti izvedbena pooblastila. Ta pooblastila bi bilo treba izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta[27].

(82) Komisija bi morala redno v posvetovanju z zainteresiranimi stranmi pregledovati to direktivo, zlasti da bi ugotovila, ali jo je treba prilagoditi spremenjenim družbenim, političnim, tehnološkim ali tržnim razmeram.

(83) Ker cilja te direktive, in sicer doseganja visoke skupne ravni kibernetske varnosti v Uniji, države članice ne morejo zadovoljivo doseči, temveč se zaradi učinkov ukrepov lažje doseže na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 Pogodbe o Evropski uniji. V skladu z načelom sorazmernosti

[26] UL L 123, 12.5.2016, str. 1.

[27] Uredba (EU) št. 182/2011 Evropskega parlamenta in Sveta z dne 16. februarja 2011 o določitvi splošnih pravil in načel, na podlagi katerih države članice nadzirajo izvajanje izvedbenih pooblastil Komisije (UL L 55, 28.2.2011, str. 13).

iz navedenega člena ta direktiva ne presega tistega, kar je potrebno za doseganje navedenega cilja.

(84) Ta direktiva upošteva temeljne pravice in načela Listine Evropske unije o temeljnih pravicah, zlasti pravico do spoštovanja zasebnega življenja in komunikacij, varstvo osebnih podatkov, svobodo gospodarske pobude, lastninsko pravico, pravico do učinkovitega pravnega sredstva in nepristranskega sodišča in pravico do izjave. To direktivo bi bilo treba izvajati v skladu s temi pravicami in načeli –

SPREJELA NASLEDNJO DIREKTIVO:

POGLAVJE I

Splošne določbe

Člen 1

Predmet urejanja

1. Ta direktiva določa ukrepe za zagotovitev visoke skupne ravni kibernetske varnosti v Uniji.

2. V ta namen ta direktiva:

(a) določa obveznosti za države članice, da sprejmejo nacionalne strategije za kibernetsko varnost, imenujejo pristojne nacionalne organe, enotne kontaktne točke in skupine za odzivanje na incidente na področju računalniške varnosti (CSIRT);

(b) določa obveznosti glede obvladovanja tveganj za kibernetsko varnost in poročanja za subjekte, ki se v skladu s Prilogo I štejejo za bistvene subjekte, in subjekte, ki se v skladu s Prilogo II štejejo za pomembne subjekte;

(c) določa obveznosti glede izmenjave informacij o kibernetski varnosti.

Člen 2

Področje uporabe

1. Ta direktiva se uporablja za javne in zasebne subjekte, ki se v skladu s Prilogo I štejejo za bistvene subjekte, ter za javne in zasebne subjekte, ki se v skladu s Prilogo II štejejo za pomembne subjekte. Ta direktiva se ne uporablja za subjekte, ki se štejejo za mikro in mala podjetja v smislu Priporočila Komisije 2003/361/ES[28].

2. Vendar pa se ta direktiva uporablja tudi za subjekte iz prilog I in II ne glede na njihovo velikost, če:

(a) storitve opravlja eden ali več naslednjih subjektov:

[28] Priporočilo Komisije 2003/361/ES z dne 6. maja 2003 o opredelitvi mikro, malih in srednjih podjetij (UL L 124, 20.5.2003, str. 36).

(i) ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev iz točke 8 Priloge I;

(ii) ponudniki storitev zaupanja iz točke 8 Priloge I;

(iii) registri vrhnjih domenskih imen in ponudniki storitev sistema domenskih imen (DNS) iz točke 8 Priloge I;

(b) je subjekt javna uprava, kot je opredeljen v točki 23 člena 4;

(c) je subjekt edini ponudnik storitve v državi članici;

(d) bi morebitna motnja pri opravljanju storitve subjekta lahko vplivala na javni red, javno varnost ali javno zdravje;

(e) bi morebitna motnja pri opravljanju storitve subjekta lahko povzročila sistemska tveganja, zlasti za sektorje, v katerih bi lahko taka motnja imela čezmejni vpliv;

(f) je subjekt kritičen zaradi njegovega posebnega pomena na regionalni ali nacionalni ravni za določen sektor ali vrsto storitve ali za druge neodvisne sektorje v državi članici;

(g) je subjekt opredeljen kot kritični subjekt v skladu z Direktivo (EU) XXXX/XXXX Evropskega parlamenta in Sveta[29] [direktiva o odpornosti kritičnih subjektov] ali kot subjekt, enakovreden kritičnemu subjektu v skladu s členom 7 navedene direktive.

Države članice pripravijo seznam subjektov, opredeljenih v skladu s točkami (b) do (f), in ga predložijo Komisiji do [6 mesecev po roku za prenos]. Države članice redno oziroma vsaj vsaki dve leti pregledajo seznam ter ga po potrebi posodobijo.

3. Ta direktiva ne posega v pristojnosti držav članic v zvezi z ohranjanjem javne varnosti, obrambe in nacionalne varnosti v skladu s pravom Unije.

4. Ta direktiva se uporablja brez poseganja v Direktivo Sveta 2008/114/ES[30] ter direktivi 2011/93/EU[31] in 2013/40/EU[32] Evropskega parlamenta in Sveta.

5. Brez poseganja v člen 346 PDEU se informacije, ki so zaupne v skladu s predpisi Unije in nacionalnimi predpisi, na primer o poslovni tajnosti, s Komisijo in drugimi ustreznimi organi izmenjajo le, če je takšna izmenjava potrebna za uporabo te direktive. Izmenjava informacij je omejena na obseg, ki je ustrezen in sorazmeren glede na namen takšne izmenjave. Pri izmenjavi informacij se ohranijo zaupnost zadevnih informacij ter zaščitijo varnost in poslovni interesi bistvenih ali pomembnih subjektov.

6. Kadar se z določbami sektorskih aktov prava Unije zahteva, da bistveni ali pomembni subjekti bodisi sprejmejo ukrepe za obvladovanje tveganj za kibernetsko

---

29 *[vstaviti polni naslov in sklic na objavo v UL, ko bosta znana]*.

30 Direktiva Sveta 2008/114/ES z dne 8. decembra 2008 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe po izboljšanju njene zaščite (UL L 345, 23.12.2008, str. 75).

31 Direktiva 2011/93/EU Evropskega parlamenta in Sveta z dne 13. decembra 2011 o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ (UL L 335, 17.12.2011, str. 1).

32 Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa Sveta 2005/222/PNZ (UL L 218, 14.8.2013, str. 8).

varnost bodisi priglasijo incidente ali pomembne kibernetske grožnje, in kadar so takšne zahteve po učinku vsaj enakovredne obveznostim iz te direktive, se ustrezne določbe te direktive, vključno z določbo o nadzoru in izvrševanju iz poglavja VI, ne uporabljajo.

Člen 3

Minimalna harmonizacija

Države članice lahko brez poseganja v svoje druge obveznosti na podlagi prava Unije v skladu s to direktivo sprejmejo ali ohranijo določbe, ki zagotavljajo višjo raven kibernetske varnosti.

Člen 4

Opredelitev pojmov

V tej direktivi se uporabljajo naslednje opredelitve pojmov:

(1) „omrežje in informacijski sistem“ pomeni:

(a) elektronsko komunikacijsko omrežje v smislu člena 2(1) Direktive (EU) 2018/1972;

(b) vsako napravo ali skupino med seboj povezanih ali sorodnih naprav, od katerih ena ali več na podlagi programa opravlja samodejno obdelavo digitalnih podatkov;

(c) digitalne podatke, ki jih elementi iz točk (a) in (b) shranjujejo, obdelujejo, pridobivajo ali prenašajo za namene njihovega delovanja, uporabe, varovanja in vzdrževanja;

(2) „varnost omrežij in informacijskih sistemov“ pomeni zmožnost omrežij in informacijskih sistemov, da na določeni ravni zaupanja preprečijo vse dogodke, ki ogrožajo razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali povezanih storitev, ki jih navedena omrežja in informacijski sistemi zagotavljajo ali so prek njih dostopni;

(3) „kibernetska varnost“ pomeni kibernetsko varnost v smislu člena 2(1) Uredbe (EU) št. 2019/881 Evropskega parlamenta in Sveta[33];

(4) „nacionalna strategija za kibernetsko varnost“ pomeni skladen okvir države članice, ki določa strateške cilje in prednostne naloge na področju varnosti omrežij in informacijskih sistemov v zadevni državi članici;

(5) „incident“ pomeni vsak dogodek, ki ogroža razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali povezanih storitev, ki jih navedena omrežja in informacijski sistemi zagotavljajo ali so prek njih dostopni;

[33] Uredba (EU) 2019/881 Evropskega Parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15).

(6) „obvladovanje incidentov“ pomeni vsa dejanja in postopke, namenjene odkrivanju, analizi in zajezitvi incidentov ter odzivanju nanje;

(7) „kibernetska grožnja“ pomeni kibernetsko grožnjo v smislu člena 2(8) Uredbe 2019/881;

(8) „šibka točka“ pomeni pomanjkljivost, dovzetnost ali napako sredstva, sistema, postopka ali nadzora, ki jo kibernetska grožnja lahko izkoristi;

(9) „predstavnik“ pomeni vsako fizično ali pravno osebo s sedežem v Uniji, ki je izrecno imenovana, da deluje v imenu (i) ponudnika storitev sistema domenskih imen (DNS), registra vrhnjih domenskih imen (TLD), ponudnika storitev računalništva v oblaku, ponudnika storitev podatkovnega centra, ponudnika omrežja za dostavo vsebine iz točke 8 Priloge I ali (ii) subjektov iz točke 6 Priloge II, ki nimajo sedeža v Uniji, s katerim lahko nacionalni pristojni organ ali skupina CSIRT vzpostavi stik namesto z zadevnim subjektom, kar zadeva obveznosti tega subjekta na podlagi te direktive;

(10) „standard“ pomeni standard v smislu člena 2(1) Uredbe (EU) št. 1025/2012 Evropskega parlamenta in Sveta[34];

(11) „tehnična specifikacija“ pomeni tehnično specifikacijo v smislu člena 2(4) Uredbe (EU) št. 1025/2012;

(12) „stičišče omrežij“ pomeni omrežno zmogljivost, ki omogoča medsebojno povezavo več kot dveh neodvisnih omrežij (avtonomnih sistemov), predvsem zaradi izmenjave internetnega prometa; stičišče omrežij zagotavlja medsebojno povezavo le avtonomnih sistemov; stičišče omrežij omogoča izmenjavo internetnega prometa med katerima koli sodelujočima avtonomnima sistemoma, brez prehoda prek tretjega avtonomnega sistema, prav tako pa ne spreminja takšnega prometa ali kako drugače posega vanj;

(13) „sistem domenskih imen (DNS)“ pomeni hierarhičen porazdeljen sistem dodeljevanja imen, ki končnim uporabnikom omogoča dostop do storitev in virov na internetu;

(14) „ponudnik storitev sistema domenskih imen (DNS)“ pomeni subjekt, ki opravlja storitve rekurzivnega ali avtoritativnega razreševanja domenskih imen za končne uporabnike interneta in druge ponudnike storitev DNS;

(15) „register vrhnjih domenskih imen“ pomeni subjekt, ki mu je bila dodeljena določena vrhnja domena in ki je odgovoren za upravljanje vrhnje domene, vključno z registracijo domenskih imen pod vrhnjo domeno in tehničnim upravljanjem vrhnje domene, vključno z upravljanjem njenih imenskih strežnikov, vzdrževanjem njenih podatkovnih zbirk in porazdelitvijo območnih datotek vrhnje domene po imenskih strežnikih;

(16) „digitalna storitev“ pomeni storitev v smislu člena 1(1)(b) Direktive (EU) 2015/1535 Evropskega parlamenta in Sveta[35];

---

[34] Uredba (EU) št. 1025/2012 Evropskega parlamenta in Sveta z dne 25. oktobra 2012 o evropski standardizaciji, spremembi direktiv Sveta 89/686/EGS in 93/15/EGS ter direktiv 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES in 2009/105/ES Evropskega parlamenta in Sveta ter razveljavitvi Sklepa Sveta 87/95/EGS in Sklepa št. 1673/2006/ES Evropskega parlamenta in Sveta (UL L 316,14.11.2012, str. 12).

(17) „spletna tržnica“ pomeni digitalno storitev v smislu člena 2(n) Direktive 2005/29/ES Evropskega parlamenta in Sveta[36];

(18) „spletni iskalnik“ pomeni digitalno storitev v smislu člena 2(5) Uredbe (EU) 2019/1150 Evropskega parlamenta in Sveta[37];

(19) „storitev računalništva v oblaku“ pomeni digitalno storitev, ki omogoča upravljanje na zahtevo in širok oddaljeni dostop do prožnega in po obsegu prilagodljivega nabora deljivih in porazdeljenih računalniških virov;

(20) „storitev podatkovnega centra“ pomeni storitev, ki vključuje strukture ali skupine struktur, namenjene centralizirani namestitvi, medsebojnemu povezovanju in delovanju opreme za informacijsko tehnologijo in omrežne opreme za storitve shranjevanja, obdelave in prenosa podatkov skupaj z vsemi zmogljivostmi in infrastrukturami za distribucijo električne energije in okoljski nadzor;

(21) „omrežje za dostavo vsebin“ pomeni mrežo geografsko porazdeljenih strežnikov za zagotavljanje visoke razpoložljivosti, dostopnosti ali hitre dostave digitalnih vsebin in storitev uporabnikom interneta v imenu ponudnikov vsebin in storitev;

(22) „platforma za storitve družbenega mreženja“ pomeni platformo, ki končnim uporabnikom omogoča, da se povezujejo, si izmenjujejo vsebine, se spoznavajo in komunicirajo med seboj prek več naprav ter zlasti prek klepetov, objav, videoposnetkov in priporočil;

(23) „subjekt javne uprave“ pomeni subjekt v državi članici, ki izpolnjuje naslednja merila:

(a) je ustanovljen za izpolnitev potreb v splošnem interesu in ni industrijske ali komercialne narave;

(b) je pravna oseba;

(c) ga večinoma financirajo država, regionalni organ ali druge osebe javnega prava; ali je pod upravljavskim nadzorom takih organov ali oseb; ali ima upravni, vodstveni ali nadzorni odbor, katerega več kot polovico članov imenujejo država, regionalni organi ali druge osebe javnega prava;

(d) ima pooblastilo, da na fizične ali pravne osebe naslovi upravne ali regulativne odločbe, ki vplivajo na njihove pravice na področju čezmejnega gibanja oseb in pretoka blaga, storitev ali kapitala.

Subjekti javne uprave, ki izvajajo dejavnosti na področjih javne varnosti, kazenskega pregona, obrambe ali nacionalne varnosti, so izključeni;

---

35 Direktiva (EU) 2015/1535 Evropskega parlamenta in Sveta z dne 9. septembra 2015 o določitvi postopka za zbiranje informacij na področju tehničnih predpisov in pravil za storitve informacijske družbe (UL L 241, 17.9.2015, str. 1).

36 Direktiva Evropskega parlamenta in Sveta 2005/29/ES z dne 11. maja 2005 o nepoštenih poslovnih praksah podjetij v razmerju do potrošnikov na notranjem trgu ter o spremembi Direktive Sveta 84/450/EGS, direktiv Evropskega parlamenta in Sveta 97/7/ES, 98/27/ES in 2002/65/ES ter Uredbe (ES) št. 2006/2004 Evropskega parlamenta in Sveta (Direktiva o nepoštenih poslovnih praksah) (UL L 149, 11.6.2005, str. 22).

37 Uredba (EU) 2019/1150 Evropskega parlamenta in Sveta z dne 20. junija 2019 o spodbujanju pravičnosti in preglednosti za poslovne uporabnike spletnih posredniških storitev (UL L 186, 11.7.2019, str. 57).

(24) „subjekt“ pomeni vsako fizično ali pravno osebo, ki je ustanovljena in priznana kot taka po nacionalnem pravu njenega kraja sedeža ter lahko v svojem imenu uveljavlja pravice in prevzema obveznosti;

(25) „bistveni subjekt“ pomeni vsak subjekt, ki je v Prilogi I naveden kot bistveni subjekt;

(26) „pomembni subjekt“ pomeni vsak subjekt, ki je v Prilogi II naveden kot pomembni subjekt;

POGLAVJE II

Usklajeni regulativni okviri za kibernetsko varnost

Člen 5

Nacionalna strategija za kibernetsko varnost

1. Vsaka država članica sprejme nacionalno strategijo za kibernetsko varnost, v kateri so opredeljeni strateški cilji ter ustrezni ukrepi politike in regulativni ukrepi za doseganje in ohranjanje visoke ravni kibernetske varnosti. Nacionalna strategija za kibernetsko varnost vključuje zlasti naslednje:

   (a) opredelitev ciljev in prednostnih nalog strategije držav članic za kibernetsko varnost;

   (b) okvir upravljanja za doseganje navedenih ciljev in prednostnih nalog, vključno s politikami iz odstavka 2 ter vlogami in odgovornostmi javnih organov in subjektov ter drugih ustreznih akterjev;

   (c) oceno za opredelitev ustreznih sredstev in tveganj za kibernetsko varnost v zadevni državi članici;

   (d) opredelitev ukrepov za zagotovitev pripravljenosti na incidente, odzivanja nanje in okrevanja po njih, vključno s sodelovanjem med javnim in zasebnim sektorjem;

   (e) seznam različnih organov in akterjev, vključenih v izvajanje nacionalne strategije za kibernetsko varnost;

   (f) okvir politike za okrepljeno usklajevanje med pristojnimi organi iz te direktive in direktive (EU) XXXX/XXXX Evropskega parlamenta in Sveta[38] [direktiva o odpornosti kritičnih subjektov] za izmenjavo informacij o incidentih in kibernetskih grožnjah ter izvajanje nadzornih nalog.

2. Države članice kot del nacionalne strategije za kibernetsko varnost sprejmejo zlasti naslednje politike:

   (a) politiko za obravnavanje kibernetske varnosti v dobavni verigi proizvodov in storitev IKT, ki jih bistveni in pomembni subjekti uporabljajo za opravljanje svojih storitev;

[38] *[vstaviti polni naslov in sklic na objavo v UL, ko bosta znana]*.

(b) smernice v zvezi z vključitvijo in specifikacijo zahtev za proizvode in storitve IKT pri javnem naročanju, povezanih s kibernetsko varnostjo;

(c) politiko za spodbujanje in olajšanje usklajenega razkrivanja šibkih točk v smislu člena 6;

(d) politiko, povezano z ohranjanjem splošne razpoložljivosti in celovitosti javnega jedra odprtega interneta;

(e) politiko za spodbujanje in razvoj znanj in spretnosti, ozaveščanja ter raziskovalnih in razvojnih pobud na področju kibernetske varnosti;

(f) politiko za podpiranje akademskih in raziskovalnih institucij pri razvoju orodij in varne omrežne infrastrukture za kibernetsko varnost;

(g) politiko, ustrezne postopke in ustrezna orodja za izmenjavo informacij za podpiranje prostovoljne izmenjave informacij o kibernetski varnosti med podjetji v skladu s pravom Unije;

(h) politiko za obravnavanje posebnih potreb MSP, zlasti tistih, ki so izključena s področja uporabe te direktive, v zvezi z usmeritvami in podporo pri povečevanju njihove odpornosti proti kibernetskim grožnjam.

3. Države članice Komisiji priglasijo svoje nacionalne strategije za kibernetsko varnost v treh mesecih od njihovega sprejetja. Države članice lahko iz priglasitve izključijo nekatere informacije, če in kolikor je to nujno potrebno za ohranitev nacionalne varnosti.

4. Države članice vsaj vsaka štiri leta ocenijo svoje nacionalne strategije za kibernetsko varnost na podlagi ključnih kazalnikov uspešnosti in jih po potrebi spremenijo. Agencija Evropske unije za kibernetsko varnost (ENISA) na zahtevo pomaga državam članicam pri razvoju nacionalne strategije in ključnih kazalnikov uspešnosti za oceno strategije.

Člen 6

Usklajeno razkrivanje šibkih točk in evropski register šibkih točk

1. Vsaka država članica imenuje eno od svojih skupin CSIRT iz člena 9 za koordinatorko za usklajeno razkrivanje šibkih točk. Imenovana skupina CSIRT deluje kot zaupanja vredna posrednica, ki po potrebi olajšuje sodelovanje med poročajočim subjektom in proizvajalcem ali ponudnikom proizvodov ali storitev IKT. Če se sporočena šibka točka nanaša na več proizvajalcev ali ponudnikov proizvodov ali storitev IKT v Uniji, imenovana skupina CSIRT vsake zadevne države članice sodeluje z mrežo skupin CSIRT.

2. Agencija ENISA razvije in vzdržuje evropski register šibkih točk. V ta namen agencija ENISA vzpostavi in vzdržuje ustrezne informacijske sisteme, politike in postopke, zlasti z namenom omogočanja pomembnim in bistvenim subjektom ter njihovim dobaviteljem omrežnih in informacijskih sistemov, da razkrijejo in evidentirajo šibke točke proizvodov in storitev IKT ter zagotovijo dostop do informacij o šibkih točkah, vsebovanih v registru, vsem zainteresiranim stranem. Register vključuje zlasti informacije, ki opisujejo šibko točko, prizadeti proizvod ali storitev IKT ter resnost šibke točke v smislu okoliščin, v katerih jo je mogoče izkoristiti, razpoložljivost povezanih popravkov ter, če popravki niso na voljo,

smernice, naslovljene na uporabnike proizvodov in storitev s šibkimi točkami, o načinih za zmanjšanje tveganj, ki izhajajo iz razkritih šibkih točk.

Člen 7

Nacionalni okviri za krizno upravljanje kibernetske varnosti

1. Vsaka država članica imenuje enega ali več pristojnih organov, odgovornih za upravljanje velikih incidentov in kriz. Države članice zagotovijo, da imajo pristojni organi ustrezne vire za učinkovito in uspešno opravljanje nalog, ki so jim bile dodeljene.
2. Vsaka država članica določi zmogljivosti, sredstva in postopke, ki se lahko uporabijo v primeru krize za namene te direktive.
3. Vsaka država članica sprejme nacionalni načrt odzivanja na kibernetske incidente in krize, v katerem so opredeljeni cilji in načini upravljanja velikih kibernetskih incidentov in kriz. V načrtu se določijo zlasti:
   (a) cilji nacionalnih ukrepov in dejavnosti za pripravljenost;
   (b) naloge in odgovornosti pristojnih nacionalnih organov;
   (c) postopki za obvladovanje kriz in kanali za izmenjavo informacij;
   (d) ukrepi za pripravljenost, vključno z vajami in dejavnostmi usposabljanja;
   (e) ustrezne vključene javne in zasebne zainteresirane strani ter infrastruktura;
   (f) nacionalni postopki in ureditve med ustreznimi nacionalnimi organi za zagotovitev učinkovitega sodelovanja države članice pri usklajenem upravljanju velikih kibernetskih incidentov in kriz na ravni Unije ter njegove podpore.
4. Države članice Komisijo obvestijo o imenovanju svojih pristojnih organov iz odstavka 1 ter predložijo svoje nacionalne načrte odzivanja na kibernetske incidente in krize iz odstavka 3 v treh mesecih od zadevnega imenovanja in sprejetja navedenih načrtov. Države članice lahko iz načrta izključijo določene informacije, če in kolikor je to nujno potrebno za njihovo nacionalno varnost.

Člen 8

Pristojni nacionalni organi in enotne kontaktne točke

1. Vsaka država članica imenuje enega ali več pristojnih organov, odgovornih za kibernetsko varnost in nadzorne naloge iz poglavja VI te direktive. Države članice lahko v ta namen imenujejo obstoječi organ ali obstoječe organe.
2. Pristojni organi iz odstavka 1 spremljajo uporabo te direktive na nacionalni ravni.
3. Vsaka država članica imenuje eno nacionalno enotno kontaktno točko za kibernetsko varnost (v nadaljnjem besedilu: enotna kontaktna točka). Kadar država članica imenuje le en pristojni organ, je ta tudi enotna kontaktna točka te države članice.
4. Vsaka enotna kontaktna točka ima povezovalno vlogo in tako zagotavlja čezmejno sodelovanje organov države članice z ustreznimi organi drugih držav članic ter

medsektorsko sodelovanje z drugimi pristojnimi nacionalnimi organi v svoji državi članici.

5. Države članice zagotovijo, da imajo pristojni organi iz odstavka 1 in enotne kontaktne točke ustrezne vire, da učinkovito in uspešno opravljajo dodeljene naloge ter tako izpolnjujejo cilje te direktive. Države članice zagotovijo učinkovito, uspešno in varno sodelovanje imenovanih predstavnikov v skupini za sodelovanje iz člena 12.

6. Vsaka država članica Komisijo brez nepotrebnega odlašanja uradno obvesti o imenovanju pristojnega organa iz odstavka 1 in enotne kontaktne točke iz odstavka 3, njunih nalogah in vseh poznejših spremembah, povezanih z določitvijo in nalogami. Vsaka država članica njihovo imenovanje objavi. Komisija objavi seznam imenovanih enotnih kontaktnih točk.

Člen 9

Skupine za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT)

1. Vsaka država članica imenuje eno ali več skupin CSIRT, ki izpolnjujejo zahteve iz člena 10(1) ter so pristojne za obvladovanje incidentov v skladu z natančno določenim postopkom, pri čemer zajame vsaj sektorje, podsektorje ali subjekte iz prilog I in II. Skupina CSIRT se lahko ustanovi v okviru pristojnega organa iz člena 8.

2. Države članice zagotovijo, da ima vsaka skupina CSIRT ustrezne vire za učinkovito izvajanje svojih nalog iz člena 10(2).

3. Države članice zagotovijo, da ima vsaka skupina CSIRT na voljo ustrezno, varno in odporno komunikacijsko in informacijsko infrastrukturo za izmenjavo informacij z bistvenimi in pomembnimi subjekti ter drugimi ustreznimi zainteresiranimi stranmi. V ta namen države članice zagotovijo, da skupine CSIRT prispevajo k uvajanju orodij za varno izmenjavo informacij.

4. Skupine CSIRT sodelujejo in si, kjer je ustrezno, v skladu s členom 26 izmenjujejo ustrezne informacije z zaupanja vrednimi sektorskimi ali medsektorskimi skupnostmi bistvenih in pomembnih subjektov.

5. Skupine CSIRT sodelujejo pri medsebojnih strokovnih pregledih, organiziranih v skladu s členom 16.

6. Države članice zagotovijo učinkovito, uspešno in varno sodelovanje svojih skupin CSIRT v mreži skupin CSIRT iz člena 13.

7. Države članice brez nepotrebnega odlašanja obvestijo Komisijo o skupinah CSIRT, imenovanih v skladu z odstavkom 1, skupini CSIRT koordinatorki, imenovani v skladu s členom 6(1), in njihovih ustreznih nalogah, določenih v zvezi s subjekti iz prilog I in II.

8. Države članice lahko pri oblikovanju nacionalnih skupin CSIRT zaprosijo za pomoč agencijo ENISA.

Člen 10

Zahteve in naloge skupin CSIRT

1. Skupine CSIRT izpolnjujejo naslednje zahteve:

   (a) skupine CSIRT zagotavljajo visoko stopnjo razpoložljivosti svojih komunikacijskih storitev, tako da preprečujejo posamezne točke odpovedi in vzpostavijo več kanalov, po katerih se drugi lahko kadar koli obrnejo nanje in one obrnejo na druge. Skupine CSIRT jasno opredelijo komunikacijske kanale ter o njih obvestijo uporabnike in partnerje;

   (b) uradi skupin CSIRT in podporni informacijski sistemi se nahajajo na varnih krajih;

   (c) skupine CSIRT imajo ustrezen sistem za upravljanje in usmerjanje zahtevkov, zlasti da se poenostavi njihova učinkovita in uspešna predaja;

   (d) skupine CSIRT imajo ustrezno osebje, s katerim lahko zagotovijo stalno razpoložljivost;

   (e) skupine CSIRT imajo redundantne sisteme in nadomestni delovni prostor, da se zagotovi neprekinjeno izvajanje njihovih storitev;

   (f) skupine CSIRT imajo možnost, da sodelujejo v mednarodnih mrežah za sodelovanje.

2. Skupine CSIRT imajo naslednje naloge:

   (a) spremljanje kibernetskih groženj, šibkih točk in incidentov na nacionalni ravni;

   (b) zagotavljanje zgodnjega opozarjanja, opozoril, obvestil in razširjanja informacij o kibernetskih grožnjah, šibkih točkah in incidentih bistvenim in pomembnim subjektom ter drugim ustreznim zainteresiranim stranem;

   (c) odzivanje na incidente;

   (d) opravljanje dinamičnih analiz tveganja in incidentov ter situacijsko zavedanje na področju kibernetske varnosti;

   (e) opravljanje, na zahtevo subjekta, proaktivnega pregleda omrežij in informacijskih sistemov, ki se uporabljajo za opravljanje njihovih storitev;

   (f) sodelovanje v mreži skupin CSIRT in zagotavljanje medsebojne pomoči drugim članicam mreže na njihovo zahtevo.

3. Skupine CSIRT sodelujejo z ustreznimi akterji v zasebnem sektorju, da bi bolje dosegle cilje Direktive.

4. Za olajšanje sodelovanja skupine CSIRT spodbujajo sprejetje in uporabo skupnih ali standardiziranih praks, sistemov razvrščanja in taksonomij v zvezi z naslednjim:

   (a) postopki obvladovanja incidentov;

   (b) kriznim upravljanjem kibernetske varnosti;

   (c) usklajenim razkrivanjem šibkih točk.

Člen 11

Sodelovanje na nacionalni ravni

1. Kadar so pristojni organi iz člena 8, enotna kontaktna točka in skupine CSIRT iste države članice ločeni subjekti, med seboj sodelujejo pri izpolnjevanju obveznosti, ki jih določa ta direktiva.
2. Države članice zagotovijo, da bodisi njihovi pristojni organi bodisi skupine CSIRT prejmejo priglasitve incidentov ter pomembnih kibernetskih groženj in skorajšnjih dogodkov, predloženih v skladu s to direktivo. Kadar država članica sklene, da njene skupine CSIRT ne prejemajo takih priglasitev, se tem skupinam v obsegu, potrebnem za opravljanje njihovih nalog, zagotovi dostop do podatkov o incidentih, ki jih v skladu s členom 20 priglasijo bistveni ali pomembni subjekti.
3. Vsaka država članica zagotovi, da njeni pristojni organi ali skupine CSIRT obvestijo njeno enotno kontaktno točko o priglasitvah incidentov, pomembnih kibernetskih groženj in skorajšnjih dogodkov v skladu s to direktivo.
4. Če je to potrebno za učinkovito opravljanje nalog in izpolnjevanje obveznosti, določenih v tej direktivi, države članice zagotovijo ustrezno sodelovanje med pristojnimi organi, enotnimi kontaktnimi točkami, organi kazenskega pregona, organi za varstvo podatkov in organi, pristojnimi za kritično infrastrukturo v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov], ter nacionalnimi finančnimi organi, imenovanimi v skladu z Uredbo (EU) XXXX/XXXX Evropskega parlamenta in Sveta[39] [uredba o digitalni operativni odpornosti] v zadevni državi članici.
5. Države članice zagotovijo, da njihovi pristojni organi pristojnim organom, imenovanim v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov], redno zagotavljajo informacije o tveganjih za kibernetsko varnost, kibernetskih grožnjah in incidentih, ki vplivajo na bistvene subjekte, ki so opredeljeni kot kritični ali kot subjekti, enakovredni kritičnim subjektom, v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov], ter o ukrepih, ki jih sprejmejo pristojni organi v odziv na taka tveganja in incidente.

POGLAVJE III

Sodelovanje

Člen 12

Skupina za sodelovanje

1. Za podpiranje in olajšanje strateškega sodelovanja ter izmenjave informacij med državami članicami na področju uporabe Direktive se ustanovi skupina za sodelovanje.

[39] *[vstaviti polni naslov in sklic na objavo v UL, ko bosta znana].*

2. Skupina za sodelovanje opravlja svoje naloge na podlagi dvoletnih delovnih programov iz odstavka 6.

3. Skupino za sodelovanje sestavljajo predstavniki držav članic, Komisije in agencije ENISA. Evropska služba za zunanje delovanje sodeluje pri dejavnostih skupine za sodelovanje kot opazovalka. Evropski nadzorni organi lahko v skladu s členom 17(5)(c) Uredbe (EU) XXXX/XXXX [uredba o digitalni operativni odpornosti] sodelujejo pri dejavnostih skupine za sodelovanje.

   Skupina za sodelovanje lahko k sodelovanju po potrebi povabi predstavnike ustreznih zainteresiranih strani.

   Komisija zagotovi sekretariat.

4. Skupina za sodelovanje ima naslednje naloge:

   (a) zagotavljanje usmeritev pristojnim organom v zvezi s prenosom in izvajanjem te direktive;

   (b) izmenjava dobrih praks in informacij v zvezi z izvajanjem te direktive, tudi v zvezi s kibernetskimi grožnjami, incidenti, šibkimi točkami, skorajšnjimi dogodki, pobudami za ozaveščanje, usposabljanji, vajami ter znanji in spretnostmi, krepitvijo zmogljivosti ter standardi in tehničnimi specifikacijami;

   (c) izmenjava nasvetov in sodelovanje s Komisijo pri nastajajočih pobudah za politiko o kibernetski varnosti;

   (d) izmenjava nasvetov in sodelovanje s Komisijo pri pripravi osnutkov izvedbenih ali delegiranih aktov Komisije, sprejetih v skladu s to direktivo;

   (e) izmenjava dobrih praks in informacij z ustreznimi institucijami, organi, uradi in agencijami Unije;

   (f) obravnavanje poročil o medsebojnih strokovnih pregledih iz člena 16(7);

   (g) obravnavanje rezultatov skupnih nadzornih dejavnosti v čezmejnih primerih iz člena 34;

   (h) zagotavljanje strateških usmeritev mreži skupin CSIRT o posebnih porajajočih se vprašanjih;

   (i) prispevanje k zmogljivostim za kibernetsko varnost v Uniji z olajšanjem izmenjave nacionalnih uradnikov v okviru programa krepitve zmogljivosti, ki vključuje osebje iz pristojnih organov ali skupin CSIRT držav članic;

   (j) organizacija rednih sestankov z ustreznimi zasebnimi zainteresiranimi stranmi iz vse Unije za razpravljanje o dejavnostih, ki jih izvaja skupina, in zbiranje informacij o nastajajočih izzivih politike;

   (k) obravnavanje dela, opravljenega v zvezi z vajami na področju kibernetske varnosti, vključno z delom, ki ga je opravila agencija ENISA.

5. Skupina za sodelovanje lahko mrežo skupin CSIRT zaprosi za tehnično poročilo o izbranih temah.

6. Skupina za sodelovanje do [24 mesecev po datumu začetka veljavnosti te direktive] in nato vsaki dve leti pripravi delovni program v zvezi z ukrepi, ki jih je treba sprejeti

za izpolnitev njenih ciljev in nalog. Časovni okvir prvega programa, sprejetega v skladu s to direktivo, je usklajen s časovnim okvirom zadnjega programa, sprejetega v skladu z Direktivo (EU) 2016/1148.

7. Komisija lahko sprejme izvedbene akte, s katerimi določi postopkovne ureditve, potrebne za delovanje skupine za sodelovanje. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 37(2).

8. Skupina za sodelovanje se redno in vsaj enkrat letno sestane s skupino za odpornost kritičnih subjektov, ustanovljeno na podlagi Direktive (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov] z namenom spodbujanja strateškega sodelovanja in izmenjave informacij.

Člen 13

Mreža skupin CSIRT

1. Za prispevanje h krepitvi zaupanja ter spodbujanje hitrega in učinkovitega operativnega sodelovanja med državami članicami se vzpostavi mreža nacionalnih skupin CSIRT.

2. Mrežo skupin CSIRT sestavljajo predstavniki tovrstnih skupin držav članic in CERT-EU. Komisija sodeluje v mreži skupin CSIRT kot opazovalka. Agencija ENISA zagotovi sekretariat in dejavno podpira sodelovanje med skupinami CSIRT.

3. Mreža skupin CSIRT ima naslednje naloge:

   (a) izmenjava informacij o zmogljivostih skupin CSIRT;

   (b) izmenjava ustreznih informacij o incidentih, skorajšnjih dogodkih, kibernetskih grožnjah, tveganjih in šibkih točkah;

   (c) na prošnjo predstavnika mreže skupin CSIRT, na katero bi lahko vplival določen incident, izmenjava in obravnavanje informacij v zvezi z zadevnim incidentom ter z njim povezanimi kibernetskimi grožnjami, tveganji in šibkimi točkami;

   (d) na prošnjo predstavnika mreže skupin CSIRT, obravnavanje in po možnosti izvajanje usklajenega odziva na incident, ki je bil ugotovljen na ozemlju v pristojnosti zadevne države članice;

   (e) zagotavljanje podpore državam članicam pri obravnavanju čezmejnih incidentov v skladu s to direktivo;

   (f) sodelovanje in zagotavljanje pomoči imenovanim skupinam CSIRT iz člena 6 v zvezi z upravljanjem razkrivanja šibkih točk, ki vplivajo na več proizvajalcev ali ponudnikov proizvodov, storitev in postopkov IKT s sedežem v različnih državah članicah, ki ga usklajuje več strani;

   (g) obravnavanje in določitev nadaljnjih oblik operativnega sodelovanja, tudi glede:

      (i) kategorij kibernetskih groženj in incidentov;

      (ii) zgodnjega opozarjanja;

      (iii) medsebojne pomoči;

(iv) načel in načinov usklajevanja pri odzivanju na čezmejna tveganja in incidente;

(v) prispevanja k načrtu odzivanja na kibernetske incidente in krize iz člena 7(3);

(h) obveščanje skupine za sodelovanje o svojih dejavnostih in nadaljnjih oblikah operativnega sodelovanja, obravnavanih v skladu s točko (g), ter po potrebi prošnja za usmeritve v zvezi s tem;

(i) pregled vaj na področju kibernetske varnosti, vključno s tistimi, ki jih organizira agencija ENISA;

(j) na prošnjo posamezne skupine CSIRT obravnavanje njenih zmogljivosti in pripravljenosti;

(k) sodelovanje in izmenjava informacij s centri za varnostne operacije na regionalni ravni in ravni Unije za izboljšanje skupnega situacijskega zavedanja na področju incidentov in groženj po vsej Uniji;

(l) obravnavanje poročil o medsebojnih strokovnih pregledih iz člena 16(7);

(m) izdajanje smernic za olajšanje konvergence operativnih praks glede uporabe določb tega člena v zvezi z operativnim sodelovanjem.

4. Mreža skupin CSIRT za namene pregleda iz člena 35 do [24 mesecev po datumu začetka veljavnosti te direktive] in nato vsaki dve leti oceni napredek, dosežen na področju operativnega sodelovanja, in pripravi poročilo. V poročilu se zlasti oblikujejo sklepi o rezultatih medsebojnih strokovnih pregledov iz člena 16, opravljenih v zvezi z nacionalnimi skupinami CSIRT, vključno s sklepi in priporočili v okviru navedenega člena. To poročilo se predloži tudi skupini za sodelovanje.

5. Mreža skupin CSIRT sprejme svoj poslovnik.

Člen 14

Evropska organizacijska mreža za povezovanje v kibernetski krizi (EU-CyCLONe)

1. Za podpiranje usklajenega upravljanja velikih kibernetskih incidentov in kriz na operativni ravni in za zagotovitev redne izmenjave informacij med državami članicami ter institucijami, organi in agencijami Unije se ustanovi evropska organizacijska mreža za povezovanje v kibernetski krizi (EU-CyCLONe).

2. Mreža EU-CyCLONe je sestavljena iz predstavnikov organov držav članic za krizno upravljanje, imenovanih v skladu s členom 7, Komisije in agencije ENISA. Agencija ENISA zagotovi sekretariat mreže in podpira varno izmenjavo informacij.

3. Mreža EU-CyCLONe ima naslednje naloge:

(a) zviševanje ravni pripravljenosti za upravljanje velikih incidentov in kriz;

(b) razvoj skupnega situacijskega zavedanja o ustreznih dogodkih na področju kibernetske varnosti;

(c) usklajevanje upravljanja velikih incidentov in kriz ter podpiranje odločanja na politični ravni v zvezi s takimi incidenti in krizami;

(d) obravnavanje načrtov odzivanja na kibernetske incidente in krize iz člena 7(2).

4. Mreža EU-CyCLONe sprejme svoj poslovnik.

5. Mreža EU-CyCLONe redno poroča skupini za sodelovanje o kibernetskih grožnjah, incidentih in trendih, pri čemer se osredotoča zlasti na njihov vpliv na bistvene in pomembne subjekte.

6. Mreža EU-CyCLONe sodeluje z mrežo skupin CSIRT na podlagi sprejetih postopkovnih ureditev.

Člen 15

Poročilo o stanju kibernetske varnosti v Uniji

1. Agencija ENISA v sodelovanju s Komisijo izda dvoletno poročilo o stanju kibernetske varnosti v Uniji. Poročilo vključuje zlasti oceno naslednjega:

   (a) razvoja zmogljivosti za kibernetsko varnost v Uniji;

   (b) tehničnih, finančnih in človeških virov, ki so na voljo pristojnim organom, in politik na področju kibernetske varnosti ter izvajanja nadzornih in izvršilnih ukrepov na podlagi rezultatov medsebojnih strokovnih pregledov iz člena 16;

   (c) indeksa kibernetske varnosti, ki določa skupno oceno ravni zrelosti zmogljivosti za kibernetsko varnost.

2. Poročilo vključuje posebna priporočila politike za zvišanje ravni kibernetske varnosti v Uniji in povzetek ugotovitev za določeno obdobje iz tehničnih poročil o stanju na področju kibernetske varnosti v EU, ki jih izda agencija ENISA v skladu s členom 7(6) Uredbe (EU) 2019/881.

Člen 16

Medsebojni strokovni pregledi

1. Komisija po posvetovanju s skupino za sodelovanje in agencijo ENISA najpozneje 18 mesecev po začetku veljavnosti te direktive določi metodologijo in vsebino sistema medsebojnih strokovnih pregledov za ocenjevanje učinkovitosti politik držav članic na področju kibernetske varnosti. Preglede izvedejo tehnični strokovnjaki za kibernetsko varnost iz držav članic, med katerimi ni države, v zvezi s katero se izvede pregled, in zajemajo vsaj naslednje:

   (i) učinkovitost izvajanja zahtev glede obvladovanja tveganj za kibernetsko varnost ter obveznosti poročanja iz členov 18 in 20;

   (ii) raven zmogljivosti, vključno z razpoložljivimi finančnimi, tehničnimi in človeškimi viri, ter učinkovitost opravljanja nalog pristojnih nacionalnih organov;

   (iii) operativne zmogljivosti in učinkovitost skupin CSIRT;

   (iv) učinkovitost medsebojne pomoči iz člena 34;

   (v) učinkovitost okvira za izmenjavo informacij iz člena 26 te direktive.

2. Metodologija vključuje objektivna, nediskriminatorna, pravična in pregledna merila, na podlagi katerih države članice imenujejo strokovnjake, ki so upravičeni izvajati

medsebojne strokovne preglede. Agencija ENISA in Komisija imenujeta strokovnjake, ki v medsebojnih strokovnih pregledih sodelujejo kot opazovalci. Komisija ob podpori agencije ENISA v okviru metodologije iz odstavka 1 vzpostavi objektiven, nediskriminatoren, pravičen in pregleden sistem za izbiro in naključno dodeljevanje strokovnjakov za posamezne medsebojne strokovne preglede.

3. Organizacijske vidike medsebojnih strokovnih pregledov določi Komisija, ob podpori agencije ENISA, na podlagi posvetovanj s skupino za sodelovanje in na podlagi meril, opredeljenih v metodologiji iz odstavka 1. Pri medsebojnih strokovnih pregledih se ocenijo vidiki iz odstavka 1 za vse države članice in sektorje, vključno s ciljno usmerjenimi vprašanji, ki se nanašajo na eno ali več držav članic ali enega ali več sektorjev.

4. Medsebojni strokovni pregledi vključujejo dejanske ali virtualne obiske na kraju samem in izmenjave na daljavo. Države članice, ki so predmet pregleda, ob upoštevanju načela dobrega sodelovanja imenovanim strokovnjakom zagotovijo zahtevane informacije, potrebne za oceno vidikov, ki se pregledujejo. Vse informacije, pridobljene v okviru postopka medsebojnega strokovnega pregleda, se uporabljajo izključno v ta namen. Strokovnjaki, ki sodelujejo pri medsebojnem strokovnem pregledu, občutljivih ali zaupnih informacij, pridobljenih med zadevnim pregledom, ne razkrijejo tretjim osebam.

5. Po opravljenem pregledu v določeni državi članici isti vidiki dve leti po zaključku medsebojnega strokovnega pregleda niso predmet nadaljnjih medsebojnih strokovnih pregledov v tej državi članici, razen če Komisija po posvetovanju z agencijo ENISA in skupino za sodelovanje ne odloči drugače.

6. Država članica zagotovi, da se drugim državam članicam, Komisiji in agenciji ENISA brez nepotrebnega odlašanja razkrijejo vsa tveganja navzkrižja interesov v zvezi z imenovanimi strokovnjaki.

7. Strokovnjaki, ki sodelujejo v medsebojnih strokovnih pregledih, pripravijo poročila o ugotovitvah in sklepih pregledov. Poročila se predložijo Komisiji, skupini za sodelovanje, mreži skupin CSIRT in agenciji ENISA. Poročila se obravnavajo v okviru skupine za sodelovanje in mreže skupin CSIRT. Poročila se lahko objavijo na posebnem spletnem mestu skupine za sodelovanje.

POGLAVJE IV

Obveznosti glede obvladovanja tveganj za kibernetsko varnost in poročanja

ODDELEK I

Obvladovanje tveganj za kibernetsko varnost in poročanje

Člen 17

Upravljanje

1. Države članice zagotovijo, da upravni organi bistvenih in pomembnih subjektov odobrijo ukrepe za obvladovanje tveganj za kibernetsko varnost, ki jih sprejmejo zadevni subjekti, da izpolnijo zahteve iz člena 18, nadzorujejo njihovo izvajanje in so odgovorni za neizpolnjevanje obveznosti subjektov, ki so jim naložene v skladu s tem členom.

2. Države članice zagotovijo, da se člani upravnega organa redno udeležujejo posebnih usposabljanj, da pridobijo dovolj znanja in spretnosti za razumevanje in ocenjevanje tveganj za kibernetsko varnost ter praks upravljanja in njihovega vpliva na dejavnosti subjekta.

Člen 18

Ukrepi za obvladovanje tveganj za kibernetsko varnost

1. Države članice zagotovijo, da bistveni in pomembni subjekti sprejmejo ustrezne in sorazmerne tehnične in organizacijske ukrepe za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih ti subjekti uporabljajo za opravljanje storitev. Ob upoštevanju stanja tehnike se s temi ukrepi zagotovi raven varnosti omrežij in informacijskih sistemov, primerna obstoječemu tveganju.

2. Ukrepi iz odstavka 1 vključujejo vsaj naslednje:

   (a) analizo tveganja in varnostna pravila za informacijske sisteme;

   (b) obvladovanje incidentov (preprečevanje in odkrivanje incidentov ter odzivanje nanje);

   (c) upravljanje neprekinjenega poslovanja in krizno upravljanje;

   (d) varnost dobavne verige, vključno z vidiki, povezanimi z varnostjo, ki se nanašajo na odnose med posameznim subjektom in njegovimi dobavitelji ali ponudniki storitev, kot so ponudniki storitev shranjevanja in obdelave podatkov ali upravljanih varnostnih storitev;

   (e) varnost pri pridobivanju, razvoju in vzdrževanju omrežij in informacijskih sistemov, vključno z obravnavanjem in razkrivanjem šibkih točk;

   (f) politike in postopke (preizkušanje in revidiranje) za oceno učinkovitosti ukrepov za obvladovanje tveganj za kibernetsko varnost;

   (g) uporabo kriptografije in šifriranja.

3. Države članice zagotovijo, da subjekti pri preučevanju ustreznih ukrepov iz točke (d) odstavka 2 upoštevajo šibke točke posameznega dobavitelja in ponudnika storitev ter splošno kakovost proizvodov ter praks svojih dobaviteljev in ponudnikov storitev na področju kibernetske varnosti, vključno z njihovimi varnimi razvojnimi postopki.

4. Države članice zagotovijo, da subjekt, če ugotovi, da njegove storitve oziroma naloge ne izpolnjujejo zahtev iz odstavka 2, brez nepotrebnega odlašanja sprejme vse potrebne popravne ukrepe za zagotovitev, da zadevna storitev izpolnjuje zahteve.

5. Komisija lahko sprejme izvedbene akte, s katerimi določi tehnične in metodološke specifikacije elementov iz odstavka 2. Komisija pri pripravi teh aktov ravna v skladu s postopkom pregleda iz člena 37(2) ter v največji možni meri upošteva mednarodne in evropske standarde ter ustrezne tehnične specifikacije.

6. Komisija je pooblaščena za sprejetje delegiranih aktov v skladu s členom 36 za dopolnitev elementov iz odstavka 2, da bi se upoštevale nove kibernetske grožnje, tehnološki razvoj ali sektorske posebnosti.

Člen 19

Usklajene ocene tveganja v EU za kritične dobavne verige

1. Skupina za sodelovanje lahko v sodelovanju s Komisijo in agencijo ENISA izvaja usklajene ocene tveganja za varnost specifičnih kritičnih storitev IKT, sistemov IKT ali dobavnih verig proizvodov IKT, ob upoštevanju tehničnih in po potrebi netehničnih dejavnikov tveganja.

2. Komisija po posvetovanju s skupino za sodelovanje in agencijo ENISA opredeli specifične kritične storitve, sisteme ali proizvode IKT, ki so lahko predmet usklajene ocene tveganja iz odstavka 1.

Člen 20

Obveznosti poročanja

1. Države članice zagotovijo, da bistveni in pomembni subjekti pristojnim organom ali skupini CSIRT brez nepotrebnega odlašanja v skladu z odstavkoma 3 in 4 priglasijo vse incidente, ki pomembno vplivajo na opravljanje njihovih storitev. Kjer je to ustrezno, navedeni subjekti prejemnike svojih storitev brez nepotrebnega odlašanja obvestijo o incidentih, ki bodo verjetno negativno vplivali na opravljanje zadevne storitve. Države članice zagotovijo, da navedeni subjekti sporočijo, med drugim, vse informacije, ki pristojnim organom ali skupini CSIRT omogočajo, da določijo čezmejni vpliv incidenta.

2. Države članice zagotovijo, da bistveni in pomembni subjekti brez nepotrebnega odlašanja pristojnim organom ali skupini CSIRT priglasijo vse pomembne kibernetske grožnje, ki jih ti subjekti prepoznajo in ki bi lahko privedle do velikega incidenta.

   Po potrebi ti subjekti prejemnike svojih storitev, ki bi jih pomembna kibernetska grožnja lahko prizadela, brez nepotrebnega odlašanja obvestijo o vseh ukrepih ali sredstvih, ki jih lahko ti prejemniki sprejmejo v odziv na zadevno grožnjo. Kjer je ustrezno, subjekti zadevne prejemnike obvestijo tudi o sami grožnji. Priglasitev ne sme nalagati priglasitelju dodatne odgovornosti.

3. Incident se šteje za pomemben, če:

   (a) je zadevnemu subjektu povzročil ali bi mu lahko povzročil znatne operativne motnje ali finančne izgube;

   (b) je vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnjih materialnih ali nematerialnih izgub.

4. Države članice zagotovijo, da zadevni subjekti za namen priglasitve iz odstavka 1 pristojnim organom in skupini CSIRT predložijo:

(a) brez nepotrebnega odlašanja in v vsakem primeru v 24 urah po seznanitvi z incidentom začetno priglasitev, v kateri je, kjer je ustrezno, navedeno, ali je bil incident domnevno povzročen z nezakonitim ali zlonamernim dejanjem;

(b) na zahtevo pristojnega organa ali skupine CSIRT vmesno poročilo o ustreznih posodobitvah stanja;

(c) končno poročilo, najpozneje v enem mesecu po predložitvi začetne priglasitve iz točke (a), ki vključuje vsaj naslednje:

(i) podroben opis incidenta, njegove resnosti in vpliva;

(ii) vrsto grožnje ali temeljnega vzroka, ki je verjetno sprožil incident;

(iii) izvedene blažilne ukrepe in take ukrepe v teku.

Države članice zagotovijo, da lahko zadevni subjekt v ustrezno utemeljenih primerih in v dogovoru s pristojnimi organi ali skupino CSIRT odstopa od rokov iz točk (a) in (c).

5. Pristojni nacionalni organi ali skupina CSIRT v 24 urah po prejemu začetne priglasitve iz točke (a) odstavka 4 odgovorijo priglasitelju, vključno z začetnimi povratnimi informacijami o incidentu in, na zahtevo subjekta, usmeritvami glede izvajanja morebitnih blažilnih ukrepov. Če skupina CSIRT ni prejela priglasitve iz odstavka 1, usmeritve zagotovi pristojni organ v sodelovanju s skupino CSIRT. Skupina CSIRT na zahtevo zadevnega subjekta zagotovi dodatno tehnično podporo. Če se za incident sumi, da je kazenske narave, pristojni nacionalni organi ali skupina CSIRT zagotovijo tudi usmeritve o poročanju o incidentih organom kazenskega pregona.

6. Kadar je to ustrezno in zlasti če incident iz odstavka 1 zadeva dve ali več držav članic, pristojni organ ali skupina CSIRT obvesti druge prizadete države članice in agencijo ENISA o incidentu. Pristojni organi, skupine CSIRT in enotne kontaktne točke pri tem v skladu s pravom Unije ali nacionalno zakonodajo, ki je skladna s pravom Unije, zaščitijo varnost in poslovne interese subjekta ter zaupnost predloženih informacij.

7. Kadar je ozaveščenost javnosti potrebna za preprečitev incidenta ali obravnavo incidenta, ki je v teku, ali kadar je razkritje incidenta kako drugače v javnem interesu, lahko pristojni organ ali skupina CSIRT in po potrebi organi ali skupine CSIRT drugih zadevnih držav članic po posvetovanju z zadevnim subjektom obvestijo javnost o incidentu ali zahtevajo, da to stori subjekt.

8. Enotna kontaktna točka na zahtevo pristojnega organa ali skupine CSIRT priglasitve, prejete v skladu z odstavkoma 1 in 2, posreduje enotnim kontaktnim točkam drugih prizadetih držav članic.

9. Enotna kontaktna točka agenciji ENISA vsak mesec predloži zbirno poročilo, vključno z anonimiziranimi in zbirnimi podatki o incidentih, pomembnih kibernetskih grožnjah in skorajšnjih dogodkih, priglašenih v skladu z odstavkoma 1 in 2 ter členom 27. Da bi prispevala k zagotavljanju primerljivih informacij, lahko agencija ENISA izda tehnične smernice o parametrih informacij, vključenih v zbirno poročilo.

10. Pristojni organi zagotovijo pristojnim organom, imenovanim v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov], informacije o

incidentih in kibernetskih grožnjah, ki so jih v skladu z odstavkoma 1 in 2 priglasili bistveni subjekti, opredeljeni kot kritični subjekti ali kot subjekti, enakovredni kritičnim subjektom, v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov].

11. Komisija lahko sprejme izvedbene akte, s katerimi se podrobneje določijo vrsta informacij, oblika in postopek priglasitve, predložene v skladu z odstavkoma 1 in 2. Komisija lahko sprejme izvedbene akte za podrobnejšo določitev primerov, v katerih se incident šteje za pomemben v skladu z odstavkom 3. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 37(2).

Člen 21

Uporaba evropskih certifikacijskih shem za kibernetsko varnost

1. Države članice lahko za dokaz izpolnjevanja nekaterih zahtev iz člena 18 od bistvenih in pomembnih subjektov zahtevajo, naj certificirajo nekatere proizvode, storitve in postopke IKT na podlagi določenih evropskih ceritfikacijskih shem za kibernetsko varnost, sprejetih v skladu s členom 49 Uredbe (EU) 2019/881. Proizvode, storitve in postopke, ki so predmet certificiranja, lahko razvije bistveni ali pomembni subjekt ali jih dobavijo tretje osebe.

2. Komisija je pooblaščena za sprejetje delegiranih aktov, ki določajo, za katere kategorije bistvenih subjektov je treba pridobiti certifikat in na podlagi katerih določenih evropskih certifikacijskih shem za kibernetsko varnost v skladu z odstavkom 1. Delegirani akti se sprejmejo v skladu s členom 36.

3. Komisija lahko od agencije ENISA zahteva, naj pripravi predlogo za shemo v skladu s členom 48(2) Uredbe (EU) 2019/881, če za namene odstavka 2 ni na voljo ustrezne evropske certifikacijske sheme za kibernetsko varnost.

Člen 22

Standardizacija

1. Za zagotovitev usklajenega izvajanja člena 18(1) in (2) države članice spodbujajo uporabo evropskih ali mednarodno sprejetih standardov in specifikacij, pomembnih za varnost omrežij in informacijskih sistemov, ne da bi predpisale uporabo določene vrste tehnologije ali ji dajale prednost.

2. Agencija ENISA v sodelovanju z državami članicami pripravi nasvete in smernice za tehnična področja, ki se upoštevajo v zvezi z odstavkom 1, ter za že obstoječe standarde, vključno z nacionalnimi standardi držav članic, s katerimi bi lahko zajeli navedena področja.

Člen 23

Podatkovne zbirke domenskih imen in podatkov o registraciji

1. Da bi prispevale k varnosti, stabilnosti in odpornosti sistema domenskih imen, države članice zagotovijo, da registri vrhnjih domen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene, z ustrezno skrbnostjo zbirajo ter vzdržujejo točne in popolne podatke o registraciji domenskih imen v posebni podatkovni zbirki, ob upoštevanju zakonodaje Unije o varstvu podatkov v zvezi s podatki, ki so osebni podatki.

2. Države članice zagotovijo, da podatkovne zbirke podatkov o registraciji domenskih imen iz odstavka 1 vsebujejo ustrezne informacije za identifikacijo imetnikov domenskih imen in kontaktnih točk, ki upravljajo domenska imena v okviru vrhnjih domen, in navezavo stika z njimi.

3. Države članice zagotovijo, da imajo registri vrhnjih domen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene, vzpostavljene politike in postopke, ki zagotavljajo, da podatkovne zbirke vključujejo točne in popolne informacije. Države članice zagotovijo, da so take politike in postopki javno dostopni.

4. Države članice zagotovijo, da registri vrhnjih domen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene, po registraciji domenskega imena brez nepotrebnega odlašanja objavijo podatke o registraciji domene, ki niso osebni podatki.

5. Države članice zagotovijo, da registri vrhnjih domen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene, omogočajo dostop do podatkov o registraciji posameznih domenskih imen na podlagi zakonitih in ustrezno utemeljenih zahtevkov oseb, ki imajo upravičen razlog za dostop, v skladu z zakonodajo Unije o varstvu podatkov. Države članice zagotovijo, da registri vrhnjih domen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene, brez nepotrebnega odlašanja odgovorijo na vse zahtevke za dostop. Države članice zagotovijo, da so politike in postopki za razkrivanje takih podatkov javno dostopni.

Oddelek II

Pristojnost in registracija

Člen 24

Sodna pristojnost in teritorialnost

1. Za ponudnike storitev sistema domenskih imen, registre vrhnjih domenskih imen, ponudnike storitev računalništva v oblaku, ponudnike storitev podatkovnih centrov in ponudnike omrežij za dostavo vsebine iz točke 8 Priloge I ter ponudnike digitalnih storitev iz točke 6 Priloge II se šteje, da so pod sodno pristojnostjo države članice, v kateri imajo glavni sedež v Uniji.

2. Z namene te direktive se za subjekte iz odstavka 1 šteje, da imajo glavni sedež v Uniji v državi članici, kjer se sprejemajo odločitve v zvezi z ukrepi za obvladovanje tveganj za kibernetsko varnost. Če se take odločitve ne sprejemajo na sedežu v Uniji, se šteje, da je glavni sedež v državi članici, kjer imajo subjekti sedež z največjim številom zaposlenih v Uniji.

3. Če subjekt iz odstavka 1 nima sedeža v Uniji, vendar v njej opravlja storitve, določi predstavnika v Uniji. Predstavnik ima sedež v eni od držav članic, v katerih se opravljajo storitve. Za tak subjekt se šteje, da je pod sodno pristojnostjo države članice, v kateri ima predstavnik sedež. Če ni imenovanega predstavnika v Uniji v skladu s tem členom, lahko katera koli država članica, v kateri subjekt opravlja storitve, uvede sodne postopke proti subjektu zaradi neizpolnjevanja obveznosti po tej direktivi.

4. Imenovanje predstavnika s strani subjekta iz odstavka 1 ne posega v sodne postopke, ki se lahko uvedejo proti samemu subjektu.

Člen 25

Register bistvenih in pomembnih subjektov

1. Agencija ENISA vzpostavi in vzdržuje register bistvenih in pomembnih subjektov iz člena 24(1). Subjekti do [najpozneje 12 mesecev po začetku veljavnosti Direktive] agenciji ENISA predložijo naslednje informacije:

   (a) ime subjekta;

   (b) naslov njegovega glavnega sedeža in njegovih drugih zakonitih sedežev v Uniji ali, če nima sedeža v Uniji, njegovega predstavnika, imenovanega v skladu s členom 24(3);

   (c) posodobljene kontaktne podatke, vključno z elektronskimi naslovi in telefonskimi številkami subjektov.

2. Subjekti iz odstavka 1 nemudoma, v vsakem primeru pa v treh mesecih od datuma začetka veljavnosti spremembe, obvestijo agencijo ENISA o kakršnih koli spremembah podatkov, ki so ji predložili v skladu z odstavkom 1.

3. Agencija ENISA po prejemu informacij iz odstavka 1 posreduje informacije enotnim kontaktnim točkam glede na navedeni kraj glavnega sedeža posameznega subjekta ali, če subjekt nima sedeža v Uniji, navedeni kraj njegovega imenovanega predstavnika. Če ima subjekt iz odstavka 1 poleg glavnega sedeža v Uniji še dodatne sedeže v drugih državah članicah, agencija ENISA obvesti tudi enotne kontaktne točke zadevnih držav članic.

4. Če subjekt ne registrira dejavnosti ali zagotovi ustreznih informacij v roku iz odstavka 1, je vsaka država članica, v kateri subjekt opravlja storitve, pristojna za zagotavljanje njegovega izpolnjevanja obveznosti iz te direktive.

POGLAVJE V

Izmenjava informacij

Člen 26

Dogovori o izmenjavi informacij o kibernetski varnosti

1. Države članice brez poseganja v Uredbo (EU) 2016/679 zagotovijo, da si bistveni in pomembni subjekti lahko izmenjujejo ustrezne informacije o kibernetski varnosti, vključno z informacijami, ki se nanašajo na kibernetske grožnje, šibke točke, kazalnike ogroženosti, taktike, tehnike in postopke, opozorila glede kibernetske varnosti in orodja za konfiguracijo, če taka izmenjava informacij:

   (a) stremi k preprečevanju in odkrivanju incidentov, odzivanju nanje ali njihovi ublažitvi;

   (b) zvišuje raven kibernetske varnosti, zlasti z ozaveščanjem v zvezi s kibernetskimi grožnjami, omejevanjem ali oviranjem zmožnosti širjenja takih groženj, podpiranjem vrste obrambnih zmogljivosti, odpravljanjem in razkrivanjem šibkih točk, tehnikami odkrivanja groženj, strategijami za zmanjšanje tveganja ali fazami odzivanja in okrevanja.

2. Države članice zagotovijo, da izmenjava informacij poteka v zaupanja vrednih skupnostih bistvenih in pomembnih subjektov. Taka izmenjava se izvaja na podlagi dogovorov o izmenjavi informacij, ob upoštevanju morebitne občutljivosti informacij, ki se izmenjujejo, in v skladu s pravili prava Unije iz odstavka 1.

3. Države članice določijo pravila o postopku, operativnih elementih (vključno z uporabo namenskih platform IKT), vsebini in pogojih dogovorov o izmenjavi informacij iz odstavka 2. Taka pravila določajo tudi podrobnosti sodelovanja javnih organov pri takih dogovorih in operativne elemente, vključno z uporabo namenskih platform informacijske tehnologije. Države članice nudijo podporo za uporabo takih dogovorov v skladu s svojimi politikami iz člena 5(2)(g).

4. Bistveni in pomembni subjekti obvestijo pristojne organe o svojem sodelovanju pri dogovorih o izmenjavi informacij iz odstavka 2 po sklenitvi takih dogovorov ali, kjer je to ustrezno, o odstopu od dogovora, ko odstop začne veljati.

5. Agencija ENISA v skladu s pravom Unije podpira sklenitev dogovorov o izmenjavi informacij o kibernetski varnosti iz odstavka 2 z zagotavljanjem dobrih praks in smernic.

Člen 27

Prostovoljna priglasitev ustreznih informacijah

Države članice zagotovijo, da lahko subjekti, ki ne spadajo na področje uporabe te direktive, brez poseganja v člen 3 prostovoljno predložijo priglasitve o pomembnih incidentih, kibernetskih grožnjah ali skorajšnjih dogodkih. Države članice pri obdelavi priglasitev ravnajo v skladu s postopkom iz člena 20. Pred prostovoljnimi priglasitvami lahko prednostno obdelajo obvezne priglasitve. Prostovoljno poročanje poročajočemu subjektu ne naloži nikakršnih dodatnih obveznosti, ki zanj ne bi veljale, če ne bi predložil priglasitve.

POGLAVJE VI

Nadzor in izvrševanje

Člen 28

Splošni vidiki, povezani z nadzorom in izvrševanjem

1. Države članice zagotovijo, da pristojni organi učinkovito spremljajo izpolnjevanje obveznosti iz te direktive, zlasti obveznosti iz členov 18 in 20, in sprejmejo ukrepe za zagotovitev takega izpolnjevanja.

2. Pristojni organi pri obravnavi incidentov, katerih posledica je kršitev varstva osebnih podatkov, tesno sodelujejo z organi za varstvo podatkov.

Člen 29

Nadzor in izvrševanje pri bistvenih subjektih

1. Države članice zagotovijo, da so ukrepi nadzora ali izvrševanja, naloženi bistvenim subjektom v zvezi z obveznostmi iz te direktive, učinkoviti, sorazmerni in odvračilni, ob upoštevanju okoliščin posameznega primera.

2. Države članice zagotovijo, da so pristojni organi pri izvajanju svojih nadzornih nalog v zvezi z bistvenimi subjekti pooblaščeni, da pri teh subjektih :

   (a) opravijo inšpekcijske preglede na kraju samem in nadzorna daljavo, vključno z naključnimi pregledi;

   (b) opravijo redne revizije;

   (c) opravijo ciljno usmerjene varnostne presoje, ki temeljijo na ocenah tveganja ali razpoložljivih informacijah o tveganju;

   (d) opravijo varnostne preglede, ki temeljijo na objektivnih, nediskriminatornih, poštenih in preglednih merilih za oceno tveganja;

   (e) zagotovijo izpolnjevanje zahtev po informacijah, potrebnih za oceno ukrepov za kibernetsko varnost, ki jih je sprejel subjekt, vključno z dokumentiranimi politikami na področju kibernetske varnosti, in izpolnjevanje obveznosti obveščanja agencije ENISA v skladu s členom 25(1) in (2);

   (f) zagotovijo izpolnjevanje zahtev po dostopu do podatkov, dokumentov ali kakršnih koli informacij, potrebnih za opravljanje njihovih nadzornih nalog;

   (g) zagotovijo izpolnjevanje zahtev po dokazih o izvajanju politik na področju kibernetske varnosti, kot so rezultati varnostnih presoj, ki jih izvede usposobljen presojevalec, in ustrezni temeljni dokazi.

3. Pristojni organi pri izvajanju svojih pooblastil iz točk (e) do (g) odstavka 2 navedejo namen zahteve in opredelijo zahtevane informacije.

4. Države članice zagotovijo, da so pristojni organi pri izvajanju svojih izvršilnih pooblastil v zvezi z bistvenimi subjekti pooblaščeni, da:

   (a) izdajo opozorila o subjektovem neizpolnjevanju obveznosti, določenih v tej direktivi;

   (b) izdajo zavezujoča navodila ali odredbo, s katero od takih subjektov zahtevajo, da odpravijo ugotovljene pomanjkljivosti ali kršitve obveznosti, določene v tej direktivi;

(c) takim subjektom odredijo, naj prenehajo z ravnanjem, ki ni skladno z obveznostmi, določenimi v tej direktivi, in naj tega ravnanja ne ponovijo več;

(d) takim subjektom odredijo, naj na določen način in v določenem roku uskladijo svoje ukrepe za obvladovanje tveganj in/ali obveznosti poročanja z obveznostmi iz členov 18 in 20;

(e) takim subjektom odredijo, naj obvestijo fizične ali pravne osebe, za katere opravljajo storitve ali dejavnosti, na katere bi lahko vplivala pomembna kibernetska grožnja, o vseh mogočih zaščitnih ali popravnih ukrepih, ki jih lahko take fizične ali pravne osebe sprejmejo v odziv na zadevno grožnjo;

(f) takim subjektom odredijo, naj v razumnem roku izvedejo priporočila, dana na podlagi varnostne presoje;

(g) imenujejo uradnika za spremljanje z natančno opredeljenimi nalogami v določenem obdobju, ki nadzoruje izpolnjevanje obveznosti, določenih v členih 18 in 20;

(h) takim subjektom odredijo, naj na določen način objavijo vidike neizpolnjevanja obveznosti, določenih v tej direktivi;

(i) podajo javno izjavo, v kateri so opredeljene pravne in fizične osebe, odgovorne za kršitev obveznosti, določene v tej direktivi, in narava zadevne kršitve;

(j) naložijo ali zahtevajo, naj ustrezni organi ali sodišča v skladu z nacionalno zakonodajo naložijo upravno globo v skladu s členom 31, poleg ali namesto ukrepov iz točk (a) do (i) tega odstavka glede na okoliščine posameznega primera.

5. Če se izvršilni ukrepi, sprejeti v skladu s točkami (a) do (d) in (f) odstavka (4) izkažejo za neučinkovite, države članice zagotovijo, da so pristojni organi pooblaščeni za določitev roka, v katerem mora bistveni subjekt sprejeti potrebne ukrepe za odpravo pomanjkljivosti ali izpolnitev zahtev teh organov. Če se zahtevani ukrepi ne sprejmejo v določenem roku, države članice zagotovijo, da so pristojni organi pooblaščeni, da:

(a) začasno prekličejo ali od certifikacijskega organa ali organa, pristojnega za izdajo dovoljenj, zahtevajo, naj začasno prekliče certifikat ali dovoljenje za del storitev ali dejavnosti ali vse storitve ali dejavnosti, ki jih opravlja bistveni subjekt;

(b) uvedejo ali zahtevajo, naj ustrezni organi ali sodišča v skladu z nacionalno zakonodajo uvedejo začasno prepoved opravljanja vodstvenih funkcij vseh oseb, ki za bistveni subjekt opravljajo poslovodne naloge na ravni glavnega izvršnega direktorja ali pravnega zastopnika, in vseh drugih fizičnih oseb, ki so odgovorne za kršitev.

Te sankcije se uporabljajo samo, dokler subjekt ne sprejme potrebnih ukrepov za odpravo pomanjkljivosti ali izpolni zahtev pristojnega organa, zaradi katerih so bile take sankcije naložene.

6. Države članice zagotovijo, da ima vsaka fizična oseba, ki je odgovorna za bistveni subjekt ali deluje kot predstavnik bistvenega subjekta na podlagi pooblastila za njegovo zastopanje, odločanje v njegovem imenu ali izvajanje nadzora nad njim, pooblastila za zagotavljanje, da bistveni subjekt izpolnjuje obveznosti, določene v tej

direktivi. Države članice zagotovijo, da lahko te fizične osebe odgovarjajo za kršitev svojih dolžnosti, da bi zagotovile izpolnjevanje obveznosti, določenih v tej direktivi.

7. Pristojni organi pri sprejemanju kakršnih koli izvršilnih ukrepov ali uporabi kakršnih koli sankcij v skladu z odstavkoma 4 in 5 spoštujejo pravice do obrambe in upoštevajo okoliščine vsakega posameznega primera ter ustrezno upoštevajo vsaj naslednje:

   (a) resnost kršitve in pomembnost kršenih določb. Med kršitvami, ki bi se morale šteti za resne, so: ponavljajoče se kršitve, nepriglasitev ali neodprava incidentov z znatnim negativnim vplivom, neodprava pomanjkljivosti v skladu z zavezujočimi navodili pristojnih organov, oviranje presoj ali dejavnosti spremljanja, ki jih je odredil pristojni organ po ugotovitvi kršitve, predložitev napačnih in zelo netočnih informacij v zvezi z zahtevami glede obvladovanja tveganj ali obveznostmi poročanja iz členov 18 in 20;

   (b) trajanje kršitve, vključno z elementom ponavljajočih se kršitev;

   (c) dejansko povzročeno škodo ali nastale izgube ali morebitno škodo ali izgube, ki bi lahko nastale, če jih je mogoče določiti. Pri ocenjevanju tega vidika se med drugim upoštevajo dejanske ali morebitne finančne ali gospodarske izgube, učinki na druge storitve, število prizadetih ali potencialno prizadetih uporabnikov;

   (d) ali je kršitev naklepna ali posledica malomarnosti;

   (e) ukrepe, ki jih je subjekt sprejel za preprečevanje ali ublažitev škode in/ali izgub;

   (f) upoštevanje odobrenih kodeksov ravnanja ali odobrenih mehanizmov certificiranja;

   (g) raven sodelovanja fizičnih ali pravnih oseb, ki se štejejo za odgovorne, s pristojnimi organi.

8. Pristojni organi podrobno utemeljijo svoje odločitve o izvrševanju. Pred sprejetjem takih odločitev obvestijo zadevne subjekte o svojih predhodnih ugotovitvah in jim dajo na voljo dovolj časa za predložitev pripomb.

9. Države članice zagotovijo, da njihovi pristojni organi obvestijo ustrezne pristojne organe zadevne države članice, imenovane v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov], kadar izvajajo nadzorna in izvršilna pooblastila, namenjena zagotavljanju, da bistveni subjekt, ki je v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov] opredeljen kot kritičen ali kot subjekt, enakovreden kritičnemu subjektu, izpolnjuje obveznosti v skladu s to direktivo. Na zahtevo pristojnih organov iz Direktive (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov] lahko pristojni organi izvajajo nadzorna in izvršilna pooblastila nad bistvenim subjektom, ki je opredeljen kot kritičen ali enakovreden.

Člen 30

Nadzor in izvrševanje pri pomembnih subjektih

1. Če obstajajo dokazi ali znaki, da pomembni subjekt ne izpolnjuje obveznosti, določenih v tej direktivi, zlasti v členih 18 in 20, države članice zagotovijo, da pristojni organi ukrepajo, po potrebi z naknadnimi nadzornimi ukrepi.

2. Države članice zagotovijo, da so pristojni organi pri izvajanju svojih nadzornih nalog v zvezi s pomembnimi subjekti pooblaščeni, da pri teh subjektih:

   (a) opravijo inšpekcijske preglede na kraju samem in naknadni nadzor na daljavo;

   (b) opravijo ciljno usmerjene varnostne presoje, ki temeljijo na ocenah tveganja ali razpoložljivih informacijah o tveganju;

   (c) opravijo varnostne preglede, ki temeljijo na objektivnih, poštenih in preglednih merilih za oceno tveganja;

   (d) zagotovijo izpolnjevanje zahtev po kakršnih koli informacijah, potrebnih za naknadno oceno ukrepov za kibernetsko varnost, vključno z dokumentiranimi politikami na področju kibernetske varnosti, in izpolnjevanje obveznosti obveščanja agencije ENISA v skladu s členom 25(1) in (2);

   (e) zagotovijo izpolnjevanje zahtev po dostopu do podatkov, dokumentov in/ali informacij, potrebnih za opravljanje nadzornih nalog.

3. Pristojni organi pri izvajanju svojih pooblastil iz točke (d) ali (e) odstavka 2 navedejo namen zahteve in opredelijo zahtevane informacije.

4. Države članice zagotovijo, da so pristojni organi pri izvajanju svojih izvršilnih pooblastil v zvezi s pomembnimi subjekti pooblaščeni, da:

   (a) izdajo opozorila o subjektovem neizpolnjevanju obveznosti, določenih v tej direktivi;

   (b) izdajo zavezujoča navodila ali odredbo, s katero od takih subjektov zahtevajo, da odpravijo ugotovljene pomanjkljivosti ali kršitev obveznosti, določenih v tej direktivi;

   (c) takim subjektom odredijo, naj prenehajo z ravnanjem, ki ni skladno z obveznostmi, določenimi v tej direktivi, in naj tega ravnanja ne ponovijo več;

   (d) takim subjektom odredijo, naj na določen način in v določenem roku uskladijo svoje ukrepe za obvladovanje tveganj ali obveznosti poročanja z obveznostmi iz členov 18 in 20;

   (e) takim subjektom odredijo, naj obvestijo fizične ali pravne osebe, za katere opravljajo storitve ali dejavnosti, na katere bi lahko vplivala pomembna kibernetska grožnja, o vseh mogočih zaščitnih ali popravnih ukrepih, ki jih lahko take fizične ali pravne osebe sprejmejo v odziv na zadevno grožnjo;

   (f) takim subjektom odredijo, naj v razumnem roku izvedejo priporočila, dana na podlagi varnostne presoje;

   (g) takim subjektom odredijo, naj na določen način objavijo vidike neizpolnjevanja svojih obveznosti, določenih v tej direktivi;

   (h) podajo javno izjavo, v kateri so opredeljene pravne in fizične osebe, odgovorne za kršitev obveznosti, določene v tej direktivi, in narava zadevne kršitve;

   (i) naložijo ali zahtevajo, naj ustrezni organi ali sodišča v skladu z nacionalno zakonodajo naložijo upravno globo v skladu s členom 31, poleg ali namesto

ukrepov iz točk (a) do (h) tega odstavka glede na okoliščine posameznega primera.

5. Člen 29(6) do (8) se uporablja tudi za nadzorne in izvršilne ukrepe, ki so v tem členu določeni za pomembne subjekte, navedene v Prilogi II.

Člen 31

Splošni pogoji za naložitev upravnih glob bistvenim in pomembnim subjektom

1. Države članice zagotovijo, da je naložitev upravnih glob bistvenim in pomembnim subjektom v skladu s tem členom v zvezi s kršitvami obveznosti, določenih v tej direktivi, v vsakem posameznem primeru učinkovita, sorazmerna in odvračilna.

2. Glede na okoliščine posameznega primera se upravne globe naložijo poleg ali namesto ukrepov iz točk (a) do (i) člena 29(4), člena 29(5) in točk (a) do (h) člena 30(4).

3. Pri odločanju o naložitvi upravne globe in njeni višini se v vsakem posameznem primeru upoštevajo vsaj elementi, določeni v členu 29(7).

4. Države članice zagotovijo, da se za kršitve obveznosti iz člena 18 ali člena 20 v skladu z odstavkoma 2 in 3 tega člena naložijo ustrezno visoke upravne globe v višini najmanj 10 000 000 EUR ali 2 % skupnega svetovnega letnega prometa podjetja, ki mu pripada bistveni ali pomembni subjekt, v preteklem proračunskem letu, kateri koli znesek je višji.

5. Države članice lahko določijo pooblastila za naložitev periodičnih denarnih kazni, s katerimi se bistveni ali pomembni subjekt prisili, da preneha s kršitvijo v skladu s predhodno odločitvijo pristojnega organa.

6. Brez poseganja v pooblastila pristojnih organov na podlagi členov 29 in 30 lahko vsaka država članica določi pravila o tem, ali in v kolikšni meri se lahko subjektom javne uprave iz člena 4(23) naložijo upravne globe, v skladu z obveznostmi, določenimi v tej direktivi.

Člen 32

Kršitve, ki pomenijo kršitev varstva osebnih podatkov

1. Če imajo pristojni organi informacije, ki kažejo, da kršitev obveznosti iz členov 18 in 20 s strani bistvenega ali pomembnega subjekta pomeni kršitev varstva osebnih podatkov, kot je opredeljena v členu 4(12) Uredbe (EU) 2016/679 in ki se uradno sporoči v skladu s členom 33 navedene uredbe, o tem v razumnem času obvestijo nadzorne organe, ki so pristojni v skladu s členoma 55 in 56 navedene uredbe.

2. Če se nadzorni organi, pristojni v skladu s členoma 55 in 56 Uredbe (EU) 2016/679, odločijo, da bodo izvajali svoja pooblastila v skladu s členom 58(i) navedene uredbe, in naložijo upravno globo, pristojni organi ne naložijo upravne globe za isto kršitev po členu 31 te direktive. Vendar lahko pristojni organi uporabijo izvršilne ukrepe ali izvajajo pooblastila za naložitev sankcij iz točk (a) do (i) člena 29(4), člena 29(5) in točk (a) do (h) člena 30(4) te direktive.

3. Če ima nadzorni organ, ki je pristojen v skladu z Uredbo (EU) 2016/679, sedež v drugi državi članici kot pristojni organ, lahko pristojni organ obvesti nadzorni organ, ki ima sedež v isti državi članici.

Člen 33

Kazni

1. Države članice določijo pravila o kaznih, ki se uporabljajo za kršitve nacionalnih določb, sprejetih v skladu s to direktivo, in sprejmejo vse potrebne ukrepe za zagotovitev njihovega izvajanja. Te kazni so učinkovite, sorazmerne in odvračilne.

2. Države članice do [dve leti po začetku veljavnosti te direktive] Komisijo uradno obvestijo o navedenih pravilih in ukrepih ter ji nemudoma uradno sporočijo vse poznejše spremembe, ki vplivajo nanje.

Člen 34

Medsebojna pomoč

1. Če bistveni ali pomembni subjekt opravlja storitve v več kot eni državi članici ali ima glavni sedež ali predstavnika v eni državi članici, omrežja in informacijske sisteme pa v eni ali več drugih državah članicah, pristojni organ države članice glavnega sedeža ali drugega sedeža ali predstavnika in pristojni organi teh drugih držav članic po potrebi sodelujejo in si pomagajo. Takšno sodelovanje vključuje vsaj naslednje:

   (a) pristojni organi, ki uporabljajo nadzorne ali izvršilne ukrepe v državi članici, prek enotne kontaktne točke obvestijo pristojne organe v drugih zadevnih državah članicah o sprejetih nadzornih in izvršilnih ukrepih ter njihovem nadaljnjem spremljanju in se posvetujejo z njimi v skladu s členoma 29 in 30;

   (b) pristojni organ lahko od drugega pristojnega organa zahteva, naj sprejme nadzorne ali izvršilne ukrepe iz členov 29 in 30;

   (c) pristojni organ po prejemu utemeljenega zahtevka drugega pristojnega organa temu organu zagotovi pomoč, da se lahko nadzorni ali izvršilni ukrepi iz členov 29 in 30 izvajajo učinkovito, uspešno in dosledno. Taka medsebojna pomoč lahko zajema zahtevke za informacije in nadzorne ukrepe, vključno z zahtevki za izvajanje inšpekcijskih pregledov na kraju samem ali nadzora na daljavo ali ciljno usmerjenih varnostnih presoj. Pristojni organ, na katerega je naslovljen zahtevek za pomoč, takega zahtevka ne sme zavrniti, razen če se po izmenjavi informacij z drugimi zadevnimi organi, agencijo ENISA in Komisijo ugotovi, da bodisi organ ni pristojen za zagotavljanje zahtevane pomoči bodisi zahtevana pomoč ni sorazmerna z nadzornimi nalogami pristojnega organa, ki se izvajajo v skladu s členom 29 ali členom 30.

2. Kjer je ustrezno in na podlagi skupnega dogovora, lahko pristojni organi iz različnih držav članic izvajajo skupne nadzorne ukrepe iz členov 29 in 30.

POGLAVJE VII

Prehodne in končne določbe

Člen 35

Pregled

Komisija redno pregleduje delovanje te direktive ter poroča Evropskemu parlamentu in Svetu. V poročilu oceni zlasti pomen sektorjev, podsektorjev, velikosti in vrste subjektov iz prilog I in II za delovanje gospodarstva in družbe v zvezi s kibernetsko varnostjo. V ta namen in zaradi nadaljnje krepitve strateškega in operativnega sodelovanja Komisija upošteva poročila skupine za sodelovanje in mreže skupin CSIRT o izkušnjah, pridobljenih na strateški in operativni ravni. Prvo poročilo se predloži do… [54 mesecev po datumu začetka veljavnosti te direktive].

Člen 36

Izvajanje prenosa pooblastila

1. Pooblastilo za sprejemanje delegiranih aktov se prenese na Komisijo pod pogoji iz tega člena.
2. Pooblastilo za sprejemanje delegiranih aktov iz členov 18(6) in 21(2) se prenese na Komisijo za obdobje petih let od […].
3. Prenos pooblastila iz členov 18(6) in 21(2) lahko kadar koli prekliče Evropski parlament ali Svet. S sklepom o preklicu preneha veljati prenos pooblastila iz navedenega sklepa. Sklep začne veljati dan po njegovi objavi v *Uradnem listu Evropske unije* ali na poznejši dan, ki je določen v navedenem sklepu. Sklep ne vpliva na veljavnost že veljavnih delegiranih aktov.
4. Komisija se pred sprejetjem delegiranega akta posvetuje s strokovnjaki, ki jih imenujejo države članice, v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje.
5. Komisija takoj po sprejetju delegiranega akta o njem sočasno uradno obvesti Evropski parlament in Svet.
6. Delegirani akt, sprejet na podlagi členov 18(6) in 21(2), začne veljati le, če mu niti Evropski parlament niti Svet ne nasprotuje v dveh mesecih od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu ali če pred iztekom tega roka Evropski parlament in Svet obvestita Komisijo, da mu ne bosta nasprotovala. Ta rok se na pobudo Evropskega parlamenta ali Sveta podaljša za dva meseca.

Člen 37

Postopek v odboru

1. Komisiji pomaga odbor. Ta odbor je odbor v smislu Uredbe (EU) št. 182/2011.
2. Pri sklicevanju na ta odstavek se uporablja člen 5 Uredbe (EU) št. 182/2011.

3. Kadar je treba pridobiti mnenje odbora na podlagi pisnega postopka, se ta postopek zaključi brez izida, ko v roku za izdajo mnenja tako odloči predsednik odbora ali to zahteva član odbora.

Člen 38

Prenos

1. Države članice sprejmejo in objavijo zakone in druge predpise, potrebne za uskladitev s to direktivo, do … [18 mesecev po datumu začetka veljavnosti te direktive]. O tem nemudoma obvestijo Komisijo. Te predpise uporabljajo od … [dan po datumu iz prvega odstavka].
2. Države članice se v sprejetih predpisih sklicujejo na to direktivo ali pa sklic nanjo navedejo ob njihovi uradni objavi. Način sklicevanja določijo države članice.

Člen 39

Sprememba Uredbe (EU) št. 910/2014

Člen 19 Uredbe (EU) št. 910/2014 se črta.

Člen 40

Sprememba Direktive (EU) 2018/1972

Člena 40 in 41 Direktive (EU) 2018/1972 se črtata.

Člen 41

Razveljavitev

Direktiva (EU) 2016/1148 se razveljavi z učinkom od [datum roka za prenos Direktive].

Sklicevanje na Direktivo (EU) 2016/1148 se šteje za sklicevanje na to direktivo in se bere v skladu s korelacijsko tabelo iz Priloge III.

Člen 42

Začetek veljavnosti

Ta direktiva začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Člen 43

Naslovniki

Ta direktiva je naslovljena na države članice.

V Bruslju,

Za Evropski parlament	*Za Svet*
Predsednik	*Predsednik*

OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

Kazalo

1. OKVIR PREDLOGA/POBUDE

1.1. Naslov predloga/pobude

Predlog direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148

1.2. Zadevna področja *(programski sklop)*

Komunikacijska omrežja, vsebine in tehnologija

1.3. Ukrep, na katerega se predlog/pobuda nanaša

☐ **Nov ukrep**

☐ **Nov ukrep na podlagi pilotnega projekta/pripravljalnega ukrepa**[40]

☒ **Podaljšanje obstoječega ukrepa**

☐ **Združitev ali preusmeritev enega ali več ukrepov v drug/nov ukrep**

1.4. Utemeljitev predloga/pobude

1.4.1. Potrebe, ki jih je treba zadovoljiti kratkoročno ali dolgoročno, vključno s podrobno časovnico za uvajanje ustreznih ukrepov za izvajanje pobude

Cilj revizije je zvišati raven kibernetske odpornosti obsežne skupine podjetij, ki delujejo v Evropski uniji, v vseh ustreznih sektorjih, zmanjšati razlike v odpornosti na notranjem trgu v sektorjih, ki so že zajeti z Direktivo, in izboljšati raven skupnega situacijskega zavedanja in skupne zmogljivosti za pripravo in odzivanje.

1.4.2. Dodana vrednost ukrepanja Unije (ki je lahko posledica različnih dejavnikov, npr. boljšega usklajevanja, pravne varnosti, večje učinkovitosti ali dopolnjevanja). Za namene te točke je „dodana vrednost ukrepanja Unije“ vrednost, ki izhaja iz ukrepanja Unije in predstavlja dodatno vrednost poleg tiste, ki bi jo sicer ustvarile države članice same.

Kibernetska odpornost v Uniji ne more biti učinkovita, če se k njej zaradi nacionalnih ali regionalnih omejitev pristopa neenotno. V direktivi o varnosti omrežij in informacijskih sistemov so te pomanjkljivosti obravnavane z določitvijo okvira za varnost omrežij in informacijskih sistemov na nacionalni ravni in ravni Unije. Vendar je prvi redni pregled direktive o varnosti omrežij in informacijskih sistemov pokazal več pomanjkljivosti, ki so sčasoma privedle do precejšnjih razlik med državami članicami, kar zadeva zmogljivosti, načrtovanje in raven zaščite, ki hkrati vplivajo na enake konkurenčne pogoje podobnih podjetij na notranjem trgu. Ukrepanje EU, ki presega sedanje ukrepe iz direktive o varnosti omrežij in informacijskih sistemov, je upravičeno zlasti zaradi: (i) čezmejne narave problematike; (ii) možnosti, da se z ukrepi EU izboljšajo in olajšajo učinkovite nacionalne politike, ter (iii) prispevka usklajenih in skupnih ukrepov politike na področju varnosti omrežij in informacijskih sistemov k učinkovitemu varstvu podatkov in zasebnosti. Navedeni cilji se lahko tako bolje dosežejo z ukrepi na ravni EU kot na ravni držav članic.

[40] Po členu 58(2)(a) oz. (b) finančne uredbe.

1.4.3. Spoznanja iz podobnih izkušenj v preteklosti

Direktiva o varnosti omrežij in informacijskih sistemov je prvi horizontalni instrument notranjega trga, ki je namenjen povečanju odpornosti omrežij in sistemov v Uniji proti tveganjem za kibernetsko varnost. Direktiva je že veliko prispevala k zvišanju skupne ravni kibernetske varnosti v državah članicah. Vendar so se pri pregledu delovanja in izvajanja Direktive pokazale številne pomanjkljivosti, ki jih je treba poleg vse večje digitalizacije in potrebe po bolj posodobljenem odzivu obravnavati v revidiranem pravnem aktu.

1.4.4. Skladnost in možne sinergije z drugimi ustreznimi instrumenti

Novi predlog je v celoti skladen z drugimi povezanimi pobudami, kot sta predlog uredbe o digitalni operativni odpornosti za finančni sektor in predlog direktive o odpornosti kritičnih izvajalcev bistvenih storitev. Skladen je tudi z Evropskim zakonikom o elektronskih komunikacijah, Splošno uredbo o varstvu podatkov in uredbo eIDAS.

Predlog je bistveni del strategije EU za varnostno unijo.

1.5. Trajanje predloga/pobude in finančnih posledic

☐ **Časovno omejeno**

– ☐ od [DD. MM.] LLLL do [DD. MM.] LLLL,

– ☐ finančne posledice med letoma LLLL in LLLL za odobritve za prevzem obveznosti ter med letoma LLLL in LLLL za odobritve plačil.

☒ **Časovno neomejeno**

– izvajanje z obdobjem uvajanja med letoma 2022 in 2025,

– ki mu sledi izvajanje v celoti.

1.6. Načrtovani načini upravljanja[41]

Neposredno upravljanje – Komisija:

– ☒ z lastnimi službami, vključno s svojim osebjem v delegacijah Unije,

– ☐prek izvajalskih agencij.

☐ **Deljeno upravljanje** z državami članicami.

☐ **Posredno upravljanje,** tako da se naloge izvrševanja proračuna poverijo:

– ☐ tretjim državam ali organom, ki jih te imenujejo,

– ☐ mednarodnim organizacijam in njihovim agencijam (navedite),

– ☐ EIB in Evropskemu investicijskemu skladu,

– ☐ organom iz členov 70 in 71 finančne uredbe,

– ☐ subjektom javnega prava,

– ☐ subjektom zasebnega prava, ki opravljajo javne storitve, kolikor ti subjekti zagotavljajo ustrezna finančna jamstva,

– ☐ subjektom zasebnega prava države članice, ki so pooblaščeni za izvajanje javno-zasebnih partnerstev in ki zagotavljajo ustrezna finančna jamstva,

– ☐ osebam, pooblaščenim za izvajanje določenih ukrepov SZVP na podlagi naslova V PEU in opredeljenim v zadevnem temeljnem aktu.

– *Pri navedbi več kot enega načina upravljanja je treba to natančneje obrazložiti v oddelku „opombe“.*

Opombe

Agencija Evropske unije za kibernetsko varnost ENISA, ki ji je bil z Aktom o kibernetski varnosti podeljen nov trajni mandat, bi pomagala državam članicam in Komisiji pri izvajanju revidirane direktive o varnosti omrežij in informacijskih sistemov.

Na podlagi revidirane direktive o varnosti omrežij in informacijskih sistemov bo imela agencija ENISA od leta 2022/23 dodatna področja ukrepanja. Čeprav bodo ta področja ukrepanja zajeta s splošnimi nalogami agencije ENISA v skladu z njenim mandatom, bodo ustvarila dodatno delovno obremenitev za Agencijo. Natančneje, poleg sedanjih področij ukrepanja bo morala agencija ENISA v skladu s predlogom Komisije za revidirano direktivo o varnosti omrežij in informacijskih sistemov v svoj delovni program posebej vključiti med drugim naslednje ukrepe: (i) razvoj in vzdrževanje evropskega registra šibkih točk (člen 6(2)

[41] Pojasnila o načinih upravljanja in sklici na finančno uredbo so na voljo na spletišču BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

predloga), (ii) zagotovitev sekretariata evropske organizacijske mreže za povezovanje v kibernetski krizi (EU-CyCLONe) (člen 14 predloga) in izdajo letnega poročila o stanju kibernetske varnosti v EU (člen 15 predloga), (iii) podpiranje organizacije medsebojnih strokovnih pregledov med državami članicami (člen 16 predloga), (iv) zbiranje zbirnih podatkov držav članic o incidentih in izdajo tehničnih smernic (člen 20(9) predloga), (v) vzpostavitev in vzdrževanje registra za subjekte, ki opravljajo čezmejne storitve (člen 25 predloga).

Zato se bo od leta 2022 zahtevalo dodatnih pet EPDČ z ustreznimi proračunskimi sredstvi v višini približno 0,61 milijona EUR na leto za pokrivanje teh novih delovnih mest (glej ločeni računovodski izkaz za agencije).

2. UKREPI UPRAVLJANJA

2.1. Pravila o spremljanju in poročanju

Navedite pogostost in pogoje.

Komisija bo redno pregledovala delovanje Direktive ter poročala Evropskemu parlamentu in Svetu, prvič tri leta po začetku njene veljavnosti. Ocenila bo tudi, ali so države članice pravilno prenesle Direktivo.

2.2. Upravljavski in kontrolni sistemi

2.2.1. Utemeljitev načinov upravljanja, mehanizmov financiranja, načinov plačevanja in predlagane strategije kontrol

Izvajanje Direktive bo upravljala enota v okviru GD CNECT, pristojna za to področje politike.

2.2.2. Podatki o ugotovljenih tveganjih in vzpostavljenih sistemih notranjih kontrol za njihovo zmanjševanje

Zelo majhno tveganje, ker je ekosistem direktive o varnosti omrežij in informacijskih sistemov že vzpostavljen.

2.2.3. Ocena in utemeljitev stroškovne učinkovitosti kontrol (razmerje „stroški kontrol ÷ vrednost z njimi povezanih upravljanih sredstev“) ter ocena pričakovane stopnje tveganja napake (ob plačilu in ob zaključku)

Ni relevantno. Samo uporaba upravnega proračuna (splošna sredstva).

2.3. Ukrepi za preprečevanje goljufij in nepravilnosti

Navedite obstoječe ali načrtovane preprečevalne in zaščitne ukrepe, npr. iz strategije za boj proti goljufijam.

Ni relevantno. Samo uporaba upravnega proračuna (splošna sredstva).

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

3.1. Zadevni razdelek večletnega finančnega okvira in predlagane nove odhodkovne proračunske vrstice

Razdelek večletnega finančnega okvira	Proračunska vrstica	Vrsta odhodkov	Prispevek			
	številka [razdelek…7……...……]	dif./nedif.[42]	držav Efte[43]	držav kandidatk[44]	tretjih držav	po členu [21(2)(b)] finančne uredbe
	20 02 06 odhodki za upravljanje 20 02 06	nedif.	NE	NE	NE	NE

[42] dif. Dif. = diferencirana sredstva/nedif. = nediferencirana sredstva.

[43] EFTA: Evropsko združenje za prosto trgovino.

[44] Države kandidatke in po potrebi potencialne države kandidatke z Zahodnega Balkana.

3.2. Ocenjene posledice za odhodke

3.2.1. Povzetek ocenjenih posledic za odhodke

v mio. EUR (na tri decimalna mesta natančno)

Razdelek večletnega finančnega okvira	**<…>**	[razdelek……..……]

			2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Po letu 2027***	**SKUPAJ**
Odobritve za poslovanje (razdeljene glede na proračunske vrstice iz naslova 3.1)	obveznosti	(1)									
	plačila	(2)									
Odobritve za upravne zadeve, ki se financirajo iz sredstev programa[45]	obveznosti = plačila	(3)									
Odobritve za sredstva programa SKUPAJ	obveznosti	= 1 + 3									
	plačila	= 2 + 3									

Razdelek večletnega finančnega okvira	7	„Upravni odhodki“ Seje: plenarne seje skupine za sodelovanje na področju varnosti omrežij in informacijskih sistemov običajno potekajo štirikrat letno. Komisija krije stroške hrane in pijače ter potne stroške predstavnikov 27 držav članic (en predstavnik na državo članico). Stroški seje lahko znašajo do 15 000 EUR. Službena potovanja: službena potovanja se nanašajo na spremljanje izvajanja direktive o varnosti omrežij in informacijskih sistemov. Primer: v enem letu (od maja 2019 do julija 2020) naj bi organizirali obiske držav v zvezi z varnostjo omrežij

[45] Tehnična in/ali upravna pomoč ter odhodki za podporo izvajanju programov in/ali ukrepov EU (prej vrstice BA), posredne raziskave, neposredne raziskave.

		in informacijskih sistemov in obiskali vseh 27 držav članic, da bi razpravljali o izvajanju direktive o varnosti omrežij in informacijskih sistemov v EU.

Ta oddelek se izpolni s „proračunskimi podatki upravne narave“, ki jih je treba najprej vnesti v Prilogo k oceni finančnih posledic zakonodajnega predloga, ki se prenese v sistem DECIDE za namene posvetovanj med službami.

v mio. EUR (na tri decimalna mesta natančno)

		2021	2022	2023	2024	2025	2026	2027	*Po letu 2027*	SKUPAJ
Človeški viri		1,14	1,14	1,14	1,14	1,14	1,14	**1,14**		**7,98**
Drugi upravni odhodki		**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**		**0,63**
Odobritve iz RAZDELKA 7 večletnega finančnega okvira SKUPAJ	(obveznosti skupaj = plačila skupaj)	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**		**8,61**

v mio. EUR (na tri decimalna mesta natančno)

		2021	2022	2023	2024	2025	2026	2027	*Po letu 2027*	SKUPAJ
Odobritve iz vseh RAZDELKOV večletnega finančnega okvira **SKUPAJ**	obveznosti									
	plačila									

3.2.2. Povzetek ocenjenih posledic za odobritve za upravne zadeve

– ☐ Za predlog/pobudo niso potrebne odobritve za upravne zadeve.

– ☐X Za predlog/pobudo so potrebne odobritve za upravne zadeve, kot je pojasnjeno v nadaljevanju:

v mio. EUR (na tri decimalna mesta natančno)

Leto	2021	2022	2023	2024	2025	2026	2027	SKUPAJ
RAZDELEK 7 večletnega finančnega okvira								
Človeški viri	1,14	1,14	1,14	1,14	1,14	1,14	**1,14**	**7,98**
Drugi upravni odhodki	0,09	0,09	0,09	0,09	0,09	0,09	**0,09**	**0,63**
Seštevek za RAZDELEK 7 večletnega finančnega okvira	1,23	1,23	1,23	1,23	1,23	1,23	**1,23**	**8,61**

Odobritve zunaj RAZDELKA 7[46] večletnega finančnega okvira								
Človeški viri								
Drugi upravni odhodki								
Seštevek za odobritve zunaj RAZDELKA 7 večletnega finančnega okvira								

SKUPAJ	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**8,61**

Potrebe po odobritvah za človeške vire in druge upravne odhodke se krijejo z odobritvami GD, ki so že dodeljene za upravljanje ukrepa in/ali so bile prerazporejene znotraj GD, po potrebi skupaj z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v postopku letne dodelitve virov glede na proračunske omejitve.

[46] Tehnična in/ali upravna pomoč ter odhodki za podporo izvajanju programov in/ali ukrepov EU (prej vrstice BA), posredne raziskave, neposredne raziskave.

3.2.2.1. Ocenjene potrebe po človeških virih

– ☐ Za predlog/pobudo niso potrebni človeški viri.

– X☐ Za predlog/pobudo so potrebni človeški viri, kot je pojasnjeno v nadaljevanju:

ocena, izražena v ekvivalentu polnega delovnega časa

Leto		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Delovna mesta v skladu s kadrovskim načrtom (uradniki in začasni uslužbenci)								
Sedež in predstavništva Komisije		6	6	6	6	6	6	6
Delegacije								
Raziskave								
• Zunanji sodelavci (v ekvivalentu polnega delovnega časa: EPDČ) – PU, LU, NNS, ZU in MSD [47] Razdelek 7								
Financirano iz RAZDELKA 7 večletnega finančnega okvira	– na sedežu	3	3	3	3	3	3	3
	– na delegacijah							
Financirano iz sredstev programa [48]	– na sedežu							
	– na delegacijah							
Raziskave								
Drugo (navedite)								
SKUPAJ		**9**	**9**	**9**	**9**	**9**	**9**	**9**

Potrebe po človeških virih se krijejo z osebjem GD, ki je že dodeljeno za upravljanje ukrepa in/ali je bilo prerazporejeno znotraj GD, po potrebi skupaj z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v postopku letne dodelitve virov glede na proračunske omejitve.

Opis nalog:

Uradniki in začasni uslužbenci	• Priprava delegiranih aktov v skladu s členom 18(6), členom 21(2) in členom 36 • Priprava izvedbenih aktov v skladu s členom 12(8), členom 18(5) in členom 20(11) • Zagotavljanje sekretariata za skupino za sodelovanje na področju varnosti omrežij in informacijskih sistemov • Organizacija plenarnih sej in sestankov o delovnem toku skupine za sodelovanje na področju varnosti omrežij in informacijskih sistemov • Usklajevanje dela držav članic v zvezi z različnimi dokumenti (smernice, zbirke orodij itd.) • Sodelovanje z drugimi službami Komisije, agencijo ENISA in nacionalnimi organi glede izvajanja direktive o varnosti omrežij in informacijskih sistemov • Analiza nacionalnih metod in dobrih praks, povezanih z izvajanjem direktive o varnosti omrežij in informacijskih sistemov
Zunanji sodelavci	Po potrebi zagotavljanje podpore pri vseh zgoraj navedenih nalogah

[47] PU = pogodbeni uslužbenec; LU = lokalni uslužbenec; NNS = napoteni nacionalni strokovnjak; ZU = začasni uslužbenec; MSD = mladi strokovnjak na delegaciji.

[48] Dodatna zgornja meja za zunanje sodelavce v okviru odobritev za poslovanje (prej vrstice BA).

3.2.3. Udeležba tretjih oseb pri financiranju

V predlogu/pobudi:

– X☐ ni načrtovano sofinanciranje tretjih oseb,

– ☐ je načrtovano sofinanciranje, kot je ocenjeno v nadaljevanju:

odobritve v mio. EUR (na tri decimalna mesta natančno)

Leto	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**SKUPAJ**
Navedite organ, ki bo sofinanciral predlog/pobudo								
Sofinancirane odobritve SKUPAJ								

3.3. Ocenjene posledice za prihodke

– ☐X Predlog/pobuda nima finančnih posledic za prihodke.

– ☐ Predlog/pobuda ima finančne posledice, kot je pojasnjeno v nadaljevanju:

☐ za lastna sredstva,

☐ za druge prihodke.

navedite, ali so prihodki dodeljeni za odhodkovne vrstice ☐

v mio. EUR (na tri decimalna mesta natančno)

Prihodkovna proračunska vrstica	Posledice predloga/pobude[49]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Člen …….							

Za namenske prejemke navedite zadevne odhodkovne proračunske vrstice.

Druge opombe (npr. metoda/formula za izračun posledic za prihodke ali druge informacije).

[49] Pri tradicionalnih lastnih sredstvih (carine, prelevmani na sladkor) se navedejo neto zneski, tj. bruto zneski po odbitku 20 % stroškov pobiranja.

PRILOGA

k OCENI FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

Naslov predloga/pobude:

Predlog direktive o reviziji Direktive (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji

……
……

1. ŠTEVILO in STROŠKI PREDVIDENIH POTREBNIH ČLOVEŠKIH VIROV

2. STROŠKI DRUGIH UPRAVNIH ODHODKOV

3. METODE IZRAČUNA ZA OCENO STROŠKOV

3.1 Človeški viri

3.2 Drugi upravni odhodki

*Ta priloga, **ki jo izpolni vsak GD/vsaka služba, ki sodeluje pri predlogu/pobudi**, mora biti priložena oceni finančnih posledic zakonodajnega predloga pri posvetovanju med službami.*

Preglednice s podatki se uporabljajo kot vir za preglednice iz ocene finančnih posledic zakonodajnega predloga. Namenjene so izključno notranji uporabi znotraj Komisije.

1. Stroški predvidenih potrebnih človeških virov

☐ Za predlog/pobudo niso potrebni človeški viri

X☐ Za predlog/pobudo so potrebni človeški viri, kot je pojasnjeno v nadaljevanju:

v mio. EUR (na tri decimalna mesta natančno)

RAZDELEK 7 večletnega finančnega okvira		2021		2022		2023		2024		2025		2026		2027		SKUPAJ	
		EPDČ	odobritve	EPDČ	odobritve	EPDČ	odobritve	EPDČ	odobritve	EPDČ	odobritve	EPDČ	odobritve	EPDČ	odobritve	EPDČ	odobritve
• Delovna mesta v skladu s kadrovskim načrtom (uradniki in začasni uslužbenci)																	
Sedež in predstavništva Komisije	uslužbenec AD	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	42	6,3
	uslužbenec AST																
V delegacijah Unije	uslužbenec AD																
	uslužbenec AST																
• Zunanji sodelavci [50] 0,24																	
Splošna sredstva	PU	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21	1,68
	NNS																
	ZU																
V delegacijah Unije	PU																

[50] PU = pogodbeni uslužbenec; LU = lokalni uslužbenec; NNS = napoteni nacionalni strokovnjak; ZU = začasni uslužbenec; MSD = mladi strokovnjak na delegaciji.

	LU																
	NNS																
	ZU																
	MSD																
Druge proračunske vrstice (*navedite*)																	
Seštevek – RAZDELEK 7 večletnega finančnega okvira		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63	7,98

Potrebe po človeških virih se krijejo z osebjem GD, ki je že dodeljeno za upravljanje ukrepa in/ali je bilo prerazporejeno znotraj GD, po potrebi skupaj z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v postopku letne dodelitve virov glede na proračunske omejitve.

Odobritve zunaj RAZDELKA 7 večletnega finančnega okvira			2021		2022		2023		2024		2025		2025		2025		SKUPAJ	
			EPDČ	odobritve	EPDČ	odobritve	EPDČ	odobritve	EPDČ	odobritve	EPDČ	odobritve	EPDČ	odobritve	EPDČ	odobritve	EPDČ	odobritve
• Delovna mesta v skladu s kadrovskim načrtom (uradniki in začasni uslužbenci)																		
Raziskave		uslužbenec AD																
		uslužbenec AST																
• Zunanji sodelavci [51]																		
Zunanji sodelavci v okviru odobritev za poslovanje (nekdanje vrstice BA)	– na sedežu	PU																
		NNS																
		ZU																
	– v delegacijah Unije	PU																
		LU																
		NNS																
		ZU																
		MSD																
Raziskave		PU																
		NNS																

[51] PU = pogodbeni uslužbenec; LU = lokalni uslužbenec; NNS = napoteni nacionalni strokovnjak; ZU = začasni uslužbenec; MSD = mladi strokovnjak na delegaciji.

	ZU																
Druge proračunske vrstice (*navedite*)																	
Seštevek – odobritve zunaj RAZDELKA 7 večletnega finančnega okvira																	

Potrebe po človeških virih se krijejo z osebjem GD, ki je že dodeljeno za upravljanje ukrepa in/ali je bilo prerazporejeno znotraj GD, po potrebi skupaj z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v postopku letne dodelitve virov glede na proračunske omejitve.

Ocenjene posledice za človeške vire agencije ENISA

Agencija Evropske unije za kibernetsko varnost ENISA, ki ji je bil z Aktom o kibernetski varnosti podeljen nov trajni mandat, bi pomagala državam članicam in Komisiji pri izvajanju revidirane direktive o varnosti omrežij in informacijskih sistemov.

Na podlagi revidirane direktive o varnosti omrežij in informacijskih sistemov bo imela agencija ENISA od leta 2022/23 dodatna področja ukrepanja. Čeprav bodo ta področja ukrepanja zajeta s splošnimi nalogami agencije ENISA v skladu z njenim mandatom, bodo ustvarila dodatno delovno obremenitev za Agencijo. Natančneje, poleg sedanjih področij ukrepanja bo morala ENISA v skladu s predlogom Komisije za revidirano direktivo o varnosti omrežij in informacijskih sistemov v svoj delovni program posebej vključiti med drugim naslednje ukrepe: (i) razvoj in vzdrževanje evropskega registra šibkih točk (člen 6(2) predloga), (ii) zagotovitev sekretariata evropske organizacijske mreže za povezovanje v kibernetski krizi (EU-CyCLONe) (člen 14 predloga) in izdajo letnega poročila o stanju kibernetske varnosti v EU (člen 15 predloga), (iii) podpiranje organizacije medsebojnih strokovnih pregledov med državami članicami (člen 16 predloga), (iv) zbiranje zbirnih podatkov držav članic o incidentih in izdajo tehničnih smernic (člen 20(9) predloga), (v) vzpostavitev in vzdrževanje registra za subjekte, ki opravljajo čezmejne storitve (člen 25 predloga).

Zato se bo od leta 2022 zahtevalo dodatnih pet EPDČ z ustreznimi proračunskimi sredstvi v višini približno 0,61 milijona EUR na leto za pokrivanje teh novih delovnih mest (glej ločeni računovodski izkaz za agencije).

Zato se bo od leta 2022 zahtevalo dodatnih pet EPDČ z ustreznimi proračunskimi sredstvi za pokrivanje teh novih delovnih mest.

☐ Za predlog/pobudo niso potrebne odobritve za upravne zadeve.

☐X Za predlog/pobudo so potrebne odobritve za upravne zadeve, kot je pojasnjeno v nadaljevanju:

v mio. EUR (na tri decimalna mesta natančno)

	Leto **N** [52] **2022**	Leto **N+1** **2023**	Leto **N+2** **2024**	Leto **N+3** **2025**	Vstavite ustrezno število let glede na trajanje posledic (glej točko 1.6)			**SKUPAJ**
Začasni uslužbenci (razredi AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**

[52] Leto N je leto začetka izvajanja predloga/pobude. Nadomestite „N“ s pričakovanim prvim letom izvajanja (na primer: 2021). Enako storite za naslednja leta.

Začasni uslužbenci (razredi AST)								
Pogodbeni uslužbenci	0,160	0,160	0,160	0,160	0,160	0,160		
Napoteni nacionalni strokovnjaki								**0,96**

SKUPAJ	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Potrebe po uslužbencih (EPDČ):

	Leto **N** [53] **2022**	Leto **N+1** **2023**	Leto **N+2** **2024**	Leto **N+3** **2025**	Vstavite ustrezno število let glede na trajanje posledic (glej točko 1.6)	**SKUPAJ**
Začasni uslužbenci (razredi AD)	3	3	3	3	3	3		**18**
Začasni uslužbenci (razredi AST)								
Pogodbeni uslužbenci	2	2	2	2	2	2		**12**
Napoteni nacionalni strokovnjaki								

[53] Leto N je leto začetka izvajanja predloga/pobude. Nadomestite „N“ s pričakovanim prvim letom izvajanja (na primer: 2021). Enako storite za naslednja leta.

SKUPAJ	**5**	**5**	**5**	**5**	**5**	**5**		**30**

2. Stroški drugih upravnih odhodkov

☐ Za predlog/pobudo niso potrebne odobritve za upravne zadeve
☐ Za predlog/pobudo so potrebne odobritve za upravne zadeve, kot je pojasnjeno v nadaljevanju:

v mio. EUR (na tri decimalna mesta natančno)

RAZDELEK 7 večletnega finančnega okvira	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Skupaj**
Na sedežu:								
Stroški za službena potovanja in reprezentančni stroški	0,03	0,03	0,03	0,03	0,03	0,03	0,03	**0,21**
Stroški za konference in sestanke	0,06	0,06	0,06	0,06	0,06	0,06	0,06	**0,42**
Odbori[54]								
Študije in posvetovanja								
Informacijski in upravljavski sistemi								
Oprema in storitve IKT[55]								

[54] Navedite vrsto odbora in skupino, v katero spada.
[55] IKT: informacijske in komunikacijske tehnologije: posvetovati se je treba z DIGIT.

Druge proračunske vrstice (*po potrebi navedite*)								
V delegacijah Unije								
Stroški za službena potovanja in konference ter reprezentančni stroški								
Nadaljnje usposabljanje osebja								
Nakup ali najem stavb in s tem povezani odhodki								
Oprema, pohištvo, dobave in storitve								
Seštevek za RAZDELEK 7 večletnega finančnega okvira	0,09	0,09	0,09	0,09	0,09	0,09	0,09	**0,63**

v mio. EUR (na tri decimalna mesta natančno)

Odobritve zunaj RAZDELKA 7 večletnega finančnega okvira	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Skupaj**
Odhodki za tehnično in upravno pomoč (brez zunanjih sodelavcev) iz odobritev za poslovanje (nekdanje vrstice BA)								
– na sedežu								
– v delegacijah Unije								
Drugi odhodki za upravljanje v raziskovalni dejavnosti								
Druge proračunske vrstice (*po potrebi navedite*)								
Seštevek – odobritve zunaj RAZDELKA 7 večletnega finančnega okvira								

SKUPAJ RAZDELEK 7 in zunaj RAZDELKA 7 večletnega finančnega okvira	1,23	1,23	1,23	1,23	1,23	1,23	1,23	**8,61**

Zahtevane upravne odobritve bodo krite iz odobritev, ki so že dodeljene za upravljanje ukrepa in/ali so bile prerazporejene znotraj GD, po potrebi skupaj z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v postopku letne dodelitve virov glede na obstoječe proračunske omejitve.

3. Metode izračuna za oceno stroškov

3.1 Človeški viri

Ta del določa metodo izračuna, ki se uporablja za ocenjevanje človeških virov, ki se štejejo za potrebne (predpostavke o količini dela, vključno s posebnimi delovnimi mesti (delovni profili Sysper 2), kategorije osebja in ustrezni povprečni stroški).

RAZDELEK 7 večletnega finančnega okvira

Opomba: povprečni stroški vsake kategorije uslužbencev na sedežu so dostopni na BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx.

• Uradniki in začasni uslužbenci

6 uradnikov v EPDČ (povprečni stroški 0,150) = 0,9 na leto

- Priprava delegiranih aktov v skladu s členom 18(6), členom 21(2) in členom 36
- Priprava izvedbenih aktov v skladu s členom 12(8), členom 18(5) in členom 20(11)
- Zagotavljanje sekretariata za skupino za sodelovanje na področju varnosti omrežij in informacijskih sistemov
- Organizacija plenarnih sej in sestankov o delovnem toku skupine za sodelovanje na področju varnosti omrežij in informacijskih sistemov
- Usklajevanje dela držav članic v zvezi z različnimi dokumenti (smernice, zbirke orodij itd.)
- Sodelovanje z drugimi službami Komisije, agencijo ENISA in nacionalnimi organi glede izvajanja direktive o varnosti omrežij in informacijskih sistemov
- Analiza nacionalnih metod in dobrih praks, povezanih z izvajanjem direktive o varnosti omrežij in informacijskih sistemov

• Zunanji sodelavci

3 PU (povprečni stroški 0,08) = 0,24 na leto

- Po potrebi zagotavljanje podpore pri vseh zgoraj navedenih nalogah

Odobritve zunaj RAZDELKA 7 večletnega finančnega okvira

• Samo delovna mesta, ki se financirajo iz proračuna za raziskave

• Zunanji sodelavci

3.2 Drugi upravni odhodki

Podrobno navedite metodo izračuna, uporabljeno za vsako proračunsko vrstico, zlasti z njo povezane predpostavke (npr. število letnih sestankov, povprečni stroški itd.).

RAZDELEK 7 večletnega finančnega okvira
Seje: plenarne seje skupine za sodelovanje na področju varnosti omrežij in informacijskih sistemov običajno potekajo štirikrat letno. Komisija krije stroške hrane in pijače ter potne stroške predstavnikov 27 držav članic (en predstavnik na državo članico). Stroški seje lahko znašajo do 15 000 EUR, kar pomeni 60 000 EUR na leto. Službena potovanja: službena potovanja se nanašajo na spremljanje izvajanja direktive o varnosti omrežij in informacijskih sistemov. Primer: v enem letu (od maja 2019 do julija 2020) naj bi organizirali obiske držav v zvezi z varnostjo omrežij in informacijskih sistemov in obiskali vseh 27 držav članic, da bi razpravljali o izvajanju direktive o varnosti omrežij in informacijskih sistemov v EU.

Odobritve zunaj RAZDELKA 7 večletnega finančnega okvira

PRILOGA 7

k SKLEPU KOMISIJE

o notranjih pravilih za izvrševanje splošnega proračuna Evropske unije (oddelek Evropske komisije), ki veljajo za službe Komisije

OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA – „AGENCIJE“

Ta ocena finančnih posledic zakonodajnega predloga zajema zahtevo za povečanje števila uslužbencev agencije ENISA za 5 EPDČ od leta 2022 za izvajanje dopolnilnih dejavnosti, povezanih z izvajanjem direktive o varnosti omrežij in informacijskih sistemov. Te dejavnosti so že zajete z mandatom agencije ENISA.

1. OKVIR PREDLOGA/POBUDE

1.1. Naslov predloga/pobude

Predlog direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148

1.2. Zadevna področja politike

Komunikacijska omrežja, vsebine in tehnologija

1.3. Ukrep, na katerega se predlog se nanaša

☐ **Nov ukrep**

☐ **Nov ukrep na podlagi pilotnega projekta/pripravljalnega ukrepa**[56]

☒ **Podaljšanje obstoječega ukrepa**

☐ **Združitev ali preusmeritev enega ali več ukrepov v drug/nov ukrep**

1.4. Cilji

1.4.1. Splošni cilji

Cilj revizije je zvišati raven kibernetske odpornosti obsežne skupine podjetij, ki delujejo v Evropski uniji, v vseh ustreznih sektorjih, zmanjšati razlike v odpornosti na notranjem trgu v sektorjih, ki so že zajeti z Direktivo, in izboljšati raven skupnega situacijskega zavedanja in skupne zmogljivosti za pripravo in odzivanje.

1.4.2. Specifični cilji

Za obravnavanje težave nizke ravni kibernetske odpornosti podjetij, ki delujejo v Evropski uniji, je specifični cilj zagotoviti, da se od subjektov v vseh sektorjih, ki so odvisni od omrežij in informacijskih sistemov ter opravljajo ključne storitve za gospodarstvo in družbo kot celoto, zahteva, naj sprejmejo ukrepe za kibernetsko varnost in poročajo o incidentih, da bi se zvišala splošna raven kibernetske odpornosti na notranjem trgu.

Za obravnavanje težave neskladne odpornosti po državah članicah in sektorjih je specifični cilj zagotoviti, da za vse subjekte, ki so dejavni v sektorjih, zajetih s pravnim okvirom za varnost omrežij in informacijskih sistemov, ter so podobno veliki in imajo primerljivo vlogo, velja ista regulativna ureditev (spadajo na področje uporabe ali ne), ne glede na to, v katero jurisdikcijo spadajo v EU.

Za zagotovitev, da morajo vsi subjekti, ki so dejavni v sektorjih, zajetih s pravnim okvirom za varnost omrežij in informacijskih sistemov, izpolnjevati enake obveznosti na podlagi koncepta obvladovanja tveganj, kar zadeva varnostne ukrepe, in poročati o vseh incidentih na podlagi enotnega sklopa meril, se mora s specifičnimi cilji zagotoviti, da pristojni organi učinkoviteje izvršujejo pravila, ki jih določa pravni instrument, z usklajenimi nadzornimi in izvršilnimi ukrepi, poleg tega pa morajo zagotoviti primerljivo raven virov po državah članicah, ki se dodelijo pristojnim organom, da bi jim omogočili izpolnjevanje temeljnih nalog, določenih z okvirom za varnost omrežij in informacijskih sistemov.

[56] V skladu s členom 58(2)(a) oz. (b) finančne uredbe.

Za obravnavanje težave skupnega situacijskega zavedanja in pomanjkanja skupnega odziva na krize se mora s specifičnim ciljem zagotoviti izmenjava bistvenih informacij med državami članicami z uvedbo jasnih obveznosti za pristojne organe, da si izmenjujejo informacije in sodelujejo na področju kibernetskih groženj in incidentov, ter z razvojem skupne zmogljivosti Unije za operativno odzivanje na krize.

1.4.3. Pričakovani rezultati in posledice

Navedite, kakšne posledice naj bi imel(-a) predlog/pobuda za upravičence/ciljne skupine.

Predlog naj bi prinesel pomembne koristi: ocene kažejo, da bi lahko privedel do znižanja stroškov kibernetskih incidentov za 11,3 milijarde EUR. Sektorsko področje uporabe bi bilo na podlagi okvira za varnost omrežij in informacijskih sistemov bistveno večje, poleg zgoraj navedenih koristi pa bi se za nove subjekte, ki bi bili zajeti, in pristojne organe uravnotežilo tudi breme, ki bi ga lahko ustvarile zahteve glede varnosti omrežij in informacijskih sistemov, zlasti z vidika nadzora. Razlog za to je, da bi bil z novim okvirom za varnost omrežij in informacijskih sistemov vzpostavljen dvostopenjski pristop, s poudarkom na velikih in ključnih subjektih ter razlikovanju nadzorne ureditve, ki omogoča samo naknadni nadzor velikega števila subjektov, zlasti tistih, ki se štejejo za „pomembne“, ne pa za „bistvene“.

Na splošno bi predlog privedel do učinkovitih kompromisov in sinergij, z največjim potencialom izmed vseh analiziranih možnosti politike za zagotovitev višje in usklajene ravni kibernetske odpornosti ključnih subjektov po vsej Uniji, ki bi na koncu privedla do znižanja stroškov za podjetja in družbo.

Predlog bi zadevnim organom držav članic prinesel tudi nekatere stroške v zvezi z izpolnjevanjem obveznosti in izvrševanjem (po ocenah naj bi se viri povečali za približno 20–30 %). Vendar bi novi okvir prinesel tudi pomembne koristi z boljšim pregledom ključnih podjetij in sodelovanjem z njimi, okrepljenim čezmejnim operativnim sodelovanjem ter medsebojno pomočjo in mehanizmi medsebojnih strokovnih pregledov. To bi privedlo do splošnega povečanja zmogljivosti za kibernetsko varnost v državah članicah.

Ocenjuje se, da bi morala podjetja, ki bi spadala na področje uporabe okvira za varnost omrežij in informacijskih sistemov, v prvih letih po uvedbi novega okvira za varnost omrežij in informacijskih sistemov svojo sedanjo porabo za varnost IKT povečati za največ 22 % (pri podjetjih, ki že spadajo na področje uporabe sedanje direktive o varnosti omrežij in informacijskih sistemov, bi bilo to povečanje 12-odstotno). Vendar bi to povprečno povečanje porabe za varnost IKT privedlo do sorazmerne koristi takih naložb, zlasti zaradi znatnega znižanja stroškov kibernetskih incidentov (ocenjenega na 118 milijard EUR v desetih letih).

Mala in mikro podjetja bi bila izvzeta s področja uporabe okvira za varnost omrežij in informacijskih sistemov. Za srednja podjetja se lahko pričakuje, da se bo raven porabe za varnost IKT v prvih letih po uvedbi novega okvira za varnost omrežij in informacijskih sistemov povečala. Hkrati bi zvišanje ravni varnostnih zahtev za te subjekte zagotovilo spodbude za njihove zmogljivosti za kibernetsko varnost in prispevalo k izboljšanju obvladovanja tveganj na področju IKT.

Vplivalo bi tudi na nacionalne proračune in uprave: kratko- in srednjeročno bi bilo po ocenah pričakovati 20–30-odstotno povečanje virov.

Drugi pomembnejši negativni učinki niso pričakovani. Predlog naj bi zagotovil zanesljivejše zmogljivosti za kibernetsko varnost, zaradi česar naj bi imel večji blažilni učinek na število in resnost incidentov, vključno s kršitvami varstva podatkov. Verjetno bo imel tudi pozitiven učinek na zagotavljanje enakih konkurenčnih pogojev po državah članicah za vse subjekte, ki spadajo na področje uporabe okvira za varnost omrežij in informacijskih sistemov, ter zmanjšal asimetrijo informacij o kibernetski varnosti.

1.4.4. Kazalniki smotrnosti

Navedite, s katerimi kazalniki se bodo spremljali napredek in dosežki.

Komisija bo s podporo agencije ENISA in skupine za sodelovanje izvedla oceno kazalnikov, ki se bo začela tri leta po začetku veljavnosti novega pravnega akta o varnosti omrežij in informacijskih sistemov. Nekateri od kazalnikov spremljanja, na podlagi katerih se bo ocenila uspešnost pregleda direktive o varnosti omrežij in informacijskih sistemov, so:

• izboljšano obvladovanje incidentov: podjetja s sprejetjem ukrepov za kibernetsko varnost ne izboljšajo le svoje sposobnosti, da v celoti preprečijo nekatere incidente, ampak tudi svojo zmogljivost odzivanja na incidente. Merila uspešnosti so zato: (i) skrajšanje povprečnega časa, potrebnega za odkritje incidenta, (ii) čas, ki ga organizacije v povprečju potrebujejo za okrevanje po incidentu, in (iii) povprečni stroški škode, ki jo povzroči incident;

• večja ozaveščenost najvišjega vodstva podjetij o tveganjih za kibernetsko varnost: z zahtevo, da podjetja sprejmejo ukrepe, bi revidirana direktiva o varnosti omrežij in informacijskih sistemov prispevala k ozaveščanju najvišjega vodstva o tveganjih, povezanih s kibernetsko varnostjo. To se lahko izmeri s preučitvijo, v kakšnem obsegu podjetja, ki spadajo na področje uporabe okvira za varnost omrežij in informacijskih sistemov, pri notranjih politikah in postopkih dajejo prednost kibernetski varnosti, kot dokazujejo notranja dokumentacija, ustrezni programi usposabljanja ter dejavnosti ozaveščanja za zaposlene in dajanje prednosti naložbam v IKT, povezanim z varnostjo. Vodstvo vseh bistvenih in pomembnih subjektov bi moralo biti seznanjeno s pravili, določenimi v direktivi o varnosti omrežij in informacijskih sistemov;

• izravnava porabe po posameznih sektorjih: poraba za varnost IKT se med sektorji v EU zelo razlikuje. Z zahtevo, da podjetja v več sektorjih sprejmejo ukrepe, bi se morale razlike med sektorji in državami članicami v povprečni porabi za varnost IKT po posameznih sektorjih kot delež celotne porabe za IKT zmanjšati;

• močnejši pristojni organi in okrepljeno sodelovanje: z revidirano direktivo o varnosti omrežij in informacijskih sistemov bi bile pristojnim organom morebiti dodeljene dodatne naloge. To bi imelo merljiv učinek na finančne in človeške vire, namenjene agencijam za kibernetsko varnost na nacionalni ravni, pozitivno pa bi moralo vplivati tudi na zmogljivost pristojnih organov za proaktivno sodelovanje in s tem povečanje števila primerov, v katerih pristojni organi medsebojno sodelujejo pri obravnavanju čezmejnih incidentov ali izvajanju skupnih nadzornih dejavnosti;

• okrepljena izmenjava informacij: z revidirano direktivo o varnosti omrežij in informacijskih sistemov bi se izboljšala tudi izmenjava informacij med podjetji in pristojnimi organi. Eden od ciljev pregleda bi lahko bil povečanje števila subjektov, ki sodelujejo v različnih oblikah izmenjave informacij.

1.5. Utemeljitev predloga/pobude

1.5.1. Potrebe, ki jih je treba zadovoljiti kratkoročno ali dolgoročno, vključno s podrobno časovnico za uvajanje ustreznih ukrepov za izvajanje pobude

Cilj predloga je zvišati raven kibernetske odpornosti obsežne skupine podjetij, ki delujejo v Evropski uniji, v vseh ustreznih sektorjih, zmanjšati razlike v odpornosti na notranjem trgu v sektorjih, ki so že zajeti z Direktivo, in izboljšati raven skupnega situacijskega zavedanja in skupne zmogljivosti za pripravo in odzivanje. Temeljil bo na dosežkih pri izvajanju Direktive (EU) 2016/1148 v zadnjih štirih letih.

1.5.2. Dodana vrednost ukrepanja Unije (ki je lahko posledica različnih dejavnikov, npr. boljšega usklajevanja, pravne varnosti, večje učinkovitosti ali dopolnjevanja). Za namene te točke je

„dodana vrednost ukrepanja Unije“ vrednost, ki izhaja iz ukrepanja Unije in predstavlja dodatno vrednost poleg tiste, ki bi jo sicer ustvarile države članice same.

Kibernetska odpornost v Uniji ne more biti učinkovita, če se k njej zaradi nacionalnih ali regionalnih omejitev pristopa neenotno. V direktivi o varnosti omrežij in informacijskih sistemov so te pomanjkljivosti obravnavane z določitvijo okvira za varnost omrežij in informacijskih sistemov na nacionalni ravni in ravni Unije. Vendar je prvi redni pregled direktive o varnosti omrežij in informacijskih sistemov pokazal več pomanjkljivosti, ki so sčasoma privedle do precejšnjih razlik med državami članicami, kar zadeva zmogljivosti, načrtovanje in raven zaščite, ki hkrati vplivajo na enake konkurenčne pogoje podobnih podjetij na notranjem trgu.

Ukrepanje EU, ki presega sedanje ukrepe iz direktive o varnosti omrežij in informacijskih sistemov, je upravičeno zlasti zaradi: (i) čezmejne narave problematike; (ii) možnosti, da se z ukrepi EU izboljšajo in olajšajo učinkovite nacionalne politike, ter (iii) prispevka usklajenih in skupnih ukrepov politike na področju varnosti omrežij in informacijskih sistemov k učinkovitemu varstvu podatkov in zasebnosti.

Navedeni cilji se lahko tako bolje dosežejo z ukrepi na ravni EU kot na ravni držav članic.

1.5.3. Spoznanja iz podobnih izkušenj v preteklosti

Direktiva o varnosti omrežij in informacijskih sistemov je prvi horizontalni instrument notranjega trga, ki je namenjen povečanju odpornosti omrežij in sistemov v Uniji proti tveganjem za kibernetsko varnost. Od začetka veljavnosti leta 2016 je že veliko prispevala k zvišanju skupne ravni kibernetske varnosti v državah članicah. Vendar so se pri pregledu delovanja in izvajanja Direktive pokazale številne pomanjkljivosti, ki jih je treba poleg vse večje digitalizacije in potrebe po bolj posodobljenem odzivu obravnavati v revidiranem pravnem aktu.

1.5.4. Skladnost z večletnim finančnim okvirom in možne sinergije z drugimi ustreznimi instrumenti

Novi predlog je v celoti skladen in se ujema z drugimi povezanimi pobudami, kot sta predlog uredbe o digitalni operativni odpornosti za finančni sektor in predlog direktive o odpornosti kritičnih izvajalcev bistvenih storitev. Skladen je tudi z Evropskim zakonikom o elektronskih komunikacijah, Splošno uredbo o varstvu podatkov in uredbo eIDAS.

Predlog je bistveni del strategije EU za varnostno unijo.

1.5.5. Ocena različnih razpoložljivih možnosti financiranja, vključno z možnostmi za prerazporeditev

Upravljanje teh nalog s strani agencije ENISA zahteva posebne profile in dodatno delovno obremenitev, ki je ni mogoče prevzeti brez povečanja človeških virov.

1.6. Trajanje predloga/pobude in finančnih posledic

☐ **Časovno omejeno**

– ☐ od [DD. MM.] LLLL do [DD. MM.] LLLL,

– ☐ finančne posledice med letoma LLLL in LLLL

☒ **Časovno neomejeno**

– izvajanje z obdobjem uvajanja med letoma 2022 in 2025,

– ki mu sledi izvajanje v celoti.

1.7. Načrtovani načini upravljanja[57]

☒ **Neposredno upravljanje** – Komisija:

prek

– ☐ izvajalskih agencij.

☐ **Deljeno upravljanje** z državami članicami.

☐X **Posredno upravljanje**, tako da se naloge izvrševanja proračuna poverijo:

☐ mednarodnim organizacijam in njihovim agencijam (navedite),

☐ EIB in Evropskemu investicijskemu skladu,

☒ organom iz členov 70 in 71 finančne uredbe,

☐ subjektom javnega prava,

☐ subjektom zasebnega prava, ki opravljajo javne storitve, kolikor ti subjekti zagotavljajo ustrezna finančna jamstva,

☐ subjektom zasebnega prava države članice, ki so pooblaščeni za izvajanje javno-zasebnih partnerstev in ki zagotavljajo ustrezna finančna jamstva,

☐ osebam, pooblaščenim za izvajanje določenih ukrepov SZVP na podlagi naslova V PEU in opredeljenim v zadevnem temeljnem aktu.

Opombe

Agencija Evropske unije za kibernetsko varnost ENISA, ki ji je bil z Aktom o kibernetski varnosti podeljen nov trajni mandat, bi pomagala državam članicam in Komisiji pri izvajanju revidirane direktive o varnosti omrežij in informacijskih sistemov.

Na podlagi revidirane direktive o varnosti omrežij in informacijskih sistemov bo imela agencija ENISA od leta 2022/23 dodatna področja ukrepanja. Čeprav bodo ta področja ukrepanja zajeta s splošnimi nalogami agencije ENISA v skladu z njenim mandatom, bodo ustvarila dodatno delovno obremenitev za Agencijo. Natančneje, poleg sedanjih področij ukrepanja bo morala ENISA v skladu s predlogom Komisije za revidirano direktivo o varnosti omrežij in informacijskih sistemov v svoj delovni program posebej vključiti med drugim naslednje ukrepe: (i) razvoj in vzdrževanje evropskega registra šibkih točk (člen 6(2) predloga), (ii) zagotovitev sekretariata evropske organizacijske mreže za povezovanje v kibernetski krizi (EU-CyCLONe) (člen 14 predloga) in izdajo letnega poročila o stanju kibernetske

[57] Pojasnila o načinih upravljanja in sklici na finančno uredbo so na voljo na spletišču BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

varnosti v EU (člen 15 predloga), (iii) podpiranje organizacije medsebojnih strokovnih pregledov med državami članicami (člen 16 predloga), (iv) zbiranje zbirnih podatkov držav članic o incidentih in izdajo tehničnih smernic (člen 20(9) predloga), (v) vzpostavitev in vzdrževanje registra za subjekte, ki opravljajo čezmejne storitve (člen 25 predloga).

Zato se bo od leta 2022 zahtevalo dodatnih pet EPDČ z ustreznimi proračunskimi sredstvi v višini približno 0,61 milijona EUR na leto za pokrivanje teh novih delovnih mest.

2. UKREPI UPRAVLJANJA

2.1. Pravila o spremljanju in poročanju

Navedite pogostost in pogoje.

Komisija bo redno pregledovala delovanje Direktive ter poročala Evropskemu parlamentu in Svetu, prvič tri leta po začetku njene veljavnosti.

Ocenila bo tudi, ali so države članice pravilno prenesle Direktivo.

Pri spremljanju predloga in poročanju o njem se bodo upoštevala načela, opisana v trajnem mandatu agencije ENISA iz UREDBE (EU) 2019/881 (Akt o kibernetski varnosti).

Vire podatkov, uporabljene za načrtovano spremljanje, bodo večinoma zagotovili agencija ENISA, skupina za sodelovanje, mreža skupin CSIRT in organi držav članic. Poleg podatkov, zbranih iz poročil (vključno z letnimi poročili o dejavnostih) agencije ENISA, skupine za sodelovanje in mreže skupin CSIRT, bi se po potrebi lahko uporabila posebna orodja za zbiranje podatkov (npr. raziskave med nacionalnimi organi, raziskave Eurobarometer ter poročila v okviru kampanje meseca kibernetske varnosti in vseevropskih vaj).

2.2. Upravljavski in kontrolni sistemi

2.2.1. Utemeljitev načinov upravljanja, mehanizmov financiranja, načinov plačevanja in predlagane strategije kontrol

Izvajanje Direktive bo upravljala enota v okviru GD CNECT, pristojna za to področje politike.

Kar zadeva upravljanje agencije ENISA, člen 15 Akta o kibernetski varnosti vsebuje podroben seznam nadzornih funkcij upravnega odbora agencije ENISA.

V skladu s členom 31 Akta o kibernetski varnosti je izvršni direktor agencije ENISA odgovoren za izvrševanje proračuna agencije ENISA, notranji revizor Komisije pa ima glede agencije ENISA enaka pooblastila kot glede služb Komisije. Upravni odbor agencije ENISA izda mnenje o končnih zaključnih računih agencije ENISA.

2.2.2. Podatki o ugotovljenih tveganjih in vzpostavljenih sistemih notranjih kontrol za njihovo zmanjševanje

Zelo majhno tveganje, ker je ekosistem direktive o varnosti omrežij in informacijskih sistemov že vzpostavljen in že zajema agencijo ENISA, ki ima od začetka veljavnosti Akta o kibernetski varnosti leta 2019 trajni mandat.

2.2.3. Ocena in utemeljitev stroškovne učinkovitosti kontrol (razmerje „stroški kontrol ÷ vrednost z njimi povezanih upravljanih sredstev“) ter ocena pričakovane stopnje tveganja napake (ob plačilu in ob zaključku)

Zahtevano povečanje proračuna se nanaša na naslov 1 in je predvideno za financiranje plač. To pomeni zelo majhno tveganje napake na ravni plačil.

2.3. Ukrepi za preprečevanje goljufij in nepravilnosti

Navedite obstoječe ali načrtovane preprečevalne in zaščitne ukrepe, npr. iz strategije za boj proti goljufijam.

Uporabljali bi se preprečevalni in zaščitni ukrepi agencije ENISA, in sicer:

– plačila zahtevanih storitev ali študij pred izplačilom preveri osebje Agencije, pri čemer upošteva pogodbene obveznosti, gospodarska načela ter dobro finančno prakso in dobro prakso upravljanja. Določbe o preprečevanju goljufij (nadzor, zahteve glede poročanja itn.) se vključijo v vse sporazume in pogodbe, ki jih sklenejo Agencija in prejemniki plačil.

– za boj proti goljufijam, korupciji in drugim nezakonitim dejavnostim se brez omejitev uporabljajo določbe Uredbe (EU, Euratom) št. 883/2013 Evropskega parlamenta in Sveta z dne 25. maja 1999 o preiskavah, ki jih izvaja Evropski urad za boj proti goljufijam (OLAF);

– v skladu s členom 33 Akta o kibernetski varnosti agencija ENISA do 28. decembra 2019 pristopi k Medinstitucionalnemu sporazumu z dne 25. maja 1999 med Evropskim parlamentom, Svetom Evropske unije in Komisijo Evropskih skupnosti o notranjih preiskavah Evropskega urada za boj proti goljufijam (OLAF). Agencija ENISA nemudoma izda ustrezne predpise, ki se uporabljajo za vse zaposlene v Agenciji.

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

3.1. Zadevni razdelki večletnega finančnega okvira in odhodkovne proračunske vrstice

- Obstoječe proračunske vrstice

Po vrstnem redu razdelkov večletnega finančnega okvira in proračunskih vrstic.

Razdelek večletnega finančnega okvira	Proračunska vrstica	Vrsta odhodkov	Prispevek			
	številka	dif./nedif.[58]	držav Efte[59]	držav kandidatk[60]	tretjih držav	po členu 21(2)(b) finančne uredbe
2	02 10 04	nedif.	DA	NE	NE	NE

- Zahtevane nove proračunske vrstice

Po vrstnem redu razdelkov večletnega finančnega okvira in proračunskih vrstic.

Razdelek večletnega finančnega okvira	Proračunska vrstica	Vrsta odhodkov	Prispevek			
	številka	dif./nedif.	držav Efte	držav kandidatk	tretjih držav	po členu 21(2)(b) finančne uredbe

[58] Dif. = diferencirana sredstva/nedif. = nediferencirana sredstva.

[59] EFTA: Evropsko združenje za prosto trgovino.

[60] Države kandidatke in po potrebi potencialne države kandidatke z Zahodnega Balkana.

	[XX.YY.YY.YY]		DA/NE	DA/NE	DA/NE	DA/NE

3.2. Ocenjene posledice za odhodke

3.2.1. Povzetek ocenjenih posledic za odhodke

v mio. EUR (na tri decimalna mesta natančno)

Razdelek večletnega finančnega okvira	številka	[razdelek…2 Enotni trg, inovacije in digitalni sektor……...……]

[Organ]: <…agencija ENISA….>			Leto **N**[61] **2022**	Leto **N+1** **2023**	Leto **N+2** **2024**	Leto **N+3** **2025**	Vstavite ustrezno število let glede na trajanje posledic (glej točko 1.6) **2026**	**2027**		**SKUPAJ**
Naslov 1:	obveznosti	(1)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	plačila	(2)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
Naslov 2:	obveznosti	(1a)								
	plačila	(2a)								
Naslov 3:	obveznosti	(3a)								
	plačila	(3b)								
Odobritve za [organ] <ENISA…….> **SKUPAJ**	obveznosti	= 1 + 1 a + 3a	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	plačila	= 2 + 2a + 3b	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[61] Leto N je leto začetka izvajanja predloga/pobude. Nadomestite „N“ s pričakovanim prvim letom izvajanja (na primer: 2021). Enako storite za naslednja leta.

Razdelek večletnega finančnega okvira	**5**	„Upravni odhodki“

v mio. EUR (na tri decimalna mesta natančno)

		Leto **N**	Leto **N+1**	Leto **N+2**	Leto **N+3**	Vstavite ustrezno število let glede na trajanje posledic (glej točko 1.6)			**SKUPAJ**
GD: <…….>									
• Človeški viri									
• Drugi upravni odhodki									
GD <….> **SKUPAJ**	odobritve								

Odobritve iz RAZDELKA 5 večletnega finančnega okvira **SKUPAJ**	(obveznosti skupaj = plačila skupaj)								

v mio. EUR (na tri decimalna mesta natančno)

		Leto **N**[62] **2022**	Leto **N+1** **2023**	Leto **N+2** **2024**	Leto **N+3** **2025**	Vstavite ustrezno število let glede na trajanje posledic (glej točko 1.6) **2026**	**2027**		**SKUPAJ**
Odobritve iz RAZDELKOV 1 do 5 večletnega finančnega okvira **SKUPAJ**	obveznosti	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	plačila	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[62] Leto N je leto začetka izvajanja predloga/pobude. Nadomestite „N“ s pričakovanim prvim letom izvajanja (na primer: 2021). Enako storite za naslednja leta.

3.2.2. Ocenjene posledice za odobritve [organa]

– ☐x Za predlog/pobudo niso potrebne odobritve za poslovanje.

– ☐ Za predlog/pobudo so potrebne odobritve za poslovanje, kot je pojasnjeno v nadaljevanju:

odobritve za prevzem obveznosti v mio. EUR (na tri decimalna mesta natančno)

Cilji in realizacije			Leto **N**		Leto **N+1**		Leto **N+2**		Leto **N+3**		Vstavite ustrezno število let glede na trajanje posledic (glej točko 1.6)						**SKUPAJ**	
	REALIZACIJE																	
⇩	vrsta[63]	povprečni stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število realizacij skupaj	stroški realizacij skupaj
SPECIFIČNI CILJ št. 1[64] ...																		
– realizacija																		
– realizacija																		
– realizacija																		
Seštevek za specifični cilj št. 1																		
SPECIFIČNI CILJ št. 2 …																		
– realizacija																		
Seštevek za specifični cilj št. 2																		
STROŠKI SKUPAJ																		

63 Realizacije so dobavljeni proizvodi in opravljene storitve (npr. število financiranih izmenjav študentov, število kilometrov novozgrajenih cest …).

64 Kakor je opisan v točki 1.4.2 „Specifični cilji …“.

3.2.3. Ocenjene posledice za človeške vire agencije ENISA

3.2.3.1. Povzetek

Zaradi revidirane direktive o varnosti omrežij in informacijskih sistemov bo imela agencija ENISA od leta 2022/23 dodatne naloge. Čeprav bodo te naloge zajete z mandatom agencije ENISA, bodo za Agencijo pomenile dodatno delovno obremenitev. Natančneje, poleg sedanjih nalog bo imela agencija ENISA v skladu s predlogom Komisije za revidirano direktivo o varnosti omrežij in informacijskih sistemov med drugim naslednje naloge: (i) razvoj in vzdrževanje evropskega registra šibkih točk (člen 6(2)), (ii) zagotovitev sekretariata evropske organizacijske mreže za povezovanje v kibernetski krizi (CyCLONe) (člen 14) in izdaja letnega poročila o stanju kibernetske varnosti v EU (člen 15), (iii) podpiranje organizacije medsebojnih strokovnih pregledov med državami članicami (člen 16), (iv) zbiranje zbirnih podatkov držav članic o incidentih in izdaja tehničnih smernic (člen 20(9)) ter (v) vzpostavitev in vzdrževanje registra za subjekte, ki opravljajo čezmejne storitve (člen 25).

Zato se bo od leta 2022 zahtevalo dodatnih pet EPDČ z ustreznimi proračunskimi sredstvi za pokrivanje teh novih delovnih mest.

– ☐ Za predlog/pobudo niso potrebne odobritve za upravne zadeve.

– ☐X Za predlog/pobudo so potrebne odobritve za upravne zadeve, kot je pojasnjeno v nadaljevanju:

v mio. EUR (na tri decimalna mesta natančno)

	Leto **N** [65] **2022**	Leto **N+1** **2023**	Leto **N+2** **2024**	Leto **N+3** **2025**	Vstavite ustrezno število let glede na trajanje posledic (glej točko 1.6) **2026**	**2027**		**SKUPAJ**
Začasni uslužbenci (razredi AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Začasni uslužbenci (razredi AST)								
Pogodbeni uslužbenci	0,160	0,160	0,160	0,160	0,160	0,160		**0,96**
Napoteni nacionalni strokovnjaki								
SKUPAJ	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

[65] Leto N je leto začetka izvajanja predloga/pobude. Nadomestite „N“ s pričakovanim prvim letom izvajanja (na primer: 2021). Enako storite za naslednja leta.

Potrebe po uslužbencih (EPDČ):

	Leto **N [66]** **2022**	Leto **N+1** **2023**	Leto **N+2** **2024**	Leto **N+3** **2025**	Vstavite ustrezno število let glede na trajanje posledic (glej točko 1.6) **2026** **2027**			**SKUPAJ**
Začasni uslužbenci (razredi AD)	3	3	3	3	3	3		**18**
Začasni uslužbenci (razredi AST)								
Pogodbeni uslužbenci	2	2	2	2	2	2		**12**
Napoteni nacionalni strokovnjaki								
SKUPAJ	**5**	**5**	**5**	**5**	**5**	**5**		**30**

3.2.3.2. Ocenjene potrebe po človeških virih za matični GD

– ☐ Za predlog/pobudo niso potrebni človeški viri.

– ☐ Za predlog/pobudo so potrebni človeški viri, kot je pojasnjeno v nadaljevanju:

ocena, izražena v celih številkah (ali na največ eno decimalno mesto natančno)

	Leto **N**	Leto **N+1**	Leto **N+2**	Leto **N+3**	Vstavite ustrezno število let glede na trajanje posledic (glej točko 1.6)		
• **Delovna mesta v skladu s kadrovskim načrtom (uradniki in začasni uslužbenci)**							
XX 01 01 01 (sedež in predstavništva Komisije)							
XX 01 01 02 (delegacije)							
XX 01 05 01 (posredne raziskave)							
10 01 05 01 (neposredne raziskave)							
• **Zunanji sodelavci (v ekvivalentu polnega delovnega časa: EPDČ)[67]**							

66 Leto N je leto začetka izvajanja predloga/pobude. Nadomestite „N“ s pričakovanim prvim letom izvajanja (na primer: 2021). Enako storite za naslednja leta.

67 PU = pogodbeni uslužbenec; LU = lokalni uslužbenec; NNS = napoteni nacionalni strokovnjak; ZU = začasni uslužbenec; MSD = mladi strokovnjak na delegaciji.

XX 01 02 01 (PU, NNS, ZU iz splošnih sredstev)								
XX 01 02 02 (PU, LU, NNS, ZU in MSD na delegacijah)								
XX 01 04 ***yy***[68]	– na sedežu[69]							
	– na delegacijah							
XX 01 05 02 (PU, NNS, ZU za posredne raziskave)								
10 01 05 02 (PU, NNS, ZU za neposredne raziskave)								
Druge proračunske vrstice (navedite)								
SKUPAJ								

XX je zadevno področje ali naslov v proračunu.

Potrebe po človeških virih se krijejo z osebjem GD, ki je že dodeljeno za upravljanje ukrepa in/ali je bilo prerazporejeno znotraj GD, po potrebi skupaj z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v postopku letne dodelitve virov glede na proračunske omejitve.

Opis nalog:

Uradniki in začasni uslužbenci	
Zunanji sodelavci	

Opis izračuna stroškov za enote EPDČ bi moral biti vključen v oddelek 3 Priloge V.

[68] Dodatna zgornja meja za zunanje sodelavce v okviru odobritev za poslovanje (prej vrstice BA).

[69] Zlasti za strukturna sklada, Evropski kmetijski sklad za razvoj podeželja (EKSRP) in Evropski sklad za ribištvo (ESR).

3.2.4. Skladnost z veljavnim večletnim finančnim okvirom

– ☐X Predlog/pobuda je v skladu z veljavnim večletnim finančnim okvirom.

– ☐ Za predlog/pobudo je potrebna sprememba zadevnega razdelka večletnega finančnega okvira.

Pojasnite zahtevano spremembo ter navedite zadevne proračunske vrstice in ustrezne zneske. Predlog je v skladu z večletnim finančnim okvirom za obdobje 2021–2027. Izravnava proračuna, ki se zahteva za kritje povečanja človeških virov v agenciji ENISA, bo izvedena z zmanjšanjem proračuna za program za digitalno Evropo v istem razdelku za enak znesek.

– ☐ Za predlog/pobudo je potrebna uporaba instrumenta prilagodljivosti ali sprememba večletnega finančnega okvira[70].

Pojasnite te zahteve ter navedite zadevne razdelke in proračunske vrstice ter ustrezne zneske.

3.2.5. Udeležba tretjih oseb pri financiranju

– V predlogu/pobudi ni načrtovano sofinanciranje tretjih oseb.

– V predlogu/pobudi je načrtovano sofinanciranje, kot je ocenjeno v nadaljevanju:

v mio. EUR (na tri decimalna mesta natančno)

	Leto **N**	Leto **N+1**	Leto **N+2**	Leto **N+3**	Vstavite ustrezno število let glede na trajanje posledic (glej točko 1.6)			Skupaj
Navedite organ, ki bo sofinanciral predlog/pobudo								
Sofinancirane odobritve SKUPAJ								

[70] Glej člena 11 in 17 Uredbe Sveta (EU, Euratom) št. 1311/2013 o večletnem finančnem okviru za obdobje 2014–2020.

3.3. Ocenjene posledice za prihodke

– ☐ Predlog/pobuda nima finančnih posledic za prihodke.

– ☐ Predlog/pobuda ima finančne posledice, kot je pojasnjeno v nadaljevanju:

☐ za lastna sredstva,

☐ za druge prihodke,

☐ navedite, ali so prihodki dodeljeni za odhodkovne vrstice.

v mio. EUR (na tri decimalna mesta natančno)

Prihodkovna proračunska vrstica	Odobritve na voljo za tekoče proračunsko leto	Posledice predloga/pobude[71]						
		Leto **N**	Leto **N+1**	Leto **N+2**	Leto **N+3**	Vstavite ustrezno število let glede na trajanje posledic (glej točko 1.6)		
Člen …….								

Za razne namenske prejemke navedite zadevne odhodkovne proračunske vrstice.

Navedite metodo za izračun posledic za prihodke.

[71] Pri tradicionalnih lastnih sredstvih (carine, prelevmani na sladkor) se navedejo neto zneski, tj. bruto zneski po odbitku 20 % stroškov pobiranja.