DIREKTIVE

DIREKTIVA (EU) 2022/2555 EVROPSKEGA PARLAMENTA IN SVETA

z dne 14. decembra 2022

o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2)

(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 Evropske centralne banke ([1]),

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora ([2]),

po posvetovanju z Odborom regij,

v skladu z rednim zakonodajnim postopkom ([3]),

ob upoštevanju naslednjega:

(1) Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta ([4]) 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 z incidenti, s čimer naj bi prispevala k varnosti Unije ter učinkovitemu delovanju njenega gospodarstva in družbe.

(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. Navedena direktiva je zagotovila dokončanje nacionalnih okvirov za varnost omrežij in informacijskih sistemov z vzpostavitvijo nacionalnih strategij za varnost omrežij in informacijskih sistemov ter z vzpostavitvijo nacionalnih zmogljivosti in izvajanjem regulativnih ukrepov, ki so zajemali bistvene infrastrukture in subjekte, ki jih je določila vsaka država članica. Direktiva (EU) 2016/1148 je prispevala tudi k sodelovanju na ravni Unije z ustanovitvijo skupine za sodelovanje in mreže nacionalnih skupin za odzivanje na incidente na področju računalniške varnosti. Kljub tem dosežkom pa so bile pri pregledu Direktive (EU) 2016/1148 razkrite pomanjkljivosti, zaradi katerih z navedeno direktivo ni mogoče učinkovito obravnavati sedanjih in nastajajočih izzivov na področju kibernetske varnosti.

(3) Omrežni 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 splošne kibernetske ogroženosti, s čimer so se pojavili novi izzivi, ki zahtevajo prilagojene, usklajene in inovativne odzive v vseh državah članicah. Število, obseg, izpopolnjenost, pogostost in vpliv incidentov so vse večji ter pomenijo večjo grožnjo delovanju omrežnih in informacijskih sistemov. Posledično lahko incidenti ovirajo gospodarske dejavnosti na notranjem trgu, ustvarjajo finančno izgubo, slabijo zaupanje uporabnikov ter povzročajo

([1]) UL C 233, 16.6.2022, str. 22.
([2]) UL C 286, 16.7.2021, str. 170.
([3]) Stališče Evropskega parlamenta z dne 10. novembra 2022 (še ni objavljeno v Uradnem listu) in odločitev Sveta z dne 28. novembra 2022.
([4]) 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).

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. Poleg tega je kibernetska varnost eden od glavnih dejavnikov, ki številnim ključnim sektorjem omogočajo, da se uspešno podajo na pot digitalne preobrazbe ter v celoti izkoristijo gospodarske, družbene in trajnostne prednosti digitalizacije.

(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 izvajajo dejavnosti, ki so gospodarsko pomembne, 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 subjekte, ki blago ali storitve ponujajo čez meje. 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 neustreznega oblikovanja ali izvajanja zahtev glede kibernetske varnosti v eni državi članici verjetno vplivala na raven kibernetske varnosti drugih držav članic, zlasti glede na intenzivnost čezmejnih izmenjav. 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 izvajale na zelo različne načine. Podobne razlike obstajajo pri izvajanju določb Direktive (EU) 2016/1148 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 ukrepov. Navsezadnje bi lahko te razlike privedle do večje ranljivosti nekaterih držav članic za kibernetske grožnje, kar bi lahko povzročilo učinke prelivanja po vsej Uniji. Cilj te direktive je odpraviti tovrstne velike razlike med državami članicami, zlasti z določitvijo minimalnih pravil v zvezi z delovanjem usklajenega regulativnega okvira, določitvijo mehanizmov za učinkovito sodelovanje med pristojnimi organi v vsaki državi članici, posodobitvijo seznama sektorjev in dejavnosti, za katere veljajo obveznosti glede kibernetske varnosti, ter določitvijo učinkovitih pravnih sredstev in izvršilnih ukrepov, ki so ključni za učinkovito izvrševanje teh obveznosti. Zato bi bilo treba Direktivo (EU) 2016/1148 razveljaviti in nadomestiti s to direktivo.

(6) Z razveljavitvijo Direktive (EU) 2016/1148 bi bilo treba področje uporabe po sektorjih razširiti na večji del gospodarstva, da bi se zagotovila celovita pokritost sektorjev in storitev, ki so bistvenega pomena za ključne družbene in gospodarske dejavnosti na notranjem trgu. Cilj te direktive je zlasti odpraviti pomanjkljivosti razlikovanja med izvajalci bistvenih storitev in ponudniki digitalnih storitev, ki se je izkazalo za zastarelo, saj ne odraža pomena sektorjev ali storitev za družbene in gospodarske dejavnosti na notranjem trgu.

(7) Na podlagi Direktive (EU) 2016/1148 so bile države članice odgovorne za določitev subjektov, ki izpolnjujejo merila, na podlagi katerih se štejejo za izvajalce bistvenih storitev. Za odpravo velikih razlik med državami članicami v zvezi s tem in zagotovitev pravne varnosti v zvezi z ukrepi kibernetske varnosti za obvladovanje tveganja in obveznosti poročanja za vse ustrezne subjekte bi bilo treba določiti enotno merilo, ki bi določalo, kateri subjekti spadajo na področje uporabe te direktive. To merilo bi moralo vključevati uporabo pravila omejitve velikosti, v skladu s katerim na področje uporabe te direktive spadajo vsi subjekti, ki se na podlagi člena 2 Priloge k Priporočilu Komisije 2003/361/ES ([5]) štejejo za srednja podjetja, ali presegajo zgornje meje za srednja podjetja iz odstavka 1 navedenega člena, in ki delujejo v sektorjih in opravljajo vrste storitev ali izvajajo dejavnosti, zajete s to

([5]) 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).

direktivo. Države članice bi morale tudi zagotoviti, da na področje uporabe te direktive spadajo nekatera mala podjetja in mikropodjetja, kot so opredeljena v členu 2(2) in (3) navedene priloge, ki izpolnjujejo posebna merila, ki kažejo na ključno vlogo za družbo, gospodarstvo ali za določene sektorje ali vrste storitev.

(8) Izključitev subjektov javne uprave s področja uporabe te direktive bi morala veljati za subjekte, katerih dejavnosti se večinoma izvajajo na področjih nacionalne varnosti, javne varnosti, obrambe ali kazenskega pregona, vključno s preprečevanjem, preiskovanjem, odkrivanjem in pregonom kaznivih dejanj. Vendar subjekti javne uprave, katerih dejavnosti so le obrobno povezane s temi področji, ne bi smeli biti izključeni s področja uporabe te direktive. Za namene te direktive se za subjekte z regulativno pristojnostjo ne šteje, da opravljajo dejavnosti na področju kazenskega pregona, in zato iz tega razloga niso izključeni s področja uporabe te direktive. Subjekti javne uprave, ki so ustanovljeni skupaj s tretjo državo v skladu z mednarodnim sporazumom, so izključeni s področja uporabe te direktive. Ta direktiva se ne uporablja za diplomatska in konzularna predstavništva držav članic v tretjih državah ali za njihove omrežne in informacijske sisteme, če so ti sistemi v prostorih predstavništva ali če delujejo za uporabnike v tretji državi.

(9) Države članice bi morale imeti možnost, da sprejmejo potrebne ukrepe, s katerimi zaščitijo bistvene interese nacionalne varnosti, javni red in javno varnost ter omogočijo preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj. V ta namen bi morale imeti države članice možnost, da posebne subjekte, ki izvajajo dejavnosti na področjih nacionalne varnosti, javne varnosti, obrambe ali kazenskega pregona, vključno s preprečevanjem, preiskovanjem, odkrivanjem in pregonom kaznivih dejanj, izvzamejo iz določenih obveznosti iz te direktive v zvezi s temi dejavnostmi. Kadar subjekt opravlja storitve izključno za subjekt javne uprave, ki je izključen s področja uporabe te direktive, bi morale imeti države članice možnost, da ta subjekt izvzamejo iz določenih obveznosti iz te direktive v zvezi s temi storitvami. Poleg tega se od nobene države članice ne bi smelo zahtevati, da daje informacije, katerih razkritje bi bilo v nasprotju z bistvenimi interesi njene nacionalne varnosti, javne varnosti ali obrambe. V tem okviru bi bilo potrebno upoštevati pravila Unije ali nacionalna pravila za varovanje tajnih podatkov, sporazume o nerazkritju informacij in neuradne sporazume o nerazkritju informacij, kot je semaforski protokol (*Traffic Light Protocol*). Semaforski protokol je treba razumeti kot sredstvo za zagotavljanje informacij o kakršnih koli omejitvah v zvezi z nadaljnjim širjenjem informacij. Uporablja se v skoraj vseh skupinah za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT) ter v nekaterih centrih za analizo in izmenjavo informacij.

(10) Čeprav se ta direktiva uporablja za subjekte, ki opravljajo dejavnosti na področju proizvodnje električne energije v jedrskih elektrarnah, so nekatere od teh dejavnosti lahko povezane z nacionalno varnostjo. V primeru, da je temu tako, bi morala imeti država članica možnost, da uveljavlja svojo odgovornost za zaščito svoje nacionalne varnosti v zvezi s temi dejavnostmi, vključno z dejavnostmi znotraj jedrske vrednostne verige, v skladu s Pogodbama.

(11) Nekateri subjekti izvajajo dejavnosti na področju nacionalne varnosti, javne varnosti, obrambe ali kazenskega pregona, vključno s preprečevanjem, preiskovanjem, odkrivanjem in pregonom kaznivih dejanj, hkrati pa zagotavljajo storitve zaupanja. Ponudniki storitev zaupanja, ki spadajo na področje uporabe Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta ([6]), bi morali spadati na področje uporabe te direktive, da se zagotovi enaka raven varnostnih zahtev in nadzora, kot je bila poprej v zvezi s ponudniki storitev zaupanja predpisana v navedeni uredbi. Skladno z izključitvijo nekaterih posebnih storitev iz Uredbe (EU) št. 910/2014 se ta uredba ne bi smela uporabljati za zagotavljanje storitev zaupanja, ki se uporabljajo izključno znotraj zaprtih sistemov, ki obstajajo na podlagi nacionalnega prava ali sporazumov med določeno skupino udeležencev.

([6]) 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).

(12) Ponudniki poštnih storitev, kot so opredeljeni v Direktivi 97/67/ES Evropskega parlamenta in Sveta ([7]), vključno s ponudniki kurirskih storitev, bi morali biti predmet te direktive, če zagotavljajo vsaj en korak v verigi poštne dostave, zlasti sprejem, usmerjanje, prevoz ali dostavo poštnih pošiljk, vključno s storitvami prevzema, ob upoštevanju stopnje njihove odvisnosti od omrežnih in informacijskih sistemov. Storitve prenosa, ki se ne izvajajo v povezavi z enim od teh korakov, bi bilo treba izključiti iz obsega poštnih storitev.

(13) Glede na okrepitev in večjo izpopolnjenost kibernetskih groženj bi si morale države članice prizadevati zagotoviti, da subjekti, ki so izključeni s področja uporabe te direktive, dosežejo visoko raven kibernetske varnosti, in podpirati izvajanje enakovrednih ukrepov za obvladovanje tveganj za kibernetsko varnost, ki odražajo občutljivo naravo teh subjektov.

(14) Pravo Unije o varstvu podatkov in pravo Unije o zasebnosti se uporablja za vsakršno obdelavo osebnih podatkov na podlagi te direktive. Ta direktiva zlasti ne posega v Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta ([8]) ter Direktivo 2002/58/ES Evropskega parlamenta in Sveta ([9]). Ta direktiva zato med drugim ne bi smela vplivati na naloge in pooblastila organov, pristojnih za spremljanje skladnosti z veljavnim pravom Unije o varstvu podatkov in pravom Unije o zasebnosti.

(15) Subjekti, ki spadajo na področje uporabe te direktive za namene izpolnjevanja ukrepov za obvladovanje tveganj za kibernetsko varnost in obveznosti poročanja, bi morali biti razvrščeni v dve kategoriji, in sicer bistvene in pomembne subjekte, ki bi odražali, v kolikšni meri so kritični glede na sektor ali vrsto storitev, ki jih zagotavljajo, ter na njihovo velikost. V zvezi s tem bi bilo treba po potrebi ustrezno upoštevati vse ustrezne sektorske ocene tveganja ali usmeritve pristojnih organov. Pri teh dveh kategorijah subjektov bi bilo treba razlikovati med ureditvijo nadzora in ureditvijo izvrševanja, da bi se zagotovilo ustrezno ravnovesje med zahtevami na podlagi tveganj in obveznostmi na eni strani ter upravnim bremenom, ki izhaja iz nadzora nad izpolnjevanjem zahtev in obveznosti, na drugi strani.

(16) Da bi se preprečilo, da bi se subjekti, ki imajo partnerska podjetja ali so povezana podjetja, šteli za bistvene ali pomembne subjekte, kadar bi bilo to nesorazmerno, lahko države članice pri uporabi člena 6(2) Priloge k Priporočilu 2003/361/ES upoštevajo stopnjo neodvisnosti, ki jo ima subjekt v razmerju do svojih partnerskih ali povezanih podjetij. Države članice lahko zlasti upoštevajo, da je subjekt neodvisen od svojega partnerja ali povezanih podjetij, kar zadeva omrežne in informacijske sisteme, ki jih ta subjekt uporablja pri opravljanju svojih storitev, in storitev, ki jih subjekt opravlja. Na podlagi tega lahko države članice po potrebi štejejo, da tak subjekt ne izpolnjuje pogojev za srednje podjetje na podlagi člena 2 Priloge k Priporočilu 2003/361/ES ali ne presega zgornjih mej za srednje podjetje iz odstavka 1 navedenega člena, če bi se ob upoštevanju stopnje neodvisnosti tega subjekta zanj štelo, da ne izpolnjuje pogojev za srednje podjetje ali da presega navedene zgornje meje, če bi se upoštevali samo njegovi podatki. To ne vpliva na obveznosti iz te direktive za partnerska in povezana podjetja, ki spadajo na področje uporabe te direktive.

(17) Države članice bi morale imeti možnost, da se odločijo, da se subjekti, ki so bili pred začetkom veljavnosti te direktive določeni kot izvajalci bistvenih storitev v skladu z Direktivo (EU) 2016/1148, štejejo za bistvene subjekte.

([7]) 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).

([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).

([9]) 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).

(18) Za zagotovitev jasnega pregleda subjektov, ki spadajo na področje uporabe te direktive, bi morale države članice oblikovati seznam bistvenih in pomembnih subjektov, kot tudi subjektov, ki opravljajo storitve registracije domenskih imen. V ta namen bi morale države članice od subjektov zahtevati, da pristojnim organom predložijo vsaj naslednje informacije, in sicer ime, naslov in ažurne kontaktne podatke, vključno z naslovi elektronske pošte, bloki naslovov IP in telefonskimi številkami subjekta, ustrezni sektor in podsektor iz prilog, kadar je to primerno, po potrebi pa tudi seznam držav članic, v katerih opravljajo storitve, ki spadajo na področje uporabe te direktive. V ta namen bi morala Komisija ob pomoči Agencije Evropske unije za kibernetsko varnost (ENISA) brez nepotrebnega odlašanja sprejeti smernice in obrazce v zvezi z obveznostjo predložitve informacij. Za lažje oblikovanje in posodabljanje seznama bistvenih in pomembnih subjektov, kot tudi subjektov, ki opravljajo storitve registracije domenskih imen, bi morale imeti države članice možnost, da vzpostavijo nacionalne mehanizme za registracijo subjektov. Če obstajajo registri na nacionalni ravni, se lahko države članice odločijo o ustreznih mehanizmih, ki omogočajo identifikacijo subjektov, ki spadajo na področje uporabe te direktive.

(19) Države članice bi morale biti odgovorne, da Komisiji predložijo vsaj število bistvenih in pomembnih subjektov za vsak sektor in podsektor iz prilog ter ustrezne informacije o številu identificiranih subjektov in določbi iz te direktive, na podlagi katere so bili identificirani, ter o vrsti storitve, ki jo zagotavljajo. Države članice se spodbuja, da si s Komisijo izmenjujejo informacije o bistvenih in pomembnih subjektih ter v primeru kibernetskega incidenta velikih razsežnosti ustrezne informacije, kot je ime zadevnega subjekta.

(20) Komisija bi morala v sodelovanju s skupino za sodelovanje in po posvetovanju z ustreznimi deležniki določiti smernice o izvajanju meril, ki se uporabljajo za ocenjevanje, ali mikropodjetja in mala podjetja spadajo na področje uporabe te direktive. Komisija bi morala pripraviti tudi ustrezne smernice za vsa mikropodjetja in mala podjetja, ki spadajo na področje uporabe ta direktive. Komisija bi morala ob pomoči držav članic mikropodjetjem in malim podjetjem dati na voljo informacije v zvezi s tem.

(21) Komisija bi lahko zagotovila navodila, da bi državam članicam pomagala pri izvajanju določb te direktive glede področja uporabe in pri oceni sorazmernosti ukrepov, ki se sprejmejo na podlagi te direktive, zlasti za subjekte z zapletenimi poslovnimi modeli ali delovnimi okolji, pri čemer lahko subjekt hkrati izpolnjuje merila, dodeljena tako bistvenim kot pomembnim subjektom, ali hkrati izvaja dejavnosti, od katerih nekatere spadajo na področje uporabe te direktive, druge pa so z njega izključene.

(22) Ta direktiva določa izhodišče za ukrepe za obvladovanje tveganj za kibernetsko varnost in obveznosti poročanja v sektorjih, ki spadajo na njeno področje uporabe. Da bi se preprečila razdrobljenost določb pravnih aktov Unije o kibernetski varnosti, bi morala Komisija, kadar se šteje, da so za zagotavljanje visoke ravni kibernetske varnosti po vsej Uniji potrebni nadaljnji sektorski pravni akti Unije glede ukrepov za obvladovanje tveganj za kibernetsko varnost in obveznosti poročanja, oceniti, ali bi se takšne nadaljnje določbe lahko določile v izvedbenem aktu na podlagi te direktive. Če takšen izvedbeni akt ne bi bil primeren za to, bi sektorski pravni akti Unije lahko prispevali k zagotavljanju visoke ravni kibernetske varnosti po vsej Uniji, ob polnem upoštevanju posebnosti in kompleksnosti zadevnih sektorjev. Zato ta direktiva ne izključuje sprejetja nadaljnjih sektorskih pravnih aktov Unije, ki bi obravnavali ukrepe za obvladovanje tveganj za kibernetsko varnost in obveznosti poročanja ter pri katerih bi se ustrezno upoštevala potrebo po celovitem in doslednem okviru za kibernetsko varnost. Ta direktiva ne posega v obstoječa izvedbena pooblastila, ki so bila podeljena Komisiji v številnih sektorjih, vključno s prometom in energetiko.

(23) Kadar sektorski pravni akti Unije vsebuje določbe, ki zahtevajo, da bistveni ali pomembni subjekti sprejmejo ukrepe za obvladovanje tveganj za kibernetsko varnost ali da priglasijo pomembne incidente, in kadar so takšne zahteve po učinku vsaj enakovredne obveznostim iz te direktive, bi se morale te določbe, tudi tiste o nadzoru in izvrševanju,

uporabljati za take subjekte. Če sektorski pravni akt Unije ne zajema vseh subjektov v določenem sektorju, ki spadajo na področje uporabe te direktive, bi se morale ustrezne določbe te direktive še naprej uporabljati za subjekte, ki jih ta akt ne zajema.

(24) Kadar določbe sektorskega pravnega akta Unije od bistvenih ali pomembnih subjektov zahtevajo, da izpolnjujejo obveznosti poročanja, ki imajo vsaj enakovreden učinek kot obveznosti poročanja iz te direktive, bi bilo treba zagotoviti skladnost in učinkovitost pri obravnavi priglasitev incidentov. V ta namen bi morale določbe sektorskega pravnega akta Unije v zvezi s priglasitvijo incidentov skupinam CSIRT, pristojnim organom ali enotnim kontaktnim točkam za kibernetsko varnost (v nadaljnjem besedilu: enotna kontaktna točka) na podlagi te direktive zagotavljati takojšen dostop do priglasitev incidentov, ki se predložijo v skladu s sektorskim pravnim aktom Unije. Tak takojšen dostop se lahko zagotovi zlasti, če se priglasitve incidentov brez nepotrebnega odlašanja posredujejo skupini CSIRT, pristojnemu organu ali enotni kontaktni točki iz te direktive. Države članice bi morale po potrebi vzpostaviti mehanizem samodejnega in neposrednega poročanja, ki bi v zvezi z obravnavo takih priglasitev incidentov zagotavljal sistematično in takojšnjo izmenjavo informacij s skupinami CSIRT, pristojnimi organi ali enotno kontaktno točko. Za namene poenostavitve poročanja in izvajanja mehanizma samodejnega in neposrednega poročanja bi lahko države članice v skladu s sektorskim pravnim aktom Unije uporabile enotno vstopno točko.

(25) V sektorskih pravnih aktih Unije, ki predpisujejo ukrepe za obvladovanje tveganj za kibernetsko varnost ali obveznosti poročanja, ki so po učinku vsaj enakovredni tistim iz te direktive, bi se lahko določilo, da pristojni organi iz tovrstnih aktov izvajajo svoja nadzorna in izvršilna pooblastila v zvezi s takšnimi ukrepi ali obveznostmi s pomočjo pristojnih organov iz te direktive. Zadevni pristojni organi bi lahko v ta namen sklenili dogovore o sodelovanju. V takšnih dogovorih o sodelovanju bi se lahko med drugim določili postopki za usklajevanje nadzornih dejavnosti, vključno s postopki preiskav in inšpekcijskih pregledov na kraju samem v skladu z nacionalnim pravom, ter mehanizem za izmenjavo relevantnih informacij o nadzoru in izvrševanju med pristojnimi organi, vključno z dostopom do informacij v zvezi s kibernetsko varnostjo, ki jih zahtevajo pristojni organi iz te direktive.

(26) Kadar se v sektorskih pravnih aktih Unije od subjektov zahteva ali se jih spodbuja, da priglasijo pomembne kibernetske grožnje, bi morale države članice spodbujati tudi izmenjavo pomembnih kibernetskih groženj s skupinami CSIRT, pristojnimi organi ali enotnimi kontaktnimi točkami na podlagi te direktive, da bi se zagotovila višja raven ozaveščenosti teh organov o splošni kibernetski ogroženosti ter se jim omogočil učinkovit in pravočasen odziv, če bi se pomembne kibernetske grožnje uresničile.

(27) V nadaljnjih sektorskih pravnih aktih Unije bi se morali ustrezno upoštevati opredelitve ter nadzorni in izvršilni okvir iz te direktive.

(28) Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta ([10]) bi se morala šteti za sektorski pravni akt Unije v zvezi s to direktivo, kar zadeva finančne subjekte. Določbe Uredbe (EU) 2022/2554 v zvezi z ukrepi za obvladovanje tveganj na področju informacijske in komunikacijske tehnologije (IKT), obvladovanjem incidentov, povezanih z IKT, in zlasti poročanjem o večjih incidentih, povezanih z IKT, kot tudi testiranjem digitalne operativne odpornosti, dogovori o izmenjavi informacij in tveganjem tretjih oseb na področju IKT bi se morale uporabljati namesto določb te direktive. Države članice zato ne bi smele uporabljati določb te direktive o obvladovanju tveganj za kibernetsko varnost in obveznostih poročanja ter nadzoru in izvrševanju za finančne subjekte, zajete z Uredbo (EU) 2022/2554. Hkrati je pomembno ohranjati tesno povezavo in izmenjavo informacij s finančnim sektorjem na podlagi te direktive. V ta namen Uredba (EU) 2022/2554 evropskim nadzornim organom in pristojnim organom iz navedene uredbe omogoča, da sodelujejo pri dejavnostih skupine za sodelovanje ter si izmenjujejo informacije in sodelujejo z enotnimi kontaktnimi točkami, kot tudi s skupinami CSIRT in pristojnimi organi iz te direktive. Pristojni organi iz Uredbe (EU) 2022/2554 bi morali podrobnosti o večjih incidentih, povezanih z IKT, in po potrebi pomembnih

([10]) Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti v finančnem sektorju in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 (glej stran 1 tega Uradnega lista).

kibernetskih grožnjah posredovati tudi skupinam CSIRT**,** pristojnim organom ali enotnim kontaktnim točkam iz te direktive. To je mogoče doseči z zagotovitvijo takojšnjega dostopa do priglasitev incidentov in njihovega posredovanja neposredno ali prek enotne vstopne točke. Poleg tega bi morale države članice še naprej vključevati finančni sektor v svoje strategije za kibernetsko varnost, skupine CSIRT pa lahko vključijo finančni sektor v svoje dejavnosti.

(29) V izogib vrzelim ali podvajanju obveznosti glede kibernetske varnosti, ki veljajo za subjekte v letalskem sektorju, bi morali nacionalni organi iz uredb (ES) št. 300/2008 ([11]) in (EU) 2018/1139 ([12]) Evropskega parlamenta in Sveta ter pristojni organi iz te direktive sodelovati pri izvajanju ukrepov za obvladovanje tveganj za kibernetsko varnost in nadzoru spoštovanja teh ukrepov na nacionalni ravni. Pristojni organi iz te direktive bi lahko skladnost subjekta z varnostnimi zahtevami iz uredb (ES) št. 300/2008 in (EU) 2018/1139 ter iz ustreznih delegiranih in izvedbenih aktov, sprejetih na podlagi navedenih uredb, šteli za skladnost z ustreznimi zahtevami iz te direktive.

(30) Glede na medsebojne povezave med kibernetsko varnostjo in fizično varnostjo subjektov bi bilo treba zagotoviti skladen pristop med Direktivo (EU) 2022/2557 Evropskega parlamenta in Sveta ([13]) in to direktivo. Za dosego tega bi se morali subjekti, ki so identificirani kot kritični na podlagi Direktive (EU) 2022/2557, šteti za bistvene subjekte iz te direktive. Poleg tega bi morala vsaka država članica zagotoviti, da njena nacionalna strategija za kibernetsko varnost določa okvir politike za okrepljeno usklajevanje v tej državi članici med njenimi pristojnimi organi iz te direktive in pristojnimi organi iz Direktive (EU) 2022/2557 v okviru izmenjave informacij o tveganjih, kibernetskih grožnjah in incidentih, pa tudi o nekibernetskih tveganjih, grožnjah in incidentih, ter izvajanja nadzornih nalog. Pristojni organi iz te direktive in pristojni organi iz Direktive (EU) 2022/2557 bi morali sodelovati in si brez nepotrebnega odlašanja izmenjevati informacije, zlasti v zvezi z identifikacijo kritičnih subjektov, tveganji, kibernetskimi grožnjami in incidenti, pa tudi v zvezi z nekibernetskimi tveganji, grožnjami in incidenti, ki vplivajo na kritične subjekte, vključno z ukrepi za kibernetsko varnost in fizičnimi ukrepi, ki jih sprejmejo kritični subjekti, kot tudi rezultati nadzornih dejavnosti, opravljenih v zvezi s takšnimi subjekti.

Poleg tega bi si morali pristojni organi za racionalizacijo nadzornih dejavnosti med pristojnimi organi iz te direktive in pristojni organi iz Direktive (EU) 2022/2557 in za zmanjšanje upravnega bremena za zadevne subjekte prizadevati za harmonizacijo predlog za priglasitev incidentov in nadzornih postopkov. Kadar je ustrezno, bi morali imeti pristojni organi iz Direktive (EU) 2022/2557 možnost, da od pristojnih organov iz te direktive zahtevajo, da izvajajo nadzorna in izvršilna pooblastila v zvezi s subjektom, ki je identificiran kot kritičen subjekt iz Direktive (EU) 2022/2557. Pristojni organi iz te direktive in pristojni organi iz Direktive (EU) 2022/2557 bi morali v ta namen sodelovati in si izmenjevati informacije, po možnosti v realnem času.

(31) Subjekti, ki spadajo v sektor digitalne infrastrukture, v bistvu temeljijo na omrežnih in informacijskih sistemih, zato bi morale obveznosti, ki se tem subjektom nalagajo na podlagi te direktive, celovito obravnavati fizično varnost takšnih sistemov kot del njihovih ukrepov obvladovanja tveganj za kibernetsko varnost in obveznosti poročanja. Ker so te zadeve zajete v tej direktivi, se obveznosti iz poglavij III, IV in VI Direktive (EU) 2022/2557 ne uporabljajo za takšne subjekte.

([11]) Uredba (ES) št. 300/2008 Evropskega parlamenta in Sveta z dne 11. marca 2008 o skupnih pravilih na področju varovanja civilnega letalstva in o razveljavitvi Uredbe (ES) št. 2320/2002 (UL L 97, 9.4.2008, str. 72).

([12]) Uredba (EU) 2018/1139 Evropskega parlamenta in Sveta z dne 4. julija 2018 o skupnih pravilih na področju civilnega letalstva in ustanovitvi Agencije Evropske unije za varnost v letalstvu ter spremembi uredb (ES) št. 2111/2005, (ES) št. 1008/2008, (EU) št. 996/2010, (EU) št. 376/2014 ter direktiv 2014/30/EU in 2014/53/EU Evropskega parlamenta in Sveta ter razveljavitvi uredb (ES) št. 552/2004 in (ES) št. 216/2008 Evropskega parlamenta in Sveta ter Uredbe Sveta (EGS) št. 3922/91 (UL L 212, 22.8.2018, str. 1).

([13]) Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o odpornosti kritičnih subjektov in razveljaviti Direktive Sveta 2008/114/ES (glej stran 164 tega Uradnega lista).

(32) 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 registre vrhnjih domenskih imen (TLD) in ponudnike storitev DNS, ki bi se morali šteti za subjekte, ki zagotavljajo javno dostopne storitve rekurzivnega razreševanja domenskih imen za končne uporabnike interneta ali storitve avtoritativnega razreševanja domenskih imen, ki jih uporabljajo tretje strani. Ta direktiva se ne bi smela uporabljati za korenske imenske strežnike.

(33) Storitve računalništva v oblaku bi morale zajemati digitalne storitve, ki omogočajo upravljanje na zahtevo in širok oddaljeni dostop do prožnega in po obsegu prilagodljivega nabora deljivih računalniških virov, tudi kadar so ti viri porazdeljeni na več lokacijah. Računalniški viri vključujejo vire, kot so omrežja, strežniki ali druga infrastruktura, operacijski sistemi, programska oprema, pomnilniki, aplikacije in storitve. Modeli storitev računalništva v oblaku med drugim vključujejo infrastrukturo kot storitev (IaaS), platformo kot storitev (PaaS), programsko opremo kot storitev (SaaS) in omrežje kot storitev (NaaS). Modeli uvajanja računalništva v oblaku bi morali vključevati zasebni, skupnostni, javni in hibridni oblak. Storitev računalništva v oblaku 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 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 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.

(34) Zaradi pojava inovativnih tehnologij in novih poslovnih modelov se pričakuje, da se bodo na notranjem trgu pojavili nove storitve računalništva v oblaku in novi modeli uvajanja 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).

(35) 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 omrežnih in informacijskih sistemov bi morala ta direktiva torej zajemati ponudnike 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 (IT) 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 bi smel nanašati na podatkovne centre v podjetjih, ki so v lasti zadevnega subjekta in jih ta upravlja za lastne namene.

(36) Raziskovalne dejavnosti imajo ključno vlogo pri razvijanju novih proizvodov in postopkov. Številne od teh dejavnosti izvajajo subjekti, ki delijo, razširjajo ali izkoriščajo rezultate svojih raziskav v komercialne namene. Ti subjekti so zato lahko pomembni akterji v vrednostnih verigah, zato je varnost njihovih omrežnih in informacijskih sistemov sestavni del splošne kibernetske varnosti notranjega trga. Raziskovalne organizacije bi bilo treba razumeti tako, da vključujejo subjekte, ki bistveni del svojih dejavnosti namenjajo izvajanju uporabnih raziskav ali

eksperimentalnega razvoja v smislu Frascatskega priročnika Organizacije za gospodarsko sodelovanje in razvoj iz leta 2015: Smernice za zbiranje in sporočanje podatkov o raziskavah in razvoju, da bi izkoristile njihove rezultate v komercialne namene, kot sta proizvodnja ali razvoj izdelka ali postopka, zagotavljanje storitve ali njihovo trženje.

(37) Vse večje medsebojne odvisnosti so rezultat vse bolj čezmejne in medsebojno odvisne mreže opravljanja storitev z uporabo ključnih infrastruktur po vsej Uniji v sektorjih, kot so energetika, promet, digitalna infrastruktura, pitna in odpadna voda, zdravje, nekateri vidiki javne uprave ter vesolje, 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 njenega vesoljskega programa. 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. Okrepljeni kibernetski napadi med pandemijo COVID-19 so razkrili ranljivost vse bolj medsebojno odvisnih družb zaradi tveganj z majhno verjetnostjo.

(38) 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, da imenujejo ali ustanovijo enega ali več pristojnih organov, odgovornih za kibernetsko varnost ter za nadzorne naloge na podlagi te direktive.

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

(40) Enotne kontaktne točke bi morale zagotavljati učinkovito čezmejno sodelovanje z ustreznimi organi drugih držav članic ter po potrebi s Komisijo in ENISA. Enotne kontaktne točke bi zato morale biti zadolžene za posredovanje priglasitev pomembnih incidentov s čezmejnim vplivom enotnim kontaktnim točkam drugih prizadetih držav članic na zahtevo skupine CSIRT ali pristojnega organa. Na nacionalni ravni bi morale enotne kontaktne točke omogočati nemoteno medsektorsko sodelovanje z drugimi pristojnimi organi. Enotne kontaktne točke bi tudi lahko prejemale ustrezne informacije o incidentih v zvezi s finančnimi subjekti od pristojnih organov iz Uredbe (EU) 2022/2554, ki bi jih morale biti sposobne posredovati, kakor je ustrezno, skupinam CSIRT ali ustreznim pristojnim nacionalnim organom iz te direktive.

(41) Države članice bi morale imeti ustrezne tehnične in organizacijske zmogljivosti za preprečevanje in odkrivanje incidentov in tveganj, odzivanje nanje in okrevanje po njih ter za ublažitev njihovih vplivov. Zato bi morale države članice v skladu s to direktivo ustanoviti ali imenovati eno ali več skupin CSIRT ter zagotoviti, da imajo ustrezna sredstva in tehnične zmogljivosti. Skupine CSIRT bi morale izpolnjevati zahteve iz te direktive, da bi se zagotovile učinkovite in združljive zmogljivosti za obvladovanje incidentov in tveganj ter zagotovilo učinkovito sodelovanje na ravni Unije. Države članice bi morale imeti možnost, da kot skupine CSIRT določijo obstoječe skupine za odzivanje na računalniške grožnje (skupine CERT). Za okrepitev odnosa zaupanja med subjekti in skupinami CSIRT, kadar je skupina CSIRT del pristojnega organa, bi morale imeti države članice možnost, da razmislijo o funkcionalnem ločevanju med operativnimi nalogami, ki jih opravljajo skupine CSIRT, zlasti v zvezi z izmenjavo informacij in podporo, ki se nudi subjektom, in nadzornimi dejavnostmi pristojnih organov.

(42) Skupine CSIRT so zadolžene za obvladovanje incidentov. To vključuje obdelavo velikih količin podatkov, ki so včasih občutljivi. Države članice bi morale zagotoviti, da imajo skupine CSIRT infrastrukturo za izmenjavo in obdelavo informacij ter ustrezno opremljeno osebje, ki zagotavlja zaupnost in zanesljivost njihovih dejavnosti. Skupine CSIRT bi lahko v zvezi s tem sprejele tudi kodekse ravnanja.

(43) Kar zadeva osebne podatke, bi moralo biti skupinam CSIRT omogočeno, da v skladu z Uredbo (EU) 2016/679 na zahtevo bistvenega ali pomembnega subjekta, zagotovijo proaktivni pregled omrežnih in informacijskih sistemov, ki se uporabljajo za opravljanje storitev subjekta. Kadar je to primerno, bi si morale države članice prizadevati za zagotovitev enake ravni tehničnih zmogljivosti za vse sektorske skupine CSIRT. Države članice bi morale imeti možnost, da pri oblikovanju svojih skupin CSIRT zaprosijo za pomoč ENISA.

(44) Skupine CSIRT bi morale imeti možnost, da na zahtevo bistvenega ali pomembnega subjekta spremljajo njegova sredstva, povezana z internetom, tako v njegovih prostorih kot drugje, da bi prepoznale, razumele in obvladale splošna organizacijska tveganja za subjekt, kar zadeva na novo odkrite grožnje v dobavni verigi ali kritične ranljivosti. Subjekt bi bilo treba spodbujati, naj skupini CSIRT sporoči, ali uporablja privilegirani upravljalni vmesnik, saj bi to lahko vplivalo na hitrost sprejemanja ublažitvenih ukrepov.

(45) 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. Zato bi morali imeti skupine CSIRT in pristojni organi za namene opravljanja svojih nalog možnost, da izmenjujejo informacije, vključno z osebnimi podatki, z nacionalnimi skupinami za odzivanje na incidente na področju računalniške varnosti ali pristojnimi organi tretjih držav, če so izpolnjeni pogoji iz prava Unije o varstvu podatkov za prenose osebnih podatkov tretjim državam, med drugim pogoji iz člena 49 Uredbe (EU) 2016/679.

(46) Bistveno je zagotoviti ustrezna sredstva za doseganje ciljev te direktive in pristojnim organom in skupinam CSIRT omogočiti izvajanje nalog, predpisanih v tej direktivi. Države članice lahko na nacionalni ravni uvedejo mehanizem financiranja za kritje potrebnih odhodkov, povezanih z izvajanjem nalog javnih subjektov, odgovornih za kibernetsko varnost v državi članici v skladu s to direktivo. Tak mehanizem bi moral biti skladen s pravom Unije ter sorazmeren in nediskriminatoren ter bi moral upoštevati različne pristope k zagotavljanju varnih storitev.

(47) Mreža skupin CSIRT bi morala še naprej prispevati h krepitvi zaupanja ter spodbujati hitro in učinkovito operativno sodelovanje med državami članicami. Za okrepitev operativnega sodelovanja na ravni Unije bi morala mreža skupin CSIRT razmisliti o tem, da bi k sodelovanju pri svojem delu povabila organe in agencije Unije, vključene v politiko na področju kibernetske varnosti, kot je Europol.

(48) Za doseganje in ohranjanje visoke ravni kibernetske varnosti bi morale biti nacionalne strategije za kibernetsko varnost, ki se zahtevajo na podlagi te direktive, sestavljene iz skladnih okvirov, ki določajo strateške cilje in prednostne naloge na področju kibernetske varnosti in upravljanja za njihovo doseganje. Te strategije lahko sestavlja eden ali več zakonodajnih ali nezakonodajnih instrumentov.

(49) Politike kibernetske higiene predstavljajo temelje za zaščito varnosti infrastruktur omrežnih in informacijskih sistemov, strojne opreme, programske opreme in spletnih aplikacij ter poslovnih podatkov ali podatkov končnih uporabnikov, ki jih subjekti uporabljajo. Politike kibernetske higiene zajemajo skupni izhodiščni nabor praks, vključno s posodobitvijo programske in strojne opreme, menjavanjem gesel, upravljanjem novih namestitev, omejevanjem računov s skrbniško ravnjo dostopa in varnostnim kopiranjem podatkov, omogočanjem proaktivnega okvira pripravljenosti ter splošno varnostjo in zaščito v primeru incidentov ali kibernetskih groženj. ENISA bi morala spremljati in analizirati politike kibernetske higiene držav članic.

(50) Ozaveščenost o kibernetski varnosti in kibernetska higiena sta bistveni za izboljšanje ravni kibernetske varnosti v Uniji, zlasti glede na vse večje število povezanih naprav, ki se vse pogosteje uporabljajo pri kibernetskih napadih. Prizadevati bi si bilo treba za izboljšanje splošne ozaveščenosti o tveganjih, povezanih s takimi napravami, ocene na ravni Unije pa bi lahko pomagale zagotoviti enotno razumevanje takih tveganj na notranjem trgu.

(51) Države članice bi morale spodbujati uporabo vseh inovativnih tehnologij, tudi umetne inteligence, katerih uporaba bi lahko izboljšala odkrivanje in preprečevanje kibernetskih napadov, kar bi omogočilo učinkovitejšo preusmeritev sredstev proti kibernetskim napadom. Zato bi morale države članice v svojih nacionalnih strategijah za kibernetsko varnost spodbujati dejavnosti na področju raziskav in razvoja, da bi olajšale uporabo teh tehnologij, zlasti tistih, ki zadevajo avtomatizirana ali polavtomatizirana orodja za kibernetsko varnost, in po potrebi izmenjave podatkov, potrebnih za usposabljanje uporabnikov take tehnologije in za njeno izboljšanje. Uporaba vsake inovativne tehnologije, tudi umetne inteligence, bi morala biti skladna s pravom Unije o varstvu podatkov, vključno z načeli varstva podatkov, in sicer točnost podatkov, minimizacija podatkov, pravičnost in preglednost, ter varnost podatkov, kot je najsodobnejše šifriranje. V celoti bi bilo treba izkoristiti zahteve glede vgrajenega in privzetega varstva podatkov, določene v Uredbi (EU) 2016/679.

(52) Odprtokodna orodja in aplikacije za kibernetsko varnost lahko prispevajo k višji stopnji odprtosti in lahko pozitivno vplivajo na učinkovitost industrijskih inovacij. Odprti standardi omogočajo interoperabilnost med orodji za varnost in koristijo varnosti industrijskih deležnikov. Odprtokodna orodja in aplikacije za kibernetsko varnost lahko spodbudijo širšo skupnost razvijalcev, kar omogoča diverzifikacijo dobaviteljev. Odprta koda lahko vodi k preglednejšemu postopku preverjanja orodij, povezanih s kibernetsko varnostjo, in k procesu odkrivanja ranljivosti, ki ga vodi skupnost. Države članice bi zato morale imeti možnost, da spodbujajo uporabo odprtokodne programske opreme in odprtih standardov z izvajanjem politik v zvezi z uporabo odprtih podatkov in odprtih virov kot dela varnosti prek preglednosti. Politike za spodbujanje uvajanja in trajnostne uporabe odprtokodnih orodij in aplikacij za kibernetsko varnost so še posebej pomembne za mala in srednja podjetja, ki se soočajo z velikimi stroški izvajanja, ki bi jih bilo mogoče zmanjšati, če bi se zmanjšala potreba po točno določenih aplikacijah ali orodjih.

(53) Javne dobrine so vse bolj povezane z digitalnimi omrežji v mestih za namene izboljšanja mestnih prometnih omrežij, nadgradnje infrastrukture za oskrbo z vodo in odlagališč odpadkov ter povečanja učinkovitost razsvetljave in ogrevanja stavb. Te digitalizirane javne dobrine so izpostavljene kibernetskim napadom in v primeru, da so ti uspešni, tvegajo, da zaradi njihove medsebojne povezanosti škodo utrpi veliko število državljanov. Države članice bi morale v okviru svojih nacionalnih strategij za kibernetsko varnost razviti politike, ki obravnavajo razvoj takih povezanih ali pametnih mest ter njihove morebitne učinke na družbo.

(54) V zadnjih letih se je v Uniji eksponentno povečalo število napadov z izsiljevalskim programjem, pri katerih zlonamerna programska oprema šifrira podatke in sisteme ter za njihovo sprostitev zahteva plačilo odkupnine. Vse pogostejši in hujši napadi z izsiljevalskim programjem so lahko posledica več dejavnikov, kot so različni vzorci napadov, kriminalni poslovni modeli v zvezi z „izsiljevalskim programjem kot storitvijo“ in kriptovalutami, zahteve po odkupninah in porast napadov na dobavne verige. Države članice bi morale v okviru svojih nacionalnih strategij za kibernetsko varnost oblikovati politike za boj proti porastu napadov z izsiljevalskim programjem.

(55) Javno-zasebna partnerstva na področju kibernetske varnosti lahko zagotovijo primeren okvir za izmenjavo znanja, širjenje dobrih praks in vzpostavitev skupne ravni razumevanja med deležniki. Države članice bi morale spodbujati politike, na katere se opira ustanavljanje javno-zasebnih partnerstev, ki se posebej ukvarjajo s kibernetsko varnostjo. Te politike bi morale med drugim jasno opredeliti področje uporabe in vključene deležnike, model upravljanja, razpoložljive možnosti financiranja in interakcijo med sodelujočimi deležniki, kar zadeva javno-zasebna partnerstva. Javno-zasebna partnerstva lahko izkoristijo strokovno znanje subjektov iz zasebnega sektorja za pomoč pristojnim organom pri razvijanju najsodobnejših storitev in procesov, vključno z izmenjavo informacij, zgodnjim opozarjanjem, vajami na področju kibernetskih groženj in incidentov, obvladovanjem kriz in načrtovanjem odpornosti.

(56) Države članice bi morale v svojih nacionalnih strategijah za kibernetsko varnost obravnavati posebne potrebe malih in srednjih podjetij na področju kibernetske varnosti. Mala in srednja podjetja po vsej Uniji predstavljajo velik odstotek industrijskega in poslovnega trga ter se pogosto težje prilagajajo novim poslovnim praksam v bolj povezanem svetu in digitalnem okolju, v katerem zaposleni delajo od doma, poslovanje pa vse bolj poteka prek spleta. Nekatera mala in srednja podjetja se soočajo s posebnimi izzivi na področju kibernetske varnosti, kot so slaba kibernetska ozaveščenost, slaba informacijska varnost pri poslovanju na daljavo, visoki stroški rešitev za kibernetsko varnost in višja stopnja ogroženosti, na primer zaradi izsiljevalskega programja, za kar bi jim bilo treba nuditi usmerjanje in podporo. Mala in srednja podjetja so vse pogosteje tarča napadov na dobavne verige zaradi manj strogih ukrepov za obvladovanje tveganj na področju kibernetske varnosti in obvladovanje napadov ter dejstva, da so njihova sredstva za varnost omejena. Taki napadi na dobavne verige ne vplivajo zgolj na mala in srednja podjetja ter njihovo poslovanje, ampak imajo lahko tudi kaskadne učinke za večje napade na subjekte, katerim ta dobavljajo blago. Države članice bi morale prek svojih nacionalnih strategij za kibernetsko varnost

pomagati malim in srednjim podjetjem pri spoprijemanju z izzivi, s katerimi se soočajo v svojih dobavnih verigah. Države članice bi morale imeti kontaktno točko na nacionalni ali regionalni ravni za mala in srednja podjetja, ki bi tem zagotavljala smernice in pomoč ali jih napotila na ustrezne organe za usmerjanje in pomoč v zvezi z vprašanji, povezanimi s kibernetsko varnostjo. Države članice se tudi spodbuja, naj mikropodjetjem in malim podjetjem, ki nimajo teh zmogljivosti, ponudijo storitve, kot sta konfiguracija spletišč in omogočanje beleženja.

(57) Države članice bi morale v okviru svojih nacionalnih strategij za kibernetsko varnost sprejeti politike za spodbujanje aktivne kibernetske zaščite kot dela širše obrambne strategije. Bolj kot za reaktivno odzivanje gre pri aktivni kibernetski zaščiti za aktivno preprečevanje, odkrivanje, spremljanje, analiziranje in ublažitev kršitev varnosti omrežja, skupaj z uporabo zmogljivosti znotraj in zunaj ogroženega omrežja. To bi lahko vključevalo nudenje, s strani držav članic, brezplačnih storitev ali orodij nekaterim subjektom, vključno s samopostrežnimi pregledi, orodji za odkrivanje in storitvami odstranjevanja. Sposobnost hitre in avtomatske izmenjave ter razumevanja informacij o grožnjah in njihove analize, opozorila o kibernetski dejavnosti ter odzivanje so kritični za doseganje enotnosti prizadevanj za uspešno preprečevanje, odkrivanje, obvladovanje in blokiranje napadov na omrežne in informacijske sisteme. Aktivna kibernetska zaščita temelji na obrambni strategiji, ki izključuje ofenzivne ukrepe.

(58) Ker lahko izkoriščanje ranljivosti v omrežnih in informacijskih sistemih povzroči hude motnje in škodo, sta hitro odkrivanje in odpravljanje takih ranljivosti pomemben dejavnik pri zmanjševanju tveganja. Subjekti, ki razvijajo ali upravljajo omrežne in informacijske sisteme, bi morali zato vzpostaviti ustrezne postopke za obravnavanje ranljivosti, ko jih odkrijejo. Ker ranljivosti pogosto odkrijejo in jih razkrijejo tretje osebe, bi moral proizvajalec ali ponudnik proizvodov IKT ali storitev IKT vzpostaviti tudi potrebne postopke za prejemanje informacij o ranljivostih od tretjih oseb. V zvezi s tem mednarodna standarda ISO/IEC 30111 in ISO/IEC 29147 določata usmeritve o obravnavanju in razkrivanju ranljivosti. Okrepitev usklajevanja med poročajočimi fizičnimi in pravnimi osebami in proizvajalci ali ponudniki proizvodov IKT ali storitev IKT je še posebej pomembna za spodbujanje prostovoljnega okvira za razkrivanje ranljivosti. Usklajeno razkrivanje ranljivosti določa strukturiran postopek, prek katerega se ranljivosti sporočijo proizvajalcu ali ponudniku potencialno ranljivega proizvoda IKT ali storitve IKT tako, da lahko diagnosticira in odpravi ranljivost, preden se podrobne informacije o ranljivosti razkrijejo tretji osebi ali javnosti. Usklajeno razkrivanje ranljivosti bi moralo vključevati tudi usklajevanje med poročajočo fizično ali pravno osebo in proizvajalcem ali ponudnikom potencialno ranljivega proizvoda IKT ali storitve IKT v zvezi s časovnim okvirom za odpravo in objavo ranljivosti.

(59) Komisija, ENISA in države članice bi morale še naprej spodbujati usklajevanje z mednarodnimi standardi in obstoječimi dobrimi praksami industrije na področju obvladovanja tveganj za kibernetsko varnost, na primer na področju ocen varnosti dobavne verige, izmenjave informacij in razkrivanja ranljivosti.

(60) Države članice bi morale v sodelovanju z ENISA sprejeti ukrepe za olajšanje usklajenega razkrivanja ranljivosti z vzpostavitvijo ustrezne nacionalne politike. Države članice bi si morale v okviru svoje nacionalne politike prizadevati, da v skladu z nacionalnim pravom čim bolje obravnavajo izzive, s katerimi se soočajo raziskovalci ranljivosti, vključno z njihovo morebitno izpostavljenostjo kazenski odgovornosti. Glede na to, da bi bile lahko fizične in pravne osebe, ki raziskujejo ranljivosti, v nekaterih državah članicah izpostavljene kazenski in civilnopravni odgovornosti, se države članice spodbuja, naj sprejmejo smernice v zvezi s tem, da se raziskovalcev informacijske varnosti kazensko ne preganja in da so njihove dejavnosti izvzete iz civilnopravne odgovornosti.

(61) Države članice bi morale eno od svojih skupin CSIRT imenovati za koordinatorja, ki bi po potrebi deloval kot zaupanja vreden posrednik med poročajočimi fizičnimi ali pravnimi osebami in proizvajalci ali ponudniki proizvodov IKT ali storitev IKT, ki bi jih ranljivost lahko prizadela. Naloge skupine CSIRT, ki je imenovana za koordinatorja, bi morale vključevati identifikacijo prizadetih subjektov in vzpostavitev stika z njimi, podpiranje

fizičnih ali pravnih oseb, ki poročajo o ranljivosti, pogajanja o časovnicah razkrivanja in obvladovanja ranljivosti, ki vplivajo na več subjektov (usklajeno razkrivanje ranljivosti več strani). Kadar bi ranljivosti lahko pomembno vplivale na subjekte v več državah članicah, bi morale skupine CSIRT, ki so imenovane kot koordinatorji, po potrebi sodelovati v okviru mreže skupin CSIRT.

(62) Dostop do točnih in pravočasnih informacij o ranljivostih, ki vplivajo na proizvode IKT in storitve IKT, prispeva k okrepljenemu obvladovanju tveganj za kibernetsko varnost. Viri javno dostopnih informacij o ranljivostih so pomembno orodje za subjekte in uporabnike njihovih storitev, pa tudi za pristojne organe in skupine CSIRT. Zato bi morala ENISA vzpostaviti evropsko podatkovno zbirko ranljivosti, v kateri bi subjekti, ne glede na to, ali spadajo na področje uporabe te direktive, in njihovi dobavitelji omrežnih in informacijskih sistemov, kot tudi pristojni organi in skupine CSIRT, lahko prostovoljno razkrivali in evidentirali javno znane ranljivosti z namenom, da se uporabnikom omogoči sprejetje ustreznih blažilnih ukrepov. Namen te podatkovne zbirke je obravnava edinstvenih izzivov, ki jih tveganja pomenijo za subjekte Unije. Poleg tega bi morala ENISA vzpostaviti ustrezen postopek v zvezi s postopkom objave, da bi imeli subjekti čas za sprejetje blažilnih ukrepov v zvezi s svojimi ranljivostmi, ter uporabiti najsodobnejše ukrepe za obvladovanje tveganj za kibernetsko varnost, kot tudi strojno berljive nabore podatkov in ustrezne vmesnike. Za spodbujanje kulture razkrivanja ranljivosti razkritje ne bi smelo negativno vplivati na poročajočo fizično ali pravno osebo.

(63) Čeprav podobni registri ali podatkovne zbirke o ranljivostih obstajajo, te upravljajo in vzdržujejo subjekti, ki nimajo sedeža v Uniji. Evropska podatkovna zbirka ranljivosti, ki bi jo vzdrževala ENISA, bi zagotovila večjo preglednost v zvezi s postopkom objave pred javnim razkritjem ranljivosti in odpornost v primeru motnje ali prekinitve pri opravljanju podobnih storitev. Da bi v največji možni meri preprečila podvajanje prizadevanj in poskušala doseči dopolnjevanje, bi morala ENISA preučiti možnost sklenitve sporazumov o strukturnem sodelovanju s podobnimi registri ali podatkovnimi zbirkami, ki spadajo v jurisdikcije tretjih držav. ENISA bi morala zlasti preučiti možnost tesnega sodelovanja z upravljavci sistema skupnih ranljivosti in izpostavljenosti.

(64) Skupina za sodelovanje bi morala podpirati in spodbujati strateško sodelovanje in izmenjavo informacij ter krepiti zaupanje med državami članicami. Skupina za sodelovanje bi morala vsaki dve leti pripraviti delovni program. Ta program bi moral vključevati ukrepe, ki jih skupina za sodelovanje sprejme za izvajanje svojih ciljev in nalog. Časovni okvir za pripravo prvega delovnega programa na podlagi te direktive bi moral biti usklajen s časovnim okvirom zadnjega delovnega programa, pripravljenega na podlagi Direktive (EU) 2016/1148, da bi se preprečile morebitne motnje pri delu skupine za sodelovanje.

(65) 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, zlasti o lažjem usklajevanju med državami članicami pri prenosu te direktive, ki bi se obravnavala z boljšim izvajanjem obstoječih pravil. Skupina za sodelovanje bi poleg tega lahko evidentirala nacionalne rešitve, da bi se spodbudila združljivost rešitev na področju kibernetske varnosti, ki se uporabljajo v vsakem posameznem sektorju po Uniji. To je zlasti pomembno za sektorje mednarodne ali čezmejne narave.

(66) 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 sredstev. Organizirala bi lahko redne skupne sestanke z ustreznimi zasebnimi deležniki iz vse Unije, na katerih bi se razpravljalo o dejavnostih, ki jih izvaja skupina za sodelovanje, in zbirali podatki in informacije o nastajajočih izzivih politike. Poleg tega bi morala skupina za sodelovanje redno ocenjevati položaj, kar zadeva kibernetske grožnje ali incidente, kot je izsiljevalsko programje. Za okrepitev sodelovanja na ravni Unije bi morala skupina za sodelovanje razmisliti o tem, da bi k sodelovanju pri svojem delu povabila ustrezne institucije, organe, urade in agencije Unije, vključene v politiko na področju

kibernetske varnosti, kot so Evropski parlament, Europol, Evropski odbor za varstvo podatkov, Agencija Evropske unije za varnost v letalstvu, ustanovljena z Uredbo (EU) 2018/1139, in Agencija Evropske unije za vesoljski program, ustanovljena z Uredbo (EU) 2021/696 Evropskega parlamenta in Sveta ([14]).

(67) Pristojni organi in skupine CSIRT bi morali imeti možnost, da sodelujejo v programih izmenjave uradnikov iz drugih držav članic, in sicer v posebnem okviru in, kadar je ustrezno, z zahtevano varnostno odobritvijo za uradnike, ki sodelujejo v takih programih izmenjave, da bi se izboljšalo sodelovanje in okrepilo zaupanje med državami članicami. Pristojni organi bi morali sprejeti potrebne ukrepe, s katerimi bi uradnikom iz drugih držav članic omogočili učinkovito sodelovanje v dejavnostih pristojnega organa ali skupine CSIRT gostiteljice.

(68) Države članice bi morale prispevati k vzpostavitvi okvira EU za odzivanje na krize na področju kibernetske varnosti, določenega v Priporočilu Komisije (EU) 2017/1584 ([15]), z obstoječimi mrežami za sodelovanje, zlasti Evropsko organizacijsko mrežo za povezovanje v kibernetski krizi (v nadaljnjem besedilu: mreža EU-CyCLONe), mrežo skupin CSIRT in skupino za sodelovanje. Mreža EU-CyCLONe in mreža skupin CSIRT bi morali sodelovati na podlagi postopkovnih ureditev, ki določajo podrobnosti tega sodelovanja, in se izogibati morebitnemu podvajanju nalog. V poslovniku mreže EU-CyCLONe bi morale biti podrobneje opredeljene ureditve delovanja te mreže, vključno z njenimi 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 enotno ureditev EU za politično odzivanje na krize iz Izvedbenega sklepa Sveta (EU) 2018/1993 ([16]). Komisija bi morala v ta namen uporabljati postopek medsektorskega kriznega usklajevanja na visoki ravni v okviru sistema ARGUS. Če ima kriza znaten vpliv na zunanjo ali skupno varnostno in obrambno politiko, bi bilo treba sprožiti mehanizem Evropske službe za zunanje delovanje za krizno odzivanje.

(69) V skladu s Prilogo k Priporočilu (EU) 2017/1584 bi moral velik kibernetski incident pomeniti incident, ki povzroči motnje, ki presegajo zmožnost države članice za odziv nanje, ali pomembno vpliva na vsaj dve državi članici. Glede na njihov vzrok in vpliv se lahko kibernetski incidenti velikih razsežnosti stopnjujejo in sprevržejo v popolno krizo, ki ne omogoča ustreznega delovanja notranjega trga, ali pomenijo resna tveganja za javno varnost ter varnost subjektov ali državljanov v več državah članicah ali Uniji kot celoti. Glede na velik obseg in večinoma čezmejno naravo takih incidentov bi morali države članice ter ustrezne institucije, organi, uradi in agencije Unije sodelovati na tehnični, operativni in politični ravni za ustrezno usklajevanje odziva po vsej Uniji.

(70) V primeru kibernetskih incidentov velikih razsežnosti in kriz na ravni Unije je potrebno usklajeno delovanje, da bi se zagotovil hiter in učinkovit odziv, saj je medsebojna odvisnost sektorjev in držav članic zelo velika. Razpoložljivost kibernetsko odpornih omrežnih in informacijskih sistemov ter razpoložljivost, zaupnost in celovitost podatkov so bistvenega pomena za varnost Unije in zaščito njenih državljanov, podjetij in institucij pred incidenti in kibernetskimi grožnjami, pa tudi za krepitev zaupanja posameznikov in organizacij v zmožnost Unije, da spodbuja in varuje globalen, odprt, svoboden, stabilen in varen kibernetski prostor, ki temelji na človekovih pravicah, temeljnih svoboščinah, demokraciji in pravni državi.

([14]) Uredba (EU) 2021/696 Evropskega parlamenta in Sveta z dne 28. aprila 2021 o vzpostavitvi Vesoljskega programa Unije in ustanovitvi Agencije Evropske unije za vesoljski program ter razveljavitvi uredb (EU) št. 912/2010, (EU) št. 1285/2013 in (EU) št. 377/2014 ter Sklepa št. 541/2014/EU (UL L 170, 12.5.2021, str. 69).

([15]) 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).

([16]) Izvedbeni sklep Sveta (EU) 2018/1993 z dne 11. decembra 2018 o enotni ureditvi EU za politično odzivanje na krize (UL L 320, 17.12.2018, str. 28).

(71) Mreža EU-CyCLONe bi morala pri kibernetskih incidentih velikih razsežnosti in krizah delovati kot posrednik med tehnično in politično ravnjo, okrepiti sodelovanje na operativni ravni in podpirati odločanje na politični ravni. Ob upoštevanju pristojnosti Komisije na področju obvladovanja kriz bi morala mreža EU-CyCLONe sodelovati s Komisijo in se opirati na ugotovitve mreže skupin CSIRT ter uporabiti lastne zmogljivosti za pripravo analize vpliva kibernetskih incidentov velikih razsežnosti in kriz.

(72) Kibernetski napadi so čezmejne narave in pomembni incident lahko zmoti ali poškoduje kritično informacijsko infrastrukturo, od katere je odvisno nemoteno delovanje notranjega trga. Priporočilo (EU) 2017/1584 obravnava vlogo vseh ustreznih akterjev. Komisija je v okviru mehanizma Unije na področju civilne zaščite, vzpostavljenega s Sklepom št. 1313/2013/EU Evropskega parlamenta in Sveta ([17]), tudi pristojna za dejavnosti splošne pripravljenosti, vključno z vodenjem Centra za usklajevanje nujnega odziva in skupnega komunikacijskega in informacijskega sistema za primer nesreč, ohranjanjem in nadaljnjim razvojem situacijskega zavedanja in analitične zmožnosti ter vodenjem zmožnosti za mobilizacijo in napotitev strokovnih ekip v primeru prošnje države članice ali tretje države za pomoč. Komisija je odgovorna tudi za zagotavljanje analitičnih poročil za enotno ureditev za politično odzivanje na krize v skladu z Izvedbenim sklepom (EU) 2018/1993, tudi v zvezi s situacijskim zavedanjem na področju kibernetske varnosti in pripravljenostjo ter za situacijsko zavedanje in krizno odzivanje na področju kmetijstva, slabih vremenskih razmer, kartiranja in napovedi konfliktov, sistemov zgodnjega opozarjanja na naravne nesreče, izrednih zdravstvenih razmer, nadzora okužb, zdravja rastlin, kemičnih incidentov, varnosti hrane in krme, migracij, carine, jedrske energije, izrednih radioloških dogodkov ter energije na splošno.

(73) Unija lahko, kadar je ustrezno, v skladu s členom 218 PDEU sklepa mednarodne sporazume s tretjimi državami ali mednarodnimi organizacijami, ki omogočajo in urejajo njihovo sodelovanje pri nekaterih dejavnostih skupine za sodelovanje, mreže skupin CSIRT ter mreže EU-CyCLONe. Taki sporazumi bi morali zagotoviti upoštevanje interesov Unije in ustrezno varstvo podatkov. To ne bi smelo izključevati pravice držav članic do sodelovanja s tretjimi državami pri obvladovanju ranljivosti in obvladovanju tveganj za kibernetsko varnost, ki omogoča poročanje in souporabo splošnih informacij v skladu s pravom Unije.

(74) Da bi se olajšalo učinkovito izvajanje te direktive, kar med drugim zadeva obvladovanje ranljivosti, ukrepe obvladovanja tveganj za kibernetsko varnost, obveznosti poročanja in dogovore o izmenjavi informacij o kibernetski varnosti, lahko države članice sodelujejo s tretjimi državami in izvajajo dejavnosti, ki se štejejo kot ustrezne za ta namen, vključno z izmenjavo informacij o kibernetskih grožnjah, incidentih, ranljivostih, orodjih in metodah, taktikah, tehnikah in postopkih, pripravljenostjo in vajami za obvladovanje kibernetskih kriz, usposabljanjem, vzpostavljanjem zaupanja in dogovori o strukturirani izmenjavi informacij.

(75) Uvesti bi bilo treba medsebojne strokovne preglede, da bi se pripomoglo k učenju iz skupnih izkušenj, krepilo medsebojno zaupanje in dosegla visoko skupno raven kibernetske varnosti. Medsebojni strokovni pregledi lahko omogočijo pomembna spoznanja in priporočila, ki krepijo splošne zmogljivosti za kibernetsko varnost, ustvarijo dodatno funkcionalno pot za izmenjavo primerov dobre prakse med državami članicami in prispevajo k izboljšanju zrelosti držav članic na področju kibernetske varnosti. Poleg tega bi morali medsebojni strokovni pregledi upoštevati rezultate podobnih mehanizmov, kot je sistem medsebojnega strokovnega pregleda mreže skupin CSIRT, dodati vrednost in preprečiti podvajanje. Izvajanje medsebojnih strokovnih pregledov ne bi smelo posegati v pravo Unije ali nacionalno pravo o varstvu zaupnih ali tajnih podatkov.

(76) Skupina za sodelovanje bi morala vzpostaviti metodologijo samoocenjevanja za države članice, da bi zajela dejavnike, kot so raven izvajanja ukrepov za obvladovanje tveganj za kibernetsko varnost in obveznosti poročanja, raven zmogljivosti in učinkovitost izvajanja nalog pristojnih organov, operativne zmogljivosti skupin CSIRT, raven izvajanja skupne pomoči, raven izvajanja dogovorov o izmenjavi informacij o kibernetski varnosti ali posebna vprašanja čezmejne ali medsektorske narave. Države članice bi bilo treba spodbujati, da redno izvajajo samoocenjevanje ter v okviru skupine za sodelovanje predstavijo rezultate svoje samoocene in o njih razpravljajo.

([17]) Sklep št. 1313/2013/EU Evropskega parlamenta in Sveta z dne 17. decembra 2013 o mehanizmu Unije na področju civilne zaščite (UL L 347, 20.12.2013, str. 924).

(77) Za zagotavljanje varnosti omrežnih in informacijskih sistemov so v veliki meri odgovorni bistveni in pomembni subjekti. Spodbujati in razvijati bi bilo treba kulturo obvladovanja tveganj, ki vključuje oceno tveganja in izvajanje ukrepov za obvladovanje tveganja na področju kibernetske varnosti, ki ustrezajo trenutnim tveganjem.

(78) Pri ukrepih za obvladovanje tveganj za kibernetsko varnost bi bilo treba upoštevati stopnjo odvisnosti bistvenega ali pomembnega subjekta od omrežnih in informacijskih sistemov, mednje pa bi morali spadati ukrepi za prepoznavanje tveganj incidentov, preprečevanje in odkrivanje incidentov, odzivanje nanje in okrevanje po njih ter ublažitev njihovega vpliva. Varnost omrežnih in informacijskih sistemov bi morala vključevati varnost shranjenih, prenesenih in obdelanih podatkov. Ukrepi za obvladovanje tveganj za kibernetsko varnost bi morali zagotoviti sistemske analize, ob upoštevanju človeškega faktorja, da bi se pridobila celotna slika varnosti omrežnega in informacijskega sistema.

(79) Ker imajo lahko grožnje za varnost omrežnih in informacijskih sistemov različen izvor, bi morali ukrepi za obvladovanje tveganj za kibernetsko varnost temeljiti na pristopu, ki vključuje vse nevarnosti in katerega namen je zaščititi omrežne in informacijske sisteme ter fizično okolje teh sistemov pred dogodki, kot so kraja, požar, poplave, izpadi telekomunikacij ali električne energije, ali pred kakršnim koli nepooblaščenim fizičnim dostopom in poškodbami ali poseganjem v informacije bistvenega ali pomembnega subjekta in njegovo opremo za obdelavo informacij, ki bi lahko ogrozili razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki se ponujajo ali so dostopne prek omrežnih in informacijskih sistemov. Ukrepi za obvladovanje tveganj za kibernetsko varnost bi zato morali obravnavati tudi fizično in okoljsko varnost omrežnih in informacijskih sistemov z vključitvijo ukrepov za zaščito tovrstnih sistemov pred okvarami sistemov, človeškimi napakami, zlonamernimi dejanji ali naravnimi pojavi v skladu z evropskimi ali mednarodno priznanimi standardi, kot so tisti iz serije ISO/IEC 27000. V zvezi s tem bi morali bistveni in pomembni subjekti v okviru svojih ukrepov za obvladovanje tveganj za kibernetsko varnost obravnavati tudi varnost človeških virov in imeti vzpostavljene ustrezne politike za nadzor dostopa. Ti ukrepi bi morali biti skladni z Direktivo (EU) 2022/2557.

(80) Države članice bi morale za dokazovanje skladnosti z ukrepi za obvladovanje tveganj za kibernetsko varnost in, če ni ustreznih evropskih certifikacijskih shem za kibernetsko varnost, sprejetih v skladu z Uredbo (EU) 2019/881 Evropskega parlamenta in Sveta ([18]), ob posvetovanju s skupino za sodelovanje in Evropsko certifikacijsko skupino za kibernetsko varnost spodbujati uporabo ustreznih evropskih in mednarodnih standardov pri bistvenih in pomembnih subjektih ali pa od subjektov zahtevati, naj uporabljajo certificirane proizvode IKT, storitve in postopke IKT.

(81) 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 tveganji za zadevni omrežni in informacijski sistem, ob upoštevanju dovršenosti takih ukrepov ter po potrebi ustreznih evropskih in mednarodnih standardov in stroškov njihovega izvajanja.

(82) Ukrepi za obvladovanje tveganj za kibernetsko varnost bi morali biti sorazmerni s stopnjo izpostavljenosti bistvenega ali pomembnega subjekta tveganjem ter družbenim in gospodarskim vplivom, ki bi ga incident imel. Pri določanju ukrepov za obvladovanje tveganj za kibernetsko varnost, prilagojenih bistvenim in pomembnih subjektom, bi bilo treba ustrezno upoštevati različno izpostavljenost tveganjem, ki jo imajo bistveni in pomembni subjekti, kot so kritična pomembnost subjekta, tveganja, vključno z družbenimi tveganji, katerim je subjekt izpostavljen, velikost subjekta ter verjetnost incidentov in njihovo resnost, vključno z njihovim družbenim in gospodarskim vplivom.

([18]) 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).

(83) Bistveni in pomembni subjekti bi morali zagotoviti varnost omrežnih in informacijskih sistemov, ki jih uporabljajo pri svojih dejavnostih. Ti sistemi so predvsem zasebni omrežni in informacijski sistemi, ki jih upravlja njihovo notranje osebje za IT ali za varnost katerih skrbi zunanji izvajalec. Zahteve glede ukrepov za obvladovanje tveganj za kibernetsko varnost in obveznosti poročanja, določene v tej direktivi, bi se morale uporabljati za ustrezne bistvene in pomembne subjekte ne glede na to, ali ti subjekti svoje omrežne in informacijske sisteme vzdržujejo sami ali pa njihovo vzdrževanje oddajajo zunanjim izvajalcem.

(84) Ponudniki storitev sistema domenskih imen, registri vrhnjih domenskih imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnih centrov, ponudniki omrežij za dostavo vsebine, ponudniki upravljanih storitev, ponudniki upravljanih varnostnih storitev, ponudniki spletnih tržnic, spletnih brskalnikov in platform za storitve družbenega mreženja ter ponudniki storitev zaupanja bi morali biti zaradi svoje čezmejne narave predmet večje harmonizacije na ravni Unije. Izvajanje ukrepov za obvladovanje tveganj za kibernetsko varnost v zvezi s temi subjekti bi bilo zato treba olajšati z izvedbenim aktom.

(85) Obravnavanje tveganj, ki izhajajo iz dobavne verige subjekta in njegovega razmerja z njegovimi dobavitelji, kot so ponudniki storitev shranjevanja in obdelave podatkov ali ponudniki upravljanih varnostnih storitev ter urejevalci programske opreme, 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 omrežnih in informacijskih sistemov subjekta z izkoriščanjem ranljivosti, ki vplivajo na proizvode in storitve tretje osebe. Bistveni in pomembni subjekti bi morali zato oceniti in upoštevati splošno kakovost in odpornost proizvodov in storitev, v njih zajetih ukrepov za obvladovanje tveganj za kibernetsko varnost ter praks svojih dobaviteljev in ponudnikov storitev na področju kibernetske varnosti, vključno z njihovimi varnimi razvojnimi postopki. Bistvene in pomembne subjekte bi bilo treba zlasti spodbujati, da ukrepe za obvladovanje tveganj za kibernetsko varnost vključijo v pogodbene dogovore s svojimi neposrednimi dobavitelji in ponudniki storitev. Ti subjekti bi lahko upoštevali tveganja, ki izhajajo iz drugih ravni dobaviteljev in ponudnikov storitev.

(86) Med ponudniki storitev imajo ponudniki upravljanih varnostnih storitev na področjih, kot so odzivanje na incidente, penetracijsko testiranje, varnostne presoje in svetovanje, še posebej pomembno vlogo pri zagotavljanju pomoči subjektom pri njihovih prizadevanjih za preprečevanje in odkrivanje incidentov ter odzivanje nanje ali okrevanje po njih. Vendar pa so bili ponudniki upravljanih varnostnih storitev tudi sami tarče kibernetskih napadov in zaradi svoje tesne vključenosti v delovanje izvajalcev pomenijo posebno tveganje. Bistveni in pomembni subjekti bi morali biti zato še bolj skrbni pri izbiri ponudnika upravljanih varnostnih storitev.

(87) Tudi pristojni organi lahko v okviru svojih nadzornih nalog uporabljajo storitve kibernetske varnosti, kot so varnostne presoje in penetracijsko testiranje ali odzivi na incidente.

(88) Bistveni in pomembni subjekti bi morali obravnavati tudi tveganja, ki izhajajo iz njihovih stikov in odnosov z drugimi deležniki v okviru širšega ekosistema, tudi v zvezi s preprečevanjem industrijskega vohunjenja in zaščito poslovnih skrivnosti. Ti 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 in sledi dobrim praksam v zvezi z varnim dostopom in razširjanjem informacij na splošno ter še posebno z varstvom intelektualne lastnine. Podobno bi morali bistveni in pomembni subjekti glede na pomen in vrednost podatkov za dejavnosti teh subjektov pri uporabi storitev pretvorbe podatkov in podatkovne analitike, ki jih opravljajo tretje osebe, sprejeti vse ustrezne ukrepe za obvladovanje tveganj za kibernetsko varnost.

(89) Bistveni in pomembni subjekti bi morali sprejeti širok nabor osnovnih praks računalniške higiene, kot so načela popolnega nezaupanja, posodobitve programske opreme, konfiguracija naprav, segmentacija omrežja, upravljanje identitete in dostopa ter ozaveščenost uporabnikov, organizirati usposabljanje in ozaveščanje svojega osebja v zvezi s kibernetskimi grožnjami podjetjem, lažnim predstavljanjem in tehnikami socialnega inženiringa. Ti subjekti bi morali tudi oceniti lastne zmogljivosti glede kibernetske varnosti in si po potrebi prizadevati za vključevanje tehnologij za povečanje kibernetske varnosti, kot so umetna inteligenca ali sistemi strojnega učenja, da okrepijo svoje zmogljivosti in varnost omrežnih in informacijskih sistemov.

(90) Za nadaljnje obravnavanje ključnih tveganj za dobavno verigo ter zagotavljanje pomoči bistvenim in pomembnim subjektom, ki delujejo v sektorjih, zajetih s to direktivo, pri ustreznem obvladovanju varnostnih tveganj, povezanih z dobavno verigo in dobavitelji, bi morala skupina za sodelovanje v sodelovanju s Komisijo in ENISA ter po potrebi po posvetovanju z ustreznimi deležniki izvesti usklajene ocene tveganja za varnost v zvezi s kritičnimi dobavnimi verigami, kot je že storila za omrežja 5G na podlagi Priporočila Komisije (EU) 2019/534 ([19]), da bi identificirala kritične storitve IKT, sisteme IKT ali proizvode IKT, zadevne grožnje in ranljivosti za posamezne sektorje. Pri teh usklajenih ocenah tveganja za varnost bi bilo treba določiti ukrepe, načrte za ublažitev in dobre prakse za preprečevanje kritičnih odvisnosti, morebitnih kritičnih točk odpovedi, groženj, ranljivosti in drugih tveganj, povezanih z dobavno verigo, ter preučiti načine za nadaljnje spodbujanje bistvenih in pomembnih subjektov k njihovemu širšemu sprejetju. Morebitni netehnični dejavniki tveganja, kot je neprimeren vpliv tretje države na dobavitelje in ponudnike storitev, zlasti v primeru alternativnih modelov upravljanja, vključujejo prikrite ranljivosti ali stranska vrata in morebitne sistemske motnje v oskrbi, zlasti v primeru tehnološke vezanosti na ponudnika ali odvisnosti od njega.

(91) Pri usklajenih ocenah tveganja za varnost v zvezi s kritičnimi dobavnimi verigami bi bilo treba glede na značilnosti zadevnega sektorja upoštevati tehnične in, kadar je ustrezno, netehnične dejavnike, vključno z dejavniki, opredeljenimi v Priporočilu (EU) 2019/534, iz usklajene ocene EU tveganj za kibernetsko varnost omrežij 5G in nabora orodij EU za kibernetsko varnost omrežij 5G, o katerem se je dogovorila skupina za sodelovanje. Za identifikacijo dobavnih verig, ki bi morale biti predmet usklajene ocene tveganja za varnost, bi bilo treba upoštevati naslednja merila: (i) obseg, v katerem bistveni in pomembni subjekti uporabljajo določene kritične storitve IKT, sisteme IKT ali proizvode IKT in se zanašajo nanje; (ii) pomembnost določenih kritičnih storitev IKT, sistemov IKT ali proizvodov IKT za izvajanje kritičnih ali občutljivih funkcij, vključno z obdelavo osebnih podatkov; (iii) razpoložljivost alternativnih storitev IKT, sistemov IKT ali proizvodov IKT; (iv) odpornost celotne dobavne verige storitev IKT, sistemov IKT ali proizvodov IKT skozi njihov življenjski cikel proti dogodkom, ki povzročajo motnje v delovanju, in (v) morebiten prihodnji pomen nastajajočih storitev, sistemov ali proizvodov IKT za dejavnosti subjektov. Poleg tega bi bilo treba posebno pozornost nameniti storitvam IKT, sistemom IKT ali izdelkom IKT, za katere veljajo posebne zahteve, ki izhajajo iz tretjih držav.

(92) Za racionalizacijo obveznosti, naloženih ponudnikom javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev in ponudnikom storitev zaupanja, povezanih z varnostjo njihovih omrežnih in informacijskih sistemov, ter za omogočanje zadevnim subjektom in pristojnim organom iz Direktive (EU) 2018/1972 Evropskega parlamenta in Sveta ([20]) oziroma Uredbe (EU) št. 910/2014, da izkoristijo pravni okvir, vzpostavljen s to direktivo, vključno z imenovanjem skupine CSIRT, odgovorne za obravnavanje incidentov, sodelovanje pristojnih organov pri delu skupine za sodelovanje in mreže skupin CSIRT, bi morali biti ti subjekti vključeni na področje uporabe te direktive. Zato bi bilo treba črtati ustrezne določbe iz Uredbe (EU) št. 910/2014 ter Direktive (EU) 2018/1972, 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.

(93) Za obveznosti glede kibernetske varnosti iz te direktive bi bilo treba šteti, da dopolnjujejo zahteve, naložene ponudnikom storitev zaupanja na podlagi Uredbe (EU) št. 910/2014. Od ponudnikov storitev zaupanja bi bilo treba zahtevati, da sprejmejo vse ustrezne in sorazmerne ukrepe za obvladovanje tveganj za njihove storitve, tudi v zvezi s strankami in zanašajočimi se tretjimi stranmi, ter da poročajo o incidentih v skladu s to direktivo. Takšne obveznosti glede kibernetske varnosti in poročanja bi se morale nanašati tudi na fizično zaščito opravljenih storitev. Zahteve za ponudnike kvalificiranih storitev zaupanja iz člena 24 Uredbe (EU) št. 910/2014 se še naprej uporabljajo.

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

([20]) 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).

(94) Države članice lahko vlogo pristojnih organov za storitve zaupanja dodelijo nadzornim organom v okviru Uredbe (EU) št. 910/2014, da zagotovijo nadaljevanje sedanjih praks ter nadgradijo znanje in izkušnje, pridobljene pri uporabi navedene uredbe. V tem primeru bi morali pristojni organi na podlagi te direktive pravočasno in tesno sodelovati s temi nadzornimi organi in si izmenjati ustrezne informacije, da se zagotovita učinkovit nadzor in skladnost ponudnikov storitev zaupanja z zahtevami iz te direktive in Uredbe (EU) št. 910/2014. Skupina CSIRT ali pristojni organ iz te direktive bi moral, kadar je ustrezno, nemudoma obvestiti nadzorni organ iz Uredbe (EU) št. 910/2014 o vsaki priglašeni pomembni kibernetski grožnji ali incidentu, ki vpliva na storitve zaupanja, ter o vseh kršitvah te direktive s strani ponudnika storitev zaupanja. Države članice lahko za namene poročanja po potrebi uporabijo enotno vstopno točko, ki je bila vzpostavljena za namene skupnega in samodejnega poročanja o incidentih nadzornemu organu iz Uredbe (EU) št. 910/2014 ter skupini CSIRT in pristojnemu organu iz te direktive.

(95) Kadar je ustrezno in za preprečitev nepotrebnih motenj, bi bilo treba pri prenosu te direktive upoštevati obstoječe nacionalne smernice, sprejete za prenos pravil, povezanih z varnostnimi ukrepi, določenimi v členih 40 in 41 Direktive (EU) 2018/1972, s čimer bi se nadgradili znanje in spretnosti, ki so že bili pridobljeni v okviru Direktive (EU) 2018/1972 glede varnostnih ukrepov in priglasitev incidentov. Da bi se olajšala harmonizacija in prehod ter bi bile motnje čim manjše, lahko ENISA pripravi tudi usmeritve v zvezi z zahtevami glede varnosti in obveznosti poročanja za ponudnike javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev. Države članice lahko vlogo pristojnih organov za elektronske komunikacije dodelijo nacionalnim regulativnim organom iz Direktive (EU) 2018/1972, da zagotovijo nadaljevanje sedanjih praks ter nadgradijo znanje in izkušnje, pridobljene pri izvajanju navedene direktive.

(96) Glede na vse večji pomen medosebnih komunikacijskih storitev, neodvisnih od številke, kot so opredeljene v Direktivi (EU) 2018/1972, je treba zagotoviti, da se tudi za take storitve uporabljajo ustrezne varnostne zahteve, ob upoštevanju njihove posebne narave in gospodarskega pomena. S širjenjem napadne površine postajajo medosebne komunikacijske storitve, neodvisne od številke, kot so sporočilne storitve, močno razširjeni napadni vektorji. Zlonamerni storilci uporabljajo platforme za komuniciranje in privabljanje žrtev, da odprejo spletne strani, ki niso varne, kar povečuje verjetnost incidentov, ki vključujejo izkoriščanje osebnih podatkov in s tem varnost omrežnih in informacijskih sistemov. Ponudniki medosebnih komunikacijskih storitev, neodvisnih od številke, bi morali zagotoviti raven varnosti omrežnih in informacijskih sistemov, primerno obstoječim tveganjem. Ker ponudniki medosebnih komunikacijskih storitev, neodvisnih od številke, običajno nimajo dejanskega nadzora nad prenosom signalov prek omrežja, je mogoče raven tveganj za take storitve v nekaterih pogledih šteti za manjšo kot pri tradicionalnih elektronskih komunikacijskih storitvah. Enako velja za medosebne komunikacijske storitve, kot so opredeljene v Direktivi (EU) 2018/1972, ki uporabljajo številke in nimajo dejanskega nadzora nad prenosom signalov.

(97) Notranji trg je bolj odvisen od delovanja interneta kot kdaj koli prej. Storitve skoraj 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 vsi ponudniki javnih elektronskih komunikacijskih omrežij vzpostavljene ustrezne ukrepe za obvladovanje tveganj za kibernetsko varnost in da poročajo o pomembnih incidentih v zvezi z njo. Države članice bi morale zagotoviti, da se ohrani varnost javnih elektronskih komunikacijskih omrežij in da so njihovi bistveni varnostni interesi zaščiteni pred sabotažo in vohunjenjem. Ker mednarodna povezljivost krepi in pospešuje konkurenčno digitalizacijo Unije in njenega gospodarstva, bi bilo treba o incidentih, ki vplivajo na podmorske komunikacijske kable, poročati skupini CSIRT ali po potrebi pristojnemu organu. Nacionalna strategija za kibernetsko varnost bi morala po potrebi upoštevati kibernetsko varnost podmorskih komunikacijskih kablov ter vključevati kartiranje morebitnih tveganj za kibernetsko varnost in blažilne ukrepe, da se zagotovi najvišja raven njihove zaščite.

(98) Za zaščito varnosti javnih elektronskih komunikacijskih omrežij in javno dostopnih elektronskih komunikacijskih storitev bi bilo treba spodbujati uporabo tehnologij šifriranja, zlasti šifriranja od konca do konca, in drugih na podatkih temelječih varnostnih tehnologij, kot so kartiranje, segmentacija, označevanje, politika in upravljanje dostopa ter samodejne odločitve za dostop. Po potrebi bi morala biti uporaba šifriranja, zlasti šifriranja od konca do konca, obvezna za ponudnike javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev v skladu z načeloma privzete in vgrajene varnosti ter zasebnosti za namene člena te direktive. Uporabo šifriranja od konca do konca bi bilo treba uskladiti s pooblastili držav članic, da zagotovijo zaščito svojih bistvenih varnostnih interesov in javne varnosti ter omogočijo preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj v skladu s pravom Unije. Vendar to ne bi smelo oslabiti šifriranja od konca do konca, ki je ključna tehnologija za učinkovito varstvo podatkov ter zasebnosti in varnosti komunikacij.

(99) Da bi se ohranila varnost ter preprečile zlorabe in manipulacije z javnimi elektronskimi komunikacijskimi omrežji in javno dostopnimi elektronskimi komunikacijskimi storitvami, bi bilo treba spodbujati uporabo varnih standardov usmerjanja za zagotovitev celovitosti in zanesljivosti funkcij usmerjanja v celotnem ekosistemu ponudnikov storitev dostopa do interneta.

(100) Da bi se zaščitili funkcionalnost in celovitost interneta ter spodbujali varnost in odpornost DNS, bi bilo treba ustrezne deležnike, vključno s subjekti zasebnega sektorja Unije, ponudnike javno dostopnih elektronskih komunikacijskih storitev, zlasti ponudnike storitev dostopa do interneta, in ponudnike spletnih iskalnikov spodbujati, naj sprejmejo strategijo za diverzifikacijo razreševanja DNS. Poleg tega bi bilo treba države članice spodbujati, naj razvijejo in uporabljajo javno in varno evropsko storitev razreševanja DNS.

(101) Direktiva določa večstopenjski pristop k poročanju o pomembnih incidentih za vzpostavitev ustreznega ravnovesja med, na eni strani, hitrim poročanjem, ki pomaga ublažiti morebitno širjenje pomembnih incidentov ter bistvenim in pomembnim subjektom omogoča, da zaprosijo za podporo, ter, na drugi strani, podrobnim poročanjem, pri katerem se pridobivajo dragocene izkušnje iz posameznih incidentov ter sčasoma poveča odpornost posameznih subjektov in celotnih sektorjev proti kibernetskim grožnjam. Glede tega bi morala direktiva vključevati poročanje o incidentih, ki lahko na podlagi začetne ocene zadevnega subjekta povzročijo znatne operativne motnje storitev ali finančne izgube za ta subjekt ali vplivajo na druge fizične ali pravne osebe, tako da bi povzročili precejšnjo premoženjsko ali nepremoženjsko škodo. Pri tovrstni začetni oceni bi bilo med drugim treba upoštevati prizadete omrežne in informacijske sisteme, zlasti njihov pomen pri zagotavljanju storitev subjekta, resnost in tehnične značilnosti kibernetske grožnje, obstoječe ranljivosti, ki se izkoriščajo, ter izkušnje subjekta s podobnimi incidenti. Kazalniki, kot so obseg vpliva na delovanje storitve, trajanje incidenta ali število prizadetih prejemnikov storitev, bi lahko imeli pomembno vlogo pri ugotavljanju, ali je operativna motnja storitve resna.

(102) Kadar se bistveni ali pomembni subjekti seznanijo s pomembnim incidentom, bi se moralo od njih zahtevati, da brez nepotrebnega odlašanja in v vsakem primeru najpozneje v 24 urah predložijo zgodnje opozorilo. Temu zgodnjemu opozorilu bi moralo slediti obvestilo o incidentu. Zadevni subjekti bi morali incident priglasiti brez nepotrebnega odlašanja, v vsakem primeru pa v 72 urah po seznanitvi s pomembnim incidentom, zlasti da bi posodobili informacije, predložene z zgodnjim opozorilom, ter navedli začetno oceno pomembnega incidenta, vključno z njegovo resnostjo in vplivom ter kazalniki ogroženosti, če so na voljo. Končno poročilo bi bilo treba predložiti najpozneje en mesec po priglasitvi incidenta. Zgodnje opozorilo bi moralo vključevati informacije, ki so potrebne za seznanitev skupine CSIRT ali po potrebi pristojnega organa s pomembnim incidentom in zadevnemu subjektu omogočajo, da po potrebi zaprosi za pomoč. V tovrstnem zgodnjem opozorilu bi bilo treba po potrebi navesti, ali obstaja sum, da je pomemben incident nastal zaradi nezakonitih ali zlonamernih dejanj, in ali je verjetno, da bo imel čezmejni vpliv. Države članice bi morale zagotoviti, da se zaradi obveznosti zgodnjega opozarjanja ali naknadnega obvestila o incidentu ne preusmerijo sredstva priglasitvenega subjekta za dejavnosti, povezane

z obvladovanjem incidentov, ki jim je treba dati prednost, ter da se zaradi obveznosti poročanja o incidentih ne bodo preusmerila sredstva od upravljanja odzivov na pomembne incidente ali drugače ogrozila prizadevanja subjektov v zvezi s tem. V primeru incidenta, ki je ob predložitvi končnega poročila še vedno v teku, bi morale države članice poskrbeti, da zadevni subjekti takrat predložijo poročilo o napredku, končno poročilo pa najpozneje en mesec po razrešitvi pomembnega incidenta.

(103) Po potrebi bi morali bistveni in pomembni subjekti brez nepotrebnega odlašanja obvestiti prejemnike storitev o ukrepih in pravnih sredstvih, ki jih lahko sprejmejo za ublažitev posledičnega tveganja zaradi pomembne kibernetske grožnje. Kadar je ustrezno in zlasti kadar je verjetno, da se bo znatna kibernetska grožnja uresničila, bi morali ti subjekti o tej grožnji obvestiti tudi svoje prejemnike storitev. Zahteva glede obveščanja zadevnih prejemnikov o takih grožnjah subjektov bi se morala izvajati po najboljših močeh, vendar teh subjektov ne bi smela odvezati obveznosti, da na lastne stroške sprejmejo ustrezne in takojšnje ukrepe za preprečevanje ali odpravo vseh tovrstnih groženj in ponovno vzpostavitev običajne ravni varnosti storitve. Zagotavljanje takih informacij o pomembnih kibernetskih varnostnih grožnjah prejemnikom storitve bi moralo biti brezplačno ter napisano v zlahka razumljivem jeziku.

(104) Ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev bi morali izvajati privzeto in vgrajeno varnost ter prejemnike storitve obvestiti o pomembnih kibernetskih grožnjah ter ukrepih, ki jih lahko sprejmejo za zagotovitev varnosti svojih naprav in komunikacij, na primer z uporabo posebnih vrst programske opreme ali tehnologij šifriranja.

(105) Proaktiven pristop h kibernetskim grožnjam je bistven element ukrepov za obvladovanje tveganj za kibernetsko varnost, ki bi moral pristojnim organom omogočiti, da učinkovito preprečijo, da bi se kibernetske grožnje udejanjile v incidentih, ki lahko povzročijo znatno premoženjsko ali nepremoženjsko škodo. V ta namen je priglasitev kibernetskih groženj ključnega pomena. Zato se subjekte spodbuja, naj prostovoljno poročajo o kibernetskih grožnjah.

(106) Da bi se poenostavilo sporočanje informacij, ki se zahtevajo s to direktivo, ter da bi se zmanjšalo upravno breme za subjekte, bi morale države članice za predložitev ustreznih informacij, ki jih je treba sporočiti, zagotoviti tehnična sredstva, kot so enotna vstopna točka, avtomatizirani sistemi, spletni obrazci, uporabniku prijazni vmesniki, predloge, namenske platforme za uporabo subjektov, ne glede na to, ali spadajo na področje uporabe te direktive. Financiranje Unije, s katerim se podpira izvajanje te direktive, zlasti v okviru programa Digitalna Evropa, vzpostavljenega z Uredbo (EU) 2021/694 Evropskega parlamenta in Sveta ([21]), bi lahko vključevalo podporo za enotne vstopne točke. Poleg tega so subjekti 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 dodatno upravno breme in lahko privedejo tudi do negotovosti v zvezi z obliko in postopki takih priglasitev. Kadar se vzpostavi enotna vstopna točka, se države članice spodbuja, naj to enotno vstopno točko uporabljajo tudi za priglasitve varnostnih incidentov, ki se zahtevajo na podlagi drugega prava Unije, kot sta Uredba (EU) 2016/679 in Direktiva 2002/58/ES. Uporaba takšne enotne vstopne točke za poročanje o varnostnih incidentih na podlagi Uredbe (EU) 2016/679 in Direktive 2002/58/ES ne bi smela vplivati na uporabo določb Uredbe (EU) 2016/679 in Direktive 2002/58/ES, zlasti tistih, ki se nanašajo na neodvisnost organov iz navedenih aktov. ENISA bi morala v sodelovanju s skupino za sodelovanje oblikovati skupne predloge za priglasitev na podlagi smernic, da bi se poenostavile in racionalizirale informacije, ki jih je treba sporočiti na podlagi prava Unije, ter zmanjšalo upravno breme za priglasitvene subjekte.

(107) 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. Kadar 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 ENISA olajšata usklajevanje med pristojnimi organi in organi kazenskega pregona različnih držav članic.

([21]) Uredba (EU) 2021/694 Evropskega parlamenta in Sveta z dne 29. aprila 2021 o vzpostavitvi programa Digitalna Evropa in razveljavitvi Sklepa (EU) 2015/2240 (UL L 166, 11.5.2021, str. 1).

(108) V številnih primerih je zaradi incidentov ogrožena varnost osebnih podatkov. V tem okviru bi morali pristojni organi sodelovati in si izmenjevati informacije o vseh pomembnih zadevah z organi iz Uredbe (EU) 2016/679 in Direktive 2002/58/ES.

(109) Vzdrževanje točnih in popolnih podatkovnih zbirk o registraciji domenskih imen (podatki WHOIS) ter omogočanje zakonitega dostopa do takih podatkov sta bistvena za zagotavljanje varnosti, stabilnosti in odpornosti sistema domenskih imen, kar posledično prispeva k višji skupni ravni kibernetske varnosti v Uniji. V ta namen bi bilo treba od registrov vrhnjih domenskih imen in subjektov, ki zagotavljajo storitve registracije domenskih imen, zahtevati, da obdelajo nekatere podatke, potrebne za dosego tega namena. Takšna obdelava bi morala pomeniti zakonsko obveznost v smislu člena 6(1), točka (c), Uredbe (EU) 2016/679. Ta obveznost ne posega v možnost zbiranja podatkov o registraciji domenskih imen za druge namene, na primer na podlagi pogodbenih dogovorov ali zakonskih zahtev, določenih v drugem pravu Unije ali nacionalnem pravu. Namen te obveznosti je doseči popoln in točen nabor podatkov o registraciji in ne bi smela povzročiti večkratnega zbiranja istih podatkov. Registri vrhnjih domenskih imen in subjekti, ki zagotavljajo storitve registracije domenskih imen, bi morali med seboj sodelovati, da bi se preprečilo podvajanje te naloge.

(110) Razpoložljivost in pravočasna dostopnost podatkov o registraciji domenskih imen za osebe, ki imajo upravičen razlog za dostop, je ključnega pomena za preprečevanje zlorab sistema domenskih imen in boj proti njim ter za preprečevanje in odkrivanje incidentov ter odzivanje nanje. Osebe, ki imajo upravičen razlog za dostop, se razumejo kot vse fizične ali pravne osebe, ki predložijo zahtevo na podlagi prava Unije ali nacionalnega prava. Vključujejo lahko organe, ki so na podlagi te direktive, in organe, ki so na podlagi prava Unije ali nacionalnega prava, pristojni za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ter skupine CERT ali CSIRT. Registri vrhnjih domenskih imen in subjekti, ki opravljajo storitve registracije domenskih imen, bi morali biti v skladu s pravom Unije in nacionalnim pravom dolžni zagotoviti zakonit dostop do podatkov o registraciji posameznih domenskih imen, ki so potrebne za namene zahteve za dostop, osebam, ki imajo upravičen razlog za dostop. Zahtevi oseb, ki imajo upravičen razlog za dostop, bi bilo treba priložiti obrazložitev, ki omogoča oceno potrebe po dostopu do podatkov.

(111) Da bi se zagotovila razpoložljivost točnih in popolnih podatkov o registraciji domenskih imen, bi morali registri vrhnjih domenskih imen in subjekti, ki opravljajo storitve registracije domenskih imen, zbirati podatke o registraciji domenskih imen ter zagotavljati njihovo celovitost in razpoložljivost. Zlasti bi morali registri vrhnjih domenskih imen in subjekti, ki opravljajo storitve registracije domenskih imen, vzpostaviti politike in postopke za zbiranje ter vzdrževanje točnih in popolnih podatkov o registraciji domenskih imen ter za preprečevanje in popravljanje netočnih podatkov o registraciji v skladu s pravili Unije o varstvu podatkov. Te politike in postopki bi morali v največji možni meri upoštevati standarde, ki so jih razvile strukture upravljanja z več deležniki na mednarodni ravni. Registri vrhnjih domenskih imen in subjekti, ki opravljajo storitve registracije domenskih imen, bi morali sprejeti in izvajati sorazmerne postopke za preverjanje podatkov o registraciji domenskih imen. Ti postopki bi morali odražati primere dobre prakse, ki se uporabljajo v panogi, in v kar največjem obsegu napredek na področju elektronske identifikacije. Primeri postopkov preverjanja lahko vključujejo predhodne kontrole, izvedene v času registracije, in naknadne kontrole, izvedene po registraciji. Registri vrhnjih domenskih imen in subjekti, ki opravljajo storitve registracije domenskih imen, bi morali zlasti preveriti vsaj en način, s katerim registrator vzpostavlja stik.

(112) Registri TLD imen in subjektov, ki zanje opravljajo storitve registracije domenskih imen, bi morali 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, v skladu s preambulo Uredbe (EU) 2016/679, narediti javno dostopne. Registri TLD imen in subjekti, ki zanje opravljajo storitve registracije domenskih imen, bi morali za pravne osebe narediti javno dostopno vsaj ime registratorja in kontaktno telefonsko številko. Objaviti bi bilo treba tudi kontaktni elektronski naslov, pod pogojem, da ta ne vsebuje osebnih podatkov, kot v primeru e-poštnega vzdevka ali funkcionalnih računov. Registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen, 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 TLD imen in subjekti, ki 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 TLD imen in subjekti, ki 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 za dostop s strani oseb, ki imajo upravičen razlog za dostop. Te politike in postopki bi morali v največji možni meri upoštevati smernice in standarde, ki so jih razvile strukture upravljanja z več deležniki na

mednarodni ravni. 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 harmoniziranih praks na notranjem trgu in brez poseganja v pristojnosti Evropskega odbora za varstvo podatkov določi smernice o takih postopkih, ki v kar največji meri upoštevajo standarde, ki so jih razvile strukture upravljanja z več deležniki na mednarodni ravni. Države članice bi morale zagotoviti, da so vse vrste dostopa do osebnih in neosebnih podatkov o registraciji domenskih imen brezplačne.

(113) Subjekti, ki spadajo na področje uporabe te direktive, bi morali spadati v pristojnost države članice, kjer imajo sedež. Vendar bi se moralo za ponudnike javnih elektronskih omrežij ali ponudnike javno dostopnih elektronskih komunikacijskih storitev šteti, da spadajo v pristojnost države članice, v kateri opravljajo svoje storitve. Za ponudnike storitev DNS, registre TLD imen, subjekte, ki opravljajo storitve registracije domenskih imen, ponudnike storitev računalništva v oblaku, ponudnike storitev podatkovnih centrov, ponudnike omrežij za dostavo vsebine, ponudnike upravljanih storitev, ponudnike upravljanih varnostnih storitev ter ponudnike spletnih tržnic, spletnih brskalnikov in platform za storitve družbenega mreženja bi se moralo šteti, da spadajo v pristojnost države članice, v kateri imajo glavni sedež v Uniji. Subjekti javne uprave bi morali spadati v pristojnost države članice, ki jih je ustanovila. Če subjekt opravlja storitve ali ima sedež v več kot eni državi članici, bi moral spadati v ločeno in sočasno pristojnost vsake od teh držav članic. Pristojni organi teh držav članic bi morali sodelovati, si medsebojno pomagati in, kadar je ustrezno, izvajati skupne nadzorne ukrepe. Kadar države članice izvajajo pristojnost, v skladu z načelom *ne bis in idem* ne bi smele več kot enkrat naložiti izvršilnih ukrepov ali sankcij za isto ravnanje.

(114) Da bi se upoštevala čezmejna narava storitev in postopkov ponudnikov storitev DNS, registrov TLD imen, subjektov, ki opravljajo storitve registracije domenskih imen, ponudnikov storitev računalništva v oblaku, ponudnikov storitev podatkovnih centrov, ponudnikov omrežij za dostavo vsebine, ponudnikov upravljanih storitev, ponudnikov upravljanih varnostnih storitev ter ponudnikov spletnih tržnic, spletnih brskalnikov in platform za storitve družbenega mreženja, bi morala biti za te subjekte pristojna samo ena država članica. 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 omrežni 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. Šteti bi bilo treba, da je glavni sedež v državi članici, kjer se v Uniji po večini sprejemajo odločitve v zvezi z ukrepi za obvladovanje tveganj za kibernetsko varnost. To običajno ustreza kraju osrednje uprave subjektov v Uniji. Če take države članice ni mogoče določiti ali če se take odločitve ne sprejemajo v Uniji, bi bilo treba šteti, da je glavni sedež v državi članici, kjer se izvajajo operacije v zvezi s kibernetsko varnostjo. Če take države članice ni mogoče določiti, bi bilo treba šteti, da je glavni sedež v državi članici, 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.

(115) Kadar javno dostopno rekurzivno storitev DNS opravlja ponudnik javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev le kot del storitve dostopa do interneta, bi bilo treba šteti, da je subjekt v pristojnosti vseh držav članic, v katerih se opravljajo njegove storitve.

(116) Kadar ponudnik storitev DNS, register TLD imen, subjekt, ki opravlja storitve registracije domenskih imen, ponudnik storitev računalništva v oblaku, ponudnik storitev podatkovnih centrov, ponudnik omrežij za dostavo vsebine, ponudnik upravljanih storitev, ponudnik upravljanih varnostnih storitev ali ponudnik spletne tržnice, spletnega brskalnika ali platforme za storitve družbenega mreženja, ki nima sedeža v Uniji, ponuja storitve v Uniji, bi moral imenovati predstavnika v Uniji. Da bi se ugotovilo, ali tak subjekt ponuja storitve v Uniji, bi bilo treba preveriti, ali namerava subjekt svoje storitve ponujati posameznikom v eni ali več državah članicah. Sama dostopnost v Uniji spletnega mesta subjekta ali posrednika ali elektronskega naslova ali drugih kontaktnih podatkov ali uporaba jezika, ki se običajno uporablja v tretji državi, v kateri ima subjekt sedež, se ne bi smela šteti, da zadošča za določitev takšne namere. Vendar bi 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 pokazalo, 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 nagovorijo predstavnika. Predstavnik bi moral biti izrecno imenovan s pisnim pooblastilom subjekta, da v njegovem imenu izvaja njegove obveznosti iz te direktive, vključno s poročanjem o incidentih.

(117) Da bi se zagotovil jasen pregled ponudnikov storitev DNS, registrov TLD imen, subjektov, ki opravljajo storitve registracije domenskih imen, ponudnikov storitev računalništva v oblaku, ponudnikov storitev podatkovnih centrov, ponudnikov omrežij za dostavo vsebine, ponudnikov upravljanih storitev, ponudnikov upravljanih varnostnih storitev ter ponudnikov spletnih tržnic, spletnih brskalnikov in platform za storitve družbenega mreženja, ki po vsej Uniji zagotavljajo storitve, ki spadajo na področje uporabe te direktive, bi morala ENISA vzpostaviti in vzdrževati register tovrstnih subjektov na podlagi informacij, ki jih prejme od države članic, po potrebi preko nacionalnih mehanizmov, vzpostavljenih za to, da se subjekti registrirajo. Enotne kontaktne točke bi morale ENISA posredovati informacije in vse njihove spremembe. Za zagotovitev točnosti in popolnosti informacij, ki se vključijo v ta register, lahko države članice ENISA predložijo informacije o teh subjektih, ki so na voljo v nacionalnih registrih. ENISA in države članice bi morale sprejeti ukrepe za lajšanje interoperabilnosti takšnih registrov, hkrati pa zagotoviti varstvo zaupnih ali tajnih informacij. ENISA bi morala vzpostaviti ustrezne protokole za razvrščanje in upravljanje informacij, s čimer bi zagotovila varnost in zaupnost razkritih informacij ter omejila dostop, shranjevanje in prenos tovrstnih informacij predvidenim uporabnikom.

(118) Kadar se podatki, ki so uvrščeni med tajne v skladu s pravom Unije ali nacionalnim pravom izmenjujejo, sporočajo ali drugače souporabljajo na podlagi te direktive, bi se morala uporabljati ustrezna pravila o ravnanju s tajnimi podatki. Poleg tega bi ENISA morala imeti vzpostavljeno infrastrukturo, postopke in pravila za obravnavo občutljivih in zaupnih informacij v skladu z veljavnimi varnostnimi predpisi za varovanje tajnih podatkov EU.

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

(120) Države članice bi morale spodbuditi subjekte in jim pomagati, da skupaj izkoristijo svoje individualno znanje in praktične izkušnje na strateški, taktični in operativni ravni, da bi tako okrepili svoje zmogljivosti za ustrezno preprečevanje in odkrivanje incidentov, odzivanje nanje in okrevanje po njih ali ublažitev njihovega vpliva. Zato je treba omogočiti, da se na ravni Unije vzpostavijo prostovoljni dogovori o izmenjavi informacij o kibernetski varnosti. V ta namen bi morale države članice dejavno podpirati in spodbujati subjekte, kot so tisti, ki opravljajo storitve in raziskave s področja kibernetske varnosti, kot tudi ustrezne subjekte, ki ne spadajo na področje uporabe te direktive, naj sodelujejo v takih dogovorih o izmenjavi informacij o kibernetski varnosti. Ti dogovori bi se morale vzpostaviti v skladu s pravili Unije o konkurenci in pravom Unije o varstvu podatkov.

(121) Obdelava osebnih podatkov v obsegu, ki je potreben in sorazmeren za zagotovitev varnosti omrežnih in informacijskih sistemov, ki jo izvajajo bistveni in pomembni subjekti, bi lahko štela za zakonito na podlagi tega, da je taka obdelava skladna s pravno obveznostjo, ki velja za upravljavca, v skladu z zahtevami iz člena 6(1), točka (c), in člena 6(3) Uredbe (EU) 2016/679. Obdelava osebnih podatkov bi lahko bila potrebna tudi za zakonite interese bistvenih in pomembnih subjektov ter ponudnikov varnostnih tehnologij in storitev, ki ravnajo v imenu teh subjektov, v skladu s členom 6(1), točka (f), Uredbe (EU) 2016/679, tudi kadar je taka obdelava potrebna za dogovore o izmenjavi informacij o kibernetski varnosti ali prostovoljno obveščanje o ustreznih informacijah v skladu s to direktivo. Ukrepi, povezani s preprečevanjem, odkrivanjem, prepoznavanjem, zajezitvijo in analizo incidentov ter odzivanjem nanje, ukrepi za ozaveščanje v zvezi s posebnimi kibernetskimi grožnjami, izmenjavo informacij v okviru odpravljanja in usklajenega razkrivanja ranljivosti ter prostovoljno izmenjavo informacij o takih incidentih, pa tudi o kibernetskih grožnjah in ranljivostih, kazalnikih ogroženosti, taktikah, tehnikah in postopkih, opozorilih glede kibernetske varnosti in orodjih za konfiguracijo, bi lahko zahtevali obdelavo nekaterih kategorij osebnih podatkov, kot so naslovi IP, enotni naslovi vira (URL), domenska imena, elektronski naslovi in, kadar ti razkrivajo osebne podatke, časovni žigi. Obdelava osebnih podatkov s strani pristojnih organov, enotnih kontaktnih točk in skupin CSIRT bi lahko pomenila pravno obveznost ali bi se lahko štela za potrebno za izvajanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu podatkov v skladu s členom 6(1), točki (c) ali (e), in členom 6(3) Uredbe (EU) 2016/679, ali za zasledovanje pravnega interesa bistvenih in pomembnih subjektov iz člena 6(1), točka (f), navedene uredbe. Poleg tega bi se lahko v nacionalnem pravu določila pravila, ki bi pristojnim organom, enotnim kontaktnim točkam in skupinam CSIRT omogočala, da v obsegu, ki je potreben in sorazmeren za zagotavljanje varnosti omrežnih in informacijskih sistemov bistvenih in pomembnih subjektov, obdelujejo posebne vrste osebnih podatkov v skladu s členom 9 Uredbe (EU) 2016/679, zlasti z določitvijo ustreznih in posebnih ukrepov za varstvo temeljnih pravic in interesov fizičnih oseb, vključno s tehničnimi omejitvami ponovne uporabe takih podatkov in uporabe najsodobnejših ukrepov za varnost in ohranjanje zasebnosti, kot so psevdonimizacija ali šifriranje, kadar lahko anonimizacija znatno vpliva na zastavljeni namen.

(122) Za okrepitev nadzornih pooblastil in ukrepov, ki pomagajo zagotavljati dejansko skladnost, 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 teh subjektov in pristojnih organov. Tako bi morala za bistvene subjekte veljati celovita ureditev predhodnega in naknadnega nadzora, medtem ko bi morala za pomembne subjekte veljati manj stroga ureditev naknadnega nadzora. Od pomembnih subjektov se torej ne bi smelo zahtevati, da sistematično evidentirajo izpolnjevanje ukrepov za obvladovanje tveganj za kibernetsko varnost, pristojni organi pa bi morali uporabljati reaktivni naknadni pristop k nadzoru in tako ne bi imeli splošne obveznosti nadzorovanja teh subjektov. Naknadni nadzor pomembnih subjektov se lahko sproži na podlagi dokazov, znakov ali informacij, s katerimi se seznanijo pristojni organi in za katere ti organi menijo, da kažejo na morebitne kršitve te direktive. Ti dokazi, znaki ali informacije so lahko na primer takšni, kot jih pristojnim organom predložijo drugi organi, subjekti, državljani, mediji ali drugi viri, ali javno dostopne informacije, ali pa lahko izhajajo iz drugih dejavnosti, ki jih izvajajo pristojni organi pri izpolnjevanju svojih nalog.

(123) Pristojni organi z izvajanjem nadzornih nalog ne bi smeli po nepotrebnem ovirati poslovnih dejavnosti zadevnega subjekta. Kadar pristojni organi izvajajo svoje nadzorne naloge v zvezi z bistvenimi subjekti, vključno z izvajanjem inšpekcijskih pregledov na kraju samem in na daljavo, preiskovanjem kršitev te direktive, izvajanjem varnostnih revizij ali varnostnih pregledov, bi morali karseda zmanjšati vpliv na poslovne dejavnosti zadevnega subjekta.

(124) Pristojni organi bi morali imeti pri izvajanju predhodnega nadzora možnost, da se na sorazmeren način odločijo o prednostni razvrstitvi uporabe nadzornih ukrepov in sredstev, ki so jim na voljo. To pomeni, da se lahko pristojni organi odločijo za takšno prednostno razvrstitev uporabe na podlagi metodologij za nadzor, ki bi morale upoštevati pristop, ki temelji na tveganju. Natančneje, take metodologije bi lahko vključevale merila ali referenčne vrednosti za razvrstitev bistvenih subjektov v kategorije tveganja in ustrezne nadzorne ukrepe ter sredstva, ki se priporočajo glede na kategorijo tveganja, kot so uporaba, pogostost ali vrsta inšpekcijskih pregledov na kraju samem, ciljno usmerjene varnostne presoje ali varnostni pregledi, vrsta informacij, ki jih je treba zahtevati, in raven podrobnosti teh

informacij. Takšne metodologije za nadzor bi lahko spremljali tudi delovni programi ter bi se lahko redno ocenjevale in pregledovale, tudi glede vidikov, kot so dodeljevanje sredstev in potrebe. V zvezi s subjekti javne uprave bi bilo treba nadzorna pooblastila izvajati v skladu z nacionalnimi zakonodajnimi in institucionalnimi okviri.

(125) Pristojni organi bi morali zagotoviti, da njihove nadzorne naloge v zvezi z bistvenimi in pomembnimi subjekti izvajajo usposobljeni strokovnjaki, ki bi morali imeti potrebna znanja in spretnosti za izvajanje teh nalog, zlasti v zvezi z izvajanjem inšpekcijskih pregledov na kraju samem in nadzorom zunaj lokacije, vključno z prepoznavanjem pomanjkljivosti v podatkovnih zbirkah, strojni opremi, požarnih zidovih, šifriranju in omrežjih. Te inšpekcijske preglede in ta nadzor bi bilo treba izvajati na objektiven način.

(126) Pristojni organ bi moral imeti v ustrezno utemeljenih primerih, ko je seznanjen s pomembno kibernetsko grožnjo ali neposrednim tveganjem, možnost, da sprejme takojšnje odločitve o izvrševanju, da bi preprečil incident ali se nanj odzval.

(127) Da bi bilo izvrševanje učinkovito, bi bilo treba določiti minimalni seznam izvršilnih pooblastil, ki se lahko uporabijo za kršitve obveznosti glede ukrepov za obvladovanje tveganj za kibernetsko varnost in obveznosti poročanja iz te direktive ter vzpostaviti jasen in skladen okvir za tako izvrševanje po vsej Uniji. Ustrezno bi bilo treba upoštevati naravo, težo in trajanje kršitve te direktive, povzročeno premoženjsko ali nepremoženjsko škodo, ali je kršitev namerna ali posledica malomarnosti, ukrepe, sprejete za preprečevanje ali omilitev nastale premoženjske ali nepremoženjske škode, stopnjo odgovornosti ali vse zadevne predhodne kršitve, stopnjo sodelovanja s pristojnim organom in morebitne druge oteževalne ali olajševalne dejavnike. Izvršilni ukrepi, vključno z upravnimi globami, bi morali biti sorazmerni in za njihovo naložitev bi morali veljati ustrezni postopkovni zaščitni ukrepi v skladu s splošnimi načeli prava Unije in Listine Evropske unije o temeljnih pravicah (v nadaljevanju: Listina), vključno s pravico do učinkovitega pravnega sredstva in nepristranskega sodišča, domnevo nedolžnosti in pravico do obrambe.

(128) Ta direktiva od držav članic ne zahteva, naj določijo kazensko ali civilnopravno odgovornost v zvezi s fizičnimi osebami, ki so odgovorne za zagotavljanje, da subjekt ravna skladno s to direktivo za škodo, ki so jo zaradi kršitve te direktive utrpele tretje osebe.

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

(130) Kadar se upravne globe naložijo bistvenemu ali pomembnemu subjektu, ki je podjetje, 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 pristojni organ pri določanju ustreznega zneska te 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 za prenos ta direktive.

(131) Državam članicam bi moralo biti omogočeno, da določijo pravila o kazenskih sankcijah za kršitve nacionalnih pravil za prenos te direktive. 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 Evropske unije.

(132) Kadar ta direktiva ne zagotavlja harmonizacije upravnih sankcij ali po potrebi v drugih primerih, denimo v primerih hude kršitve te direktive, bi morale države članice uporabiti sistem, ki zagotavlja učinkovite, sorazmerne in odvračilne sankcije. Narava takšnih sankcij, in dejstvo, ali so kazenske ali upravne, bi morala biti določena z nacionalnim pravom.

(133) Za nadaljnjo krepitev učinkovitosti in odvračilnosti izvršilnih ukrepov, ki se uporabljajo za kršitve te direktive, bi morali biti pristojni organi pooblaščeni za začasen preklic ali zahtevo za uvedbo začasnega preklica certifikata ali dovoljenja za del ustreznih storitev ali vse ustrezne storitve, ki jih opravlja bistveni subjekt, in zahtevo za uvedbo začasne prepovedi opravljanja vodstvenih funkcij za fizično osebo, ki opravlja vodstvene funkcije na ravni glavnega izvršnega direktorja ali pravnega zastopnika. Glede na njihovo resnost in vpliv na dejavnosti subjektov ter končno na uporabnike bi se morali takšni začasni preklici ali prepovedi uporabljati le sorazmerno z resnostjo kršitve in ob upoštevanju posebnih okoliščin posameznega primera, vključno s tem, ali je kršitev namerna ali posledica malomarnosti, ter vseh ukrepov, sprejetih za preprečevanje ali ublažitev premoženjske ali nepremoženjske škode. Taki začasni preklici ali prepovedi bi se morali uporabljati le kot zadnje sredstvo, in sicer šele potem, ko so bili uporabljeni vsi drugi ustrezni izvršilni ukrepi, določeni v tej direktivi, in le dokler zadevni subjekt ne sprejme potrebnih ukrepov za odpravo pomanjkljivosti ali izpolnitev zahtev pristojnega organa, zaradi katerih so bili takšni začasni preklici ali prepovedi naloženi. Za uvedbo takšnega začasnega preklica ali prepovedi bi morali veljati ustrezni postopkovni zaščitni ukrepi v skladu s splošnimi načeli prava Unije in Listine, vključno s pravico do učinkovitega pravnega sredstva in nepristranskega sodišča, domnevo nedolžnosti in pravico do obrambe.

(134) Da bi se zagotovilo, da subjekti izpolnjujejo svoje obveznosti, določene v tej direktivi, bi morale države članice sodelovati in si pomagati v zvezi z nadzornimi in izvršilnimi ukrepi, zlasti kadar subjekt opravlja storitve v več kot eni državi članici ali kadar se njegovi omrežni in informacijski sistemi nahajajo v državi članici, ki ni država članica, v kateri opravlja storitve. Zaprošeni pristojni organ bi moral pri zagotavljanju pomoči sprejeti nadzorne ali izvršilne ukrepe v skladu z nacionalnim pravom. Za zagotovitev nemotenega delovanja medsebojne pomoči na podlagi te direktive bi morali pristojni organi uporabiti skupino za sodelovanje kot forum za razpravo o zadevah in posebnih prošnjah za pomoč.

(135) Za zagotovitev učinkovitega nadzora in izvrševanja, zlasti v primeru s čezmejno razsežnostjo, bi morale države članice, ki so prejele prošnjo za medsebojno pomoč, kolikor je to del prošnje, sprejeti ustrezne nadzorne in izvršilne ukrepe v zvezi z zadevnim subjektom, ki opravlja storitve ali ima omrežni in informacijski sistem na njihovem ozemlju.

(136) V tej direktivi bi bilo treba določiti pravila sodelovanja med pristojnimi in nadzornimi organi iz Uredbe (EU) 2016/679 za obravnavanje kršitev te direktive, povezanih z osebnimi podatki.

(137) Ta direktiva bi morala biti namenjena zagotavljanju visoke ravni odgovornosti za ukrepe za obvladovanje tveganj za kibernetsko varnost in obveznosti poročanja na ravni bistvenih in pomembnih subjektov. Zato bi morali upravljalni organi bistvenih in pomembnih subjektov odobriti ukrepe za obvladovanje tveganj za kibernetsko varnost in nadzorovati njihovo izvajanje.

(138) Za zagotovitev visoke skupne ravni kibernetske varnosti po vsej Uniji na podlagi te direktive bi bilo treba na Komisijo prenesti pooblastilo, da v skladu s členom 290 PDEU sprejeme akte v zvezi z dopolnitvijo te direktive z določitvijo, za katere kategorije bistvenih in pomembnih subjektov je treba uporabiti nekatere certificirane proizvode IKT, storitve IKT in postopke IKT ali pridobiti certifikat v okviru evropske certifikacijske sheme za kibernetsko varnost. Zlasti je pomembno, da se Komisija pri svojem pripravljalnem delu ustrezno posvetuje, vključno na ravni strokovnjakov, in da se ta posvetovanja izvedejo v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje ([22]). Za zagotovitev enakopravnega sodelovanja pri pripravi delegiranih aktov Evropski parlament in Svet zlasti prejmeta vse dokumente sočasno s strokovnjaki iz držav članic, njuni strokovnjaki pa se sistematično lahko udeležujejo sestankov strokovnih skupin Komisije, ki zadevajo pripravo delegiranih aktov.

([22]) UL L 123, 12.5.2016, str. 1.

(139) Za zagotovitev enotnih pogojev izvajanja te direktive, bi bilo treba na Komisijo prenesti izvedbena pooblastila, da določi postopkovne ureditve, potrebne za delovanje skupine za sodelovanje, ter tehnične, metodične in sektorske zahteve v zvezi z ukrepi za obvladovanje tveganj na področju kibernetske varnosti ter dodatno opredeli vrste informacij, oblike in postopki priglasitve incidentov, kibernetskih groženj in skorajšnjih incidentov ter obveščanja o pomembnih kibernetskih grožnjah in kdaj se incident šteje za pomembnega. Ta pooblastila bi bilo treba izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta ([23]).

(140) Komisija bi morala redno po posvetovanju z deležniki pregledovati to direktivo, zlasti da bi ugotovila, ali je treba predlagati spremembe ob upoštevanju družbenih, političnih, tehnoloških ali tržnih razmer. V okviru teh pregledov bi morala Komisija oceniti pomen velikosti zadevnih subjektov, sektorjev, podsektorjev in vrste subjektov iz prilog k tej direktivi za delovanje gospodarstva in družbe v zvezi s kibernetsko varnostjo. Komisija bi morala med drugim oceniti, ali je ponudnike, ki spadajo na področje uporabe te direktive, ki so imenovani kot zelo velike spletne platforme v smislu člena 33 Uredbe (EU) 2022/2065 Evropskega parlamenta in Sveta ([24]), mogoče identificirati kot bistvene subjekte na podlagi te direktive.

(141) Ta direktiva ENISA nalaga nove naloge, s čimer bi se okrepila njena vloga, lahko pa bi tudi povzročila, da bi morala ENISA svoje obstoječe naloge v skladu z Uredbo (EU) 2019/881 izvajati na višji ravni kot prej. Da bi se ENISA zagotovili potrebni finančni in človeški viri za izvajanje obstoječih in novih nalog ter za izpolnjevanje vsakršnih višjih standardov izvajanja teh nalog, ki izhajajo iz njene okrepljene vloge, bi bilo treba njen proračun ustrezno povečati. Poleg tega bi bilo treba za zagotavljanje učinkovite rabe sredstev ENISA omogočiti večjo prožnost pri omogočanju notranjega razporejanja sredstev, da bi lahko učinkovito opravljala svoje naloge in izpolnila pričakovanja.

(142) Ker cilja te direktive, in sicer doseganja visoke skupne ravni kibernetske varnosti po vsej 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 iz navedenega člena ta direktiva ne presega tistega, kar je potrebno za doseganje navedenega cilja.

(143) Ta direktiva upošteva temeljne pravice in načela iz Listine, zlasti pravico do spoštovanja zasebnega življenja in komunikacij, varstvo osebnih podatkov, svobodo gospodarske pobude, lastninsko pravico, pravico do učinkovitega pravnega sredstva in pravičnega sojenja, domnevo nedolžnosti ter pravico do obrambe. Pravica do učinkovitega pravnega sredstva zajema prejemnike storitev, ki jih zagotavljajo bistveni in pomembni subjekti. To direktivo bi bilo treba izvajati v skladu s temi pravicami in načeli.

(144) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta ([25]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 11. marca 2021 ([26]) –

([23]) 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).

([24]) Uredba (EU) 2022/2065 Evropskega parlamenta in Sveta z dne 19. oktobra 2022 o enotnem trgu digitalnih storitev in spremembi Direktive 2000/31/ES (akt o digitalnih storitvah) (UL L 277, 27.10.2022 , str. 1).

([25]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).

([26]) UL C 183, 11.5.2021, str. 3.

SPREJELA NASLEDNJO DIREKTIVO:

POGLAVJE I

SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja

1. Ta direktiva določa ukrepe, katerih cilj je zagotoviti visoko skupno raven kibernetske varnosti v Uniji, da bi se izboljšalo delovanje notranjega trga.

2. V ta namen ta direktiva določa:

(a) obveznosti, ki od držav članic zahtevajo, da sprejmejo nacionalne strategije za kibernetsko varnost in imenujejo ali ustanovijo pristojne organe, organe za obvladovanje kibernetskih kriz, enotne kontaktne točke za kibernetsko varnost (v nadaljnjem besedilu: enotne kontaktne točke) in skupine za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT);

(b) ukrepe za obvladovanja tveganj za kibernetsko varnost in obveznosti poročanja za subjekte vrste iz Priloge I ali II, kot tudi za subjekte, ki so identificirani kot kritični subjekti na podlagi Direktive (EU) 2022/2557;

(c) pravila in obveznosti glede izmenjave informacij o kibernetski varnosti;

(d) obveznosti nadzora in izvrševanja za države članice.

Člen 2

Področje uporabe

1. Ta direktiva se uporablja za javne ali zasebne subjekte vrste iz Priloge I ali II, ki izpolnjujejo pogoje za srednja podjetja iz člena 2 Priloge k Priporočilu 2003/361/ES, ali presegajo zgornje meje za srednja podjetja, določene v odstavku 1 navedenega člena, in ki opravljajo svoje storitve ali izvajajo svoje dejavnosti v Uniji.

Člen 3(4) Priloge k navedenemu priporočilu se ne uporablja za namene te direktive.

2. Ta direktiva se uporablja tudi za subjekte vrste iz Priloge I ali II ne glede na njihovo velikost, kadar:

(a) storitve opravljajo:

  (i) ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev;

  (ii) ponudniki storitev zaupanja;

  (iii) registri vrhnjih domenskih imen in ponudniki storitev sistema domenskih imen;

(b) je subjekt edini ponudnik storitve, ki je bistvena za ohranjanje kritičnih družbenih ali gospodarskih dejavnosti, v državi članici;

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

(d) bi motnja pri opravljanju storitve subjekta lahko povzročila pomembno sistemsko tveganje, zlasti za sektorje, v katerih bi lahko taka motnja imela čezmejni vpliv;

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

(f) gre za subjekt javne uprave:

(i) na osrednji državni ravni, kot ga opredeli država članica v skladu z nacionalnim pravom, ali

(ii) na regionalni ravni, kot ga opredeli država članica v skladu z nacionalnim pravom, in ki po oceni tveganja opravlja storitve, katerih motnje bi lahko pomembno vplivale na ključne družbene ali gospodarske dejavnosti.

3. Ta direktiva se uporablja tudi za subjekte, ki so identificirani kot kritični na podlagi Direktive (EU) 2022/2557, ne glede na njihovo velikost.

4. Ta direktiva se uporablja tudi za subjekte, ki opravljajo storitve registracije domenskih imen, ne glede na njihovo velikost.

5. Države članice lahko določijo, da se ta direktiva uporablja za:

(a) subjekte javne uprave na lokalni ravni;

(b) izobraževalne ustanove, zlasti kadar izvajajo kritične raziskovalne dejavnosti.

6. Ta direktiva ne posega v pristojnosti držav članic, da zaščitijo nacionalno varnost, in v njihova pooblastila za zaščito drugih bistvenih državnih funkcij, vključno z zagotavljanjem ozemeljske celovitosti države ter vzdrževanjem javnega reda in miru.

7. Ta direktiva se ne uporablja za subjekte javne uprave, ki izvajajo svoje dejavnosti na področju nacionalne varnosti, javne varnosti, obrambe ali kazenskega pregona, vključno s preprečevanjem, preiskovanjem, odkrivanjem in pregonom kaznivih dejanj.

8. Države članice lahko določene subjekte, ki izvajajo dejavnosti na področjih nacionalne varnosti, javne varnosti, obrambe ali kazenskega pregona, vključno s preprečevanjem, preiskovanjem, odkrivanjem in pregonom kaznivih dejanj, ali ki opravljajo storitve izključno za subjekte javne uprave iz odstavka 7 tega člena, izvzamejo iz obveznosti iz člena 21 ali 23 v zvezi s temi dejavnostmi ali storitvami. V takih primerih se nadzorni in izvršilni ukrepi iz poglavja VII ne uporabljajo v zvezi s temi posebnimi dejavnostmi ali storitvami. Kadar subjekti izvajajo dejavnosti ali opravljajo storitve, ki so izključno take vrste, kot je navedena v tem odstavku, se lahko države članice odločijo, da tudi te subjekte izvzamejo iz obveznosti iz členov 3 in 27.

9. Odstavka 7 in 8 se ne uporabljata, kadar subjekt deluje kot ponudnik storitev zaupanja.

10. Ta direktiva se ne uporablja za subjekte, ki so jih države članice izvzele s področja uporabe Uredbe (EU) 2022/2554 v skladu s členom 2(4) navedene uredbe.

11. Obveznosti iz te direktive ne vključujejo posredovanja informacij, katerih razkritje bi bilo v nasprotju z bistvenimi interesi držav članic na področju nacionalne varnosti, javne varnosti ali obrambe.

12. Ta direktiva se uporablja brez poseganja v Uredbo (EU) 2016/679, Direktivo 2002/58/ES, direktivi 2011/93/EU ([27]) in 2013/40/EU ([28]) Evropskega parlamenta in Sveta ter Direktivo (EU) 2022/2557.

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

([27]) 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).

([28]) 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).

14. Subjekti, pristojni organi, enotne kontaktne točke in skupine CSIRT obdelujejo osebne podatke v obsegu, ki je potreben za namene te direktive, in v skladu z Uredbo (EU) 2016/679, pri čemer mora taka obdelava zlasti temeljiti na členu 6 Uredbe.

Kar zadeva obdelavo osebnih podatkov na podlagi te direktive, jo morajo ponudniki javnih elektronskih komunikacijskih omrežij ali ponudniki javno dostopnih elektronskih komunikacijskih storitev izvajati v skladu s pravom Unije o varstvu podatkov in pravom Unije o zasebnosti, zlasti z Direktivo 2002/58/ES.

Člen 3

Bistveni in pomembni subjekti

1. Za namene te direktive se šteje, da so bistveni subjekti:

(a) subjekti vrste iz Priloge I, ki presegajo zgornje meje za srednja podjetja, določene v členu 2(1) Priloge k Priporočilu 2003/361/ES;

(b) ponudniki kvalificiranih storitev zaupanja in registri vrhnjih domenskih imen ter ponudniki storitev DNS, ne glede na njihovo velikost;

(c) ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, ki se štejejo za srednja podjetja na podlagi člena 2 Priloge k Priporočilu 2003/361/ES;

(d) subjekti javne uprave iz člena 2(2), točka (f)(i);

(e) vsi drugi subjekti vrste iz Priloge I ali II, ki jih država članica identificira kot bistvene subjekte na podlagi člena 2(2), točke (b) do (e);

(f) subjekti, identificirani kot kritični subjekti na podlagi Direktive (EU) 2022/2557, iz člena 2(3) te direktive;

(g) če država članica tako določi, subjekti, ki jih je ta država članica pred 16. januarjem 2023 določila kot izvajalce bistvenih storitev v skladu z Direktivo (EU) 2016/1148 ali nacionalnim pravom.

2. Za namene te direktive se subjekti vrste iz Priloge I ali II, ki se ne štejejo za bistvene subjekte na podlagi odstavka 1 tega člena, štejejo za pomembne subjekte. To vključuje subjekte, ki jih država članica identificira kot pomembne subjekte na podlagi člena 2(2), točke (b) do (e).

3. Države članice do 17. aprila 2025 oblikujejo seznam bistvenih in pomembnih subjektov ter subjektov, ki opravljajo storitve registracije domenskih imen. Države članice ta seznam redno oziroma vsaj vsaki dve leti pregledajo in ga po potrebi posodobijo.

4. Za namene priprave seznama iz odstavka 3 države članice od subjektov iz navedenega odstavka zahtevajo, da pristojnim organom predložijo vsaj naslednje informacije:

(a) ime subjekta;

(b) naslov in ažurne kontaktne podatke, vključno z elektronskimi naslovi, dodeljenimi bloki naslovov IP in telefonskimi številkami;

(c) po potrebi ustrezen sektor in podsektor iz Priloge I ali II ter

(d) po potrebi seznam držav članic, v katerih opravljajo storitve, ki spadajo na področje uporabe te direktive.

Subjekti iz odstavka 3 nemudoma sporočijo morebitne spremembe podatkov, ki so jih predložili na podlagi prvega pododstavka tega odstavka, v vsakem primeru pa v dveh tednih od datuma spremembe.

V ta namen bi morala Komisija ob pomoči Agencije Evropske unije za kibernetsko varnost (ENISA) brez nepotrebnega odlašanja določiti smernice in obrazce v zvezi z obveznostmi, določenimi v tem odstavku.

Države članice lahko vzpostavijo nacionalne mehanizme za samoregistracijo subjektov.

5. Pristojni organi do 17. aprila 2025 in nato vsaki dve leti uradno obvestijo:

(a) Komisijo in skupino za sodelovanje o številu bistvenih in pomembnih subjektov, ki so na seznamu na podlagi odstavka 3, za vsak sektor in podsektor iz Priloge I ali II ter

(b) Komisijo o ustreznih informacijah o številu bistvenih in pomembnih subjektov, identificiranih na podlagi člena 2(2), točke (b) do (e), sektorju in podsektorju iz Priloge I ali II, ki jim pripadajo, vrsti storitev, ki jih opravljajo, ter opravljanju storitev iz člena 2(2), točke (b) do (e), na podlagi katerih so bili identificirani.

6. Države članice lahko do 17. aprila 2025 Komisiji na njeno zahtevo uradno sporočijo imena bistvenih in pomembnih subjektov iz odstavka 5, točka (b).

Člen 4

Sektorski pravni akti Unije

1. Kadar se s sektorskimi pravnimi akti Unije zahteva, da bistveni ali pomembni subjekti bodisi sprejmejo ukrepe za obvladovanje tveganj za kibernetsko varnost bodisi priglasijo pomembne incidente, in kadar so takšne zahteve po učinku vsaj enakovredne obveznostim iz te direktive, se ustrezne določbe te direktive, vključno z določbami o nadzoru in izvrševanju iz poglavja VII, za take subjekte ne uporabljajo. Kadar sektorski pravni akti Unije ne zajemajo vseh subjektov v določenem sektorju, ki spadajo na področje uporabe te direktive, se ustrezne določbe te direktive še naprej uporabljajo za subjekte, ki niso zajeti v sektorskih pravnih aktih Unije.

2. Zahteve iz odstavka 1 tega člena se štejejo za enakovredne obveznostim iz te direktive, kadar:

(a) imajo ukrepi za obvladovanje tveganj za kibernetsko varnost vsaj enakovreden učinek kot ukrepi iz člena 21(1) in (2) ali

(b) sektorski pravni akt Unije določa takojšen, po potrebi samodejen in neposreden, dostop do priglasitev incidentov za skupine CSIRT, pristojne organe ali enotne kontaktne točke iz te direktive, in kadar so zahteve za priglasitev pomembnih incidentov po učinku vsaj enakovredne tistim iz člena 23(1) do (6) te direktive.

3. Komisija do 17. julija 2023 določi smernice o uporabi odstavkov 1 in 2. Komisija te smernice redno pregleduje. Komisija pri pripravi teh smernic upošteva vsa opažanja skupine za sodelovanje in ENISA.

Člen 5

Minimalna harmonizacija

Ta direktiva državam članicam ne preprečuje, da sprejmejo ali ohranijo določbe, ki zagotavljajo višjo raven kibernetske varnosti, pod pogojem, da so take določbe v skladu z obveznostmi držav članic, določenimi v pravu Unije.

Člen 6

Opredelitev pojmov

V tej direktivi se uporabljajo naslednje opredelitve pojmov:

(1) „omrežni in informacijski sistem“ pomeni:

(a) elektronsko komunikacijsko omrežje, kot je opredeljeno v členu 2, točka 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, ali

(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 omrežnih in informacijskih sistemov“ pomeni zmožnost omrežnih in informacijskih sistemov, da na določeni ravni zaupanja preprečijo vsak dogodek, ki lahko ogrozi razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki jih ti omrežni in informacijski sistemi zagotavljajo ali so prek njih dostopni;

(3) „kibernetska varnost“ pomeni kibernetsko varnost, kot je opredeljena v členu 2, točka 1, Uredbe (EU) 2019/881;

(4) „nacionalna strategija za kibernetsko varnost“ pomeni skladen okvir države članice, ki določa strateške cilje in prednostne naloge na področju kibernetske varnosti in upravljanja za njihovo uresničitev v tej državi članici;

(5) „skorajšnji incident“ pomeni dogodek, ki bi lahko ogrozil razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki jih omrežni in informacijski sistemi zagotavljajo ali so prek njih dostopni, vendar se je uspešno preprečilo, da bi se ta dogodek uresničil, ali se ni uresničil;

(6) „incident“ pomeni dogodek, ki ogroža razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki jih ti omrežni in informacijski sistemi zagotavljajo ali so prek njih dostopni;

(7) „incident velikih razsežnosti“ pomeni incident, ki povzroči motnjo, ki presega zmožnost države članice za odziv nanj, ali incident, ki pomembno vpliva na vsaj dve državi članici;

(8) „obvladovanje incidentov“ pomeni vsa dejanja in postopke, namenjene preprečevanju, odkrivanju, analizi in zajezitvi incidentov ali odzivanju nanje in okrevanju po njih;

(9) „tveganje“ pomeni možnost izgube ali motnje zaradi incidenta ter je izraženo kot kombinacija razsežnosti izgube ali motnje in verjetnosti, da bi do incidenta prišlo;

(10) „kibernetska grožnja“ pomeni kibernetsko grožnjo, kot je opredeljena v členu 2, točka 8, Uredbe (EU) 2019/881;

(11) „pomembna kibernetska grožnja“ pomeni kibernetsko grožnjo, za katero se glede na njene tehnične značilnosti lahko domneva, da bi lahko resno vplivala na omrežne in informacijske sisteme subjekta ali na uporabnike njegovih storitev tako da bi povzročila znatno premoženjsko ali nepremoženjsko škodo;

(12) „proizvod IKT“ pomeni proizvod IKT, kot je opredeljen v členu 2, točka 12, Uredbe (EU) 2019/881;

(13) „storitev IKT“ pomeni storitev IKT, kot je opredeljena v členu 2, točka 13, Uredbe (EU) 2019/881;

(14) „postopek IKT“ pomeni postopek IKT, kot je opredeljen v členu 2, točka 14, Uredbe (EU) 2019/881;

(15) „ranljivost“ pomeni pomanjkljivost, dovzetnost ali napako proizvoda IKT ali storitve IKT, ki jo kibernetska grožnja lahko izkoristi;

(16) „standard“ pomeni standard, kot je opredeljen v členu 2, točka 1, Uredbe (EU) št. 1025/2012 Evropskega parlamenta in Sveta ([29]);

(17) „tehnična specifikacija“ pomeni tehnično specifikacijo, kot je opredeljena v členu 2, točka 4, Uredbe (EU) št. 1025/2012;

([29]) 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).

(18) „stičišče omrežij“ pomeni omrežno zmogljivost, ki omogoča medsebojno povezavo več kot dveh neodvisnih omrežij (avtonomnih sistemov), predvsem zaradi izmenjave internetnega prometa, ki zagotavlja medsebojno povezavo zgolj avtonomnim sistemom in ki ne zahteva, da izmenjava internetnega prometa med katerima koli sodelujočima avtonomnima sistemoma prehaja prek tretjega avtonomnega sistema, in ne spreminja takšnega prometa ali kako drugače posega vanj;

(19) „sistem domenskih imen“ ali „DNS“ pomeni hierarhično porazdeljen sistem dodeljevanja imen, ki omogoča identifikacijo internetnih storitev in virov ter napravam končnih uporabnikov omogoča, da z uporabo internetnih storitev usmerjanja in povezljivosti dostopajo do teh storitev in virov;

(20) „ponudnik storitev DNS“ pomeni subjekt, ki opravlja:

(a) javno dostopne storitve rekurzivnega razreševanja domenskih imen za končne uporabnike interneta ali

(b) storitve avtoritativnega razreševanja domenskih imen za uporabo s strani tretjih oseb, razen za korenske imenske strežnike;

(21) „register vrhnjih domenskih imen“ ali „register TLD imen“ pomeni subjekt, ki mu je bila dodeljena določena vrhnja domena in je odgovoren za njeno upravljanje, 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 datotek območij vrhnje domene po imenskih strežnikih, ne glede na to, ali katero od teh dejavnosti subjekt izvaja sam ali jo izvajajo zunanji izvajalci, izključeni pa so primeri, v katerih register TLD imen uporablja vrhnja domenska imena zgolj za lastne potrebe;

(22) „subjekt, ki opravlja storitve registracije domenskih imen“ pomeni registratorja ali zastopnika, ki deluje v imenu registratorja, kot je ponudnik storitev registracije za zasebnost ali pooblaščenec ali preprodajalec;

(23) „digitalna storitev“ pomeni storitev, kot je opredeljena v členu 1(1), točka (b), Direktive (EU) 2015/1535 Evropskega parlamenta in Sveta ([30]);

(24) „storitev zaupanja“ pomeni storitev zaupanja, kot je opredeljena v členu 3, točka 16, Uredbe (EU) št. 910/2014;

(25) „ponudnik storitev zaupanja“ pomeni ponudnika storitev zaupanja, kot je opredeljen v členu 3, točka 19, Uredbe (EU) št. 910/2014;

(26) „kvalificirana storitev zaupanja“ pomeni kvalificirano storitev zaupanja, kot je opredeljena v členu 3, točka 17, Uredbe (EU) št. 910/2014;

(27) „ponudnik kvalificiranih storitev zaupanja“ pomeni ponudnika kvalificiranih storitev zaupanja, kot je opredeljen v členu 3, točka 20, Uredbe (EU) št. 910/2014;

(28) „spletna tržnica“ pomeni spletno tržnico, kot je opredeljena v členu 2, točka (n), Direktive 2005/29/ES Evropskega parlamenta in Sveta ([31]);

(29) „spletni iskalnik“ pomeni spletni iskalnik, kot je opredeljen v členu 2, točka 5, Uredbe (EU) 2019/1150 Evropskega parlamenta in Sveta ([32]);

(30) „storitev v oblaku“ pomeni digitalno storitev, ki omogoča upravljanje na zahtevo in širok oddaljeni dostop do prožnega in po obsegu prilagodljivega nabora deljivih računalniških virov, tudi kadar so ti viri porazdeljeni na več lokacijah;

([30]) 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).

([31]) 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).

([32]) 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).

(31) „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;

(32) „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;

(33) „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;

(34) „predstavnik“ pomeni fizično ali pravno osebo s sedežem v Uniji, ki je izrecno imenovana, da deluje v imenu ponudnika storitev DNS, registra TLD imen, subjekta, ki opravlja storitve registracije domenskih imen, ponudnika storitev računalništva v oblaku, ponudnika storitev podatkovnega centra, ponudnika omrežja za dostavo vsebine, ponudnika upravljanih storitev, ponudnika upravljanih varnostnih storitev ali ponudnika spletne tržnice, spletnega iskalnika ali platforme za storitve družbenega mreženja, ki nima sedeža v Uniji, s katerim lahko pristojni organ ali skupina CSIRT vzpostavi stik namesto s samim subjektom, kar zadeva obveznosti tega subjekta na podlagi te direktive;

(35) „subjekt javne uprave“ pomeni subjekt, ki je v državi članici v skladu z nacionalnim pravom priznan kot tak, razen sodstva, parlamentov ali centralnih bank, in ki izpolnjuje naslednja merila:

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

(b) je pravna oseba ali ima po zakonu pravico delovati v imenu drugega subjekta, ki je pravna oseba;

(c) pretežno ga financirajo država, regionalni organi ali druge osebe javnega prava, njegovo upravljanje nadzorujejo ti organi ali osebe ali pa ima upravni, upraviteljski ali nadzorni odbor, v 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;

(36) „javno elektronsko komunikacijsko omrežje“ pomeni javno elektronsko komunikacijsko omrežje, kot je opredeljeno v členu 2, točka 8, Direktive (EU) 2018/1972;

(37) „elektronska komunikacijska storitev“ pomeni elektronsko komunikacijsko storitev, kot je opredeljena v členu 2, točka 4, Direktive (EU) 2018/1972;

(38) „subjekt“ pomeni 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;

(39) „ponudnik upravljanih storitev“ pomeni subjekt, ki opravlja storitve v zvezi z namestitvijo, upravljanjem, delovanjem ali vzdrževanjem izdelkov, omrežij, infrastrukture, aplikacij IKT ali katerih koli drugih omrežnih in informacijskih sistemov, in sicer s pomočjo ali aktivnim upravljanjem, ki se izvaja bodisi v prostorih strank bodisi na daljavo;

(40) „ponudnik upravljanih varnostnih storitev“ pomeni ponudnika upravljanih storitev, ki izvaja ali opravlja pomoč za dejavnosti, povezane z obvladovanjem tveganj za kibernetsko varnost;

(41) „raziskovalna organizacija“ pomeni subjekt, katerega glavni cilj je izvajati uporabne raziskave ali eksperimentalni razvoj z namenom uporabe rezultatov teh raziskav v komercialne namene, vendar ne vključuje izobraževalnih ustanov.

POGLAVJE II

USKLAJENI OKVIRI ZA KIBERNETSKO VARNOST

Člen 7

Nacionalna strategija za kibernetsko varnost

1. Vsaka država članica sprejme nacionalno strategijo za kibernetsko varnost, v kateri so opredeljeni strateški cilji, potrebna sredstva za dosego teh ciljev ter ustrezni ukrepi politike in regulativni ukrepi za doseganje in ohranjanje visoke ravni kibernetske varnosti. V nacionalno strategijo za kibernetsko varnost se vključijo:

(a) cilji in prednostne naloge strategije držav članic za kibernetsko varnost, ki zajemajo zlasti sektorje iz prilog I in II;

(b) okvir upravljanja za doseganje ciljev in prednostnih nalog iz točke (a) tega odstavka, vključno s politikami iz odstavka 2;

(c) okvir upravljanja, ki pojasnjuje vloge in odgovornosti ustreznih zainteresiranih strani na nacionalni ravni ter podpira sodelovanje in usklajevanje na nacionalni ravni med pristojnimi organi, enotnimi kontaktnimi točkami in skupinami CSIRT iz te direktive, pa tudi usklajevanje in sodelovanje med temi organi in pristojnimi organi na podlagi sektorskih pravnih aktov Unije;

(d) mehanizem za opredelitev ustreznih sredstev in oceno tveganj v zadevni državi članici;

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

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

(g) okvir politike za okrepljeno usklajevanje med pristojnimi organi iz te direktive in pristojnimi organi iz Direktive (EU) 2022/2557 za namene izmenjave informacij o tveganjih, kibernetskih grožnjah in incidentih ter o nekibernetskih tveganjih, grožnjah in incidentih ter izvajanju nadzornih nalog, kot je ustrezno;

(h) načrt, vključno s potrebnimi ukrepi, za povečanje splošne ozaveščenosti državljanov o kibernetski varnosti.

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

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

(b) o vključitvi in specifikaciji zahtev za proizvode IKT in storitve IKT pri javnem naročanju, povezanih s kibernetsko varnostjo, vključno v zvezi s certificiranjem kibernetske varnosti, šifriranjem in uporabo odprtokodnih proizvodov za kibernetsko varnost;

(c) obvladovanja ranljivosti, vključno s spodbujanjem in omogočanjem usklajenega razkrivanja ranljivosti na podlagi člena 12(1);

(d) povezane z ohranjanjem splošne razpoložljivosti, celovitosti in zaupnosti javnega jedra odprtega interneta, vključno, kadar je to ustrezno, s kibernetsko varnostjo podmorskih komunikacijskih kablov;

(e) spodbujanja razvoja in vključevanja ustreznih naprednih tehnologij za izvajanje najsodobnejših ukrepov za obvladovanje tveganj na področju kibernetske varnosti;

(f) spodbujanja in razvoja izobraževanja in usposabljanja na področju kibernetske varnosti, spretnosti na področju kibernetske varnosti, dviganja ozaveščanja ter raziskovalnih in razvojnih pobud na področju kibernetske varnosti ter smernic o dobrih praksah in nadzoru kibernetske higiene, namenjenih državljanom, deležnikom in subjektom;

(g) podpiranja akademskih in raziskovalnih institucij pri razvoju, izboljševanju in spodbujanju uvajanja orodij kibernetske varnosti in varne omrežne infrastrukture;

(h) vključevanja ustreznih postopkov in primernih orodij za izmenjavo informacij za podpiranje prostovoljne izmenjave informacij o kibernetski varnosti med subjekti v skladu s pravom Unije;

(i) krepitve kibernetske odpornosti in osnovne kibernetske higiene malih in srednjih podjetij, zlasti tistih, ki so izključena s področja uporabe te direktive, z zagotavljanjem lahko dostopnih smernic in pomoči za njihove posebne potrebe;

(j) spodbujanja aktivne kibernetske zaščite.

3. Države članice Komisiji uradno sporočijo svoje nacionalne strategije za kibernetsko varnost v treh mesecih od njihovega sprejetja. Države članice lahko iz teh uradnih sporočil izključijo informacije, ki se nanašajo na njihovo nacionalno varnost.

4. Države članice redno in vsaj vsakih pet let ocenijo svoje nacionalne strategije za kibernetsko varnost na podlagi ključnih kazalnikov uspešnosti in jih po potrebi posodobijo. ENISA državam članicam na njihovo zahtevo pomaga pri razvoju ali posodabljanju nacionalne strategije za kibernetsko varnost in ključnih kazalnikov uspešnosti za oceno te strategije, da bi se uskladila z zahtevami in obveznostmi iz te direktive.

Člen 8

Pristojni organi in enotne kontaktne točke

1. Vsaka država članica imenuje ali ustanovi enega ali več pristojnih organov, odgovornih za kibernetsko varnost in nadzorne naloge iz poglavja VII (v nadaljnjem besedilu: pristojni organi).

2. Pristojni organi iz odstavka 1 spremljajo izvajanje te direktive na nacionalni ravni.

3. Vsaka država članica določi ali vzpostavi enotno kontaktno točko. Kadar država članica na podlagi odstavka 1 imenuje ali ustanovi le en pristojni organ, je ta organ 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 in, kadar je to ustrezno, Komisijo in ENISA ter medsektorsko sodelovanje z drugimi pristojnimi nacionalnimi organi v svoji državi članici.

5. Države članice zagotovijo, da imajo njihovi pristojni organi in enotne kontaktne točke ustrezna sredstva, da učinkovito in uspešno opravljajo dodeljene naloge ter tako izpolnjujejo cilje te direktive.

6. Vsaka država članica Komisijo brez nepotrebnega odlašanja uradno obvesti o identiteti pristojnega organa iz odstavka 1 in enotne kontaktne točke iz odstavka 3, njunih nalogah in o vseh naknadnih spremembah v zvezi z njima. Vsaka država članica objavi identiteto pristojnega organa. Komisija seznam obstoječih enotnih kontaktnih točk naredi javno dostopen.

Člen 9

Nacionalni okviri za obvladovanje kibernetskih kriz

1. Vsaka država članica imenuje ali ustanovi enega ali več pristojnih organov, odgovornih za obvladovanje kibernetskih incidentov velikih razsežnosti in kriz (v nadaljnjem besedilu: organi za obvladovanje kibernetskih kriz). Države članice tem organom zagotovijo ustrezna sredstva za učinkovito in uspešno opravljanje nalog, ki so jim bile dodeljene. Države članice zagotovijo skladnost z obstoječimi splošnimi nacionalnimi okviri za obvladovanje kriz.

2. Kadar država članica na podlagi odstavka 1 imenuje ali ustanovi več kot en organ za obvladovanje kibernetskih kriz, jasno navede, kateri od njih bo koordinator za obvladovanje kibernetskih incidentov velikih razsežnosti in kriz.

3. Vsaka država članica določi zmogljivosti, sredstva in postopke, ki se lahko uporabijo v primeru krize za namene te direktive.

4. Vsaka država članica sprejme nacionalni načrt odzivanja na kibernetske incidente velikih razsežnosti in krize, v katerem so opredeljeni cilji in ureditve obvladovanja kibernetskih incidentov velikih razsežnosti in kriz. V tem načrtu se zlasti določijo:

(a) cilji nacionalnih ukrepov in dejavnosti za pripravljenost;

(b) naloge in odgovornosti organov za obvladovanje kibernetskih kriz;

(c) postopki za obvladovanje kibernetskih kriz, vključno z njihovo vključitvijo v splošni nacionalni okvir za obvladovanje kriz, in kanali za izmenjavo informacij;

(d) nacionalni ukrepi za pripravljenost, vključno z vajami in dejavnostmi usposabljanja;

(e) ustrezni javni in zasebni deležniki ter vključena infrastruktura;

(f) nacionalni postopki in ureditve med ustreznimi nacionalnimi organi za zagotovitev učinkovitega sodelovanja države članice pri usklajenem obvladovanju kibernetskih incidentov velikih razsežnosti in kriz na ravni Unije ter njegove podpore.

5. Vsaka država članica v treh mesecih po imenovanju ali ustanovitvi organa za obvladovanje kibernetskih kriz iz odstavka 1 Komisijo uradno obvesti o identiteti svojega organa in o vseh naknadnih spremembah v zvezi z njim. Države članice Komisiji in Evropski mreži organizacij za zvezo za kibernetske krize (v nadaljnjem besedilu: mreža EU-CyCLONe) predložijo ustrezne informacije v zvezi z zahtevami iz odstavka 4 o svojih nacionalnih načrtih za odzivanje na kibernetske incidente velikih razsežnosti in krize v treh mesecih od sprejetja teh načrtov. Države članice lahko informacije izključijo, kadar in kolikor je to potrebno za njihovo nacionalno varnost.

Člen 10

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

1. Vsaka država članica določi ali vzpostavi eno ali več skupin CSIRT. Skupine CSIRT se lahko imenujejo ali ustanovijo znotraj pristojnega organa. Skupine CSIRT morajo izpolnjevati zahteve iz člena 11(1), pokrivati vsaj sektorje, podsektorje in vrste subjektov iz prilog I in II ter so pristojne za obvladovanje incidentov v skladu z natančno določenim postopkom.

2. Države članice zagotovijo, da ima vsaka skupina CSIRT ustrezna sredstva za učinkovito izvajanje svojih nalog iz člena 11(3).

3. Države članice zagotovijo, da ima vsaka skupina CSIRT na voljo ustrezno, varno in odporno komunikacijsko in informacijsko infrastrukturo, prek katere izmenjuje informacije z bistvenimi in pomembnimi subjekti ter drugimi ustreznimi deležniki. V ta namen države članice zagotovijo, da vsaka skupina CSIRT prispeva k uvajanju orodij za varno izmenjavo informacij.

4. Skupine CSIRT sodelujejo in si, kadar je ustrezno, v skladu s členom 29 izmenjujejo ustrezne informacije s sektorskimi ali medsektorskimi skupnostmi bistvenih in pomembnih subjektov.

5. Skupine CSIRT sodelujejo pri medsebojnih strokovnih pregledih, organiziranih v skladu s členom 19.

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

7. Skupine CSIRT lahko vzpostavijo sodelovanje z nacionalnimi skupinami za odzivanje na incidente na področju računalniške varnosti iz tretjih držav. Države članice v okviru takšnih odnosov sodelovanja spodbujajo uspešno, učinkovito in varno izmenjavo informacij s temi nacionalnimi skupinami za odzivanje na računalniške varnostne incidente iz tretjih držav z uporabo ustreznih protokolov za izmenjavo informacij, vključno s protokolom semaforja. Skupine CSIRT si lahko izmenjujejo ustrezne informacije z nacionalnimi skupinami za odzivanje na incidente na področju računalniške varnosti iz tretjih držav, vključno z osebnimi podatki v skladu s pravom Unije o varstvu podatkov.

8. Skupine CSIRT lahko sodelujejo z nacionalnimi skupinami za odzivanje na incidente na področju računalniške varnosti iz tretjih držav ali enakovrednimi organi tretjih držav, zlasti za zagotavljanje pomoči na področju kibernetske varnosti.

9. Vsaka država članica Komisijo brez nepotrebnega odlašanja uradno obvesti o identiteti skupine CSIRT iz odstavka 1 tega člena in skupine CSIRT, ki je imenovana za koordinatorja na podlagi člena 12(1), njunih nalogah v povezavi z bistvenimi in pomembnimi subjekti, in o vseh naknadnih spremembah v zvezi z njima.

10. Države članice lahko pri oblikovanju skupin CSIRT zaprosijo za pomoč ENISA.

Člen 11

Zahteve, tehnične zmogljivosti in naloge skupin CSIRT

1. Skupine CSIRT izpolnjujejo naslednje zahteve:

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

(b) prostori 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 zagotovijo zaupnost in zanesljivost svojih dejavnosti;

(e) skupine CSIRT imajo dovolj osebja za zagotavljanje neprekinjene razpoložljivosti storitev, pri čemer zagotavljajo, da je to osebje ustrezno usposobljeno;

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

Skupine CSIRT lahko sodelujejo v mrežah za mednarodno sodelovanje.

2. Države članice zagotovijo, da imajo njihove skupine CSIRT skupno potrebne tehnične zmogljivosti za izvajanje nalog iz odstavka 3. Države članice zagotovijo, da se njihovim skupinam CSIRT dodelijo zadostna sredstva za zagotovitev ustreznega števila osebja, ki skupinam CSIRT omogoča razvoj njihovih tehničnih zmogljivosti.

3. Skupine CSIRT imajo naslednje naloge:

(a) spremljanje in analiziranje kibernetskih groženj, ranljivosti in incidentov na nacionalni ravni ter, na zahtevo, pomoč zadevnim bistvenim in pomembnim subjektom v zvezi s spremljanjem njihovih omrežnih in informacijskih sistemov v realnem času ali v skoraj realnem času;

(b) zagotavljanje zgodnjega opozarjanja, opozoril, obvestil in razširjanja informacij o kibernetskih grožnjah, ranljivostih in incidentih zadevnim bistvenim in pomembnim subjektom ter pristojnim organom in drugim ustreznim deležnikom, če je mogoče v skoraj realnem času;

(c) odzivanje na incidente in zagotavljanje pomoči zadevnim bistvenim in pomembnim subjektom, kadar je to potrebno;

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

(e) opravljanje, na zahtevo bistvenega ali pomembnega subjekta, proaktivnega pregleda omrežnih in informacijskih sistemov zadevnega subjekta, da se odkrijejo ranljivosti, ki bi lahko imele pomemben vpliv;

(f) sodelovanje v mreži skupin CSIRT in zagotavljanje medsebojne pomoči v skladu z zmožnostmi in pristojnostmi drugim članicam mreže skupin CSIRT na njihovo zahtevo;

(g) kadar je ustrezno, vlogo koordinatorja za namene postopka usklajenega razkrivanja ranljivosti iz člena 12(1);

(h) prispevek k uporabi orodij za varno izmenjavo informacij na podlagi člena 10(3).

Skupine CSIRT lahko izvajajo proaktivno in nevsiljivo pregledovanje javno dostopnih omrežnih in informacijskih sistemov bistvenih in pomembnih subjektov. Takšno pregledovanje se izvede za odkrivanje ranljivih ali nezanesljivo konfiguriranih omrežnih in informacijskih sistemov ter za obveščanje zadevnih subjektov. Takšno pregledovanje ne sme negativno vplivati na delovanje storitev subjektov.

Skupine CSIRT lahko pri izvajanju nalog iz prvega pododstavka prednostno razvrstijo nekatere naloge na podlagi pristopa, ki temelji na tveganju.

4. Skupine CSIRT za dosego ciljev te direktive sodelujejo z ustreznimi deležniki iz zasebnega sektorja.

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

(a) postopki obvladovanja incidentov;

(b) obvladovanjem kriz ter

(c) usklajenim razkrivanjem ranljivosti na podlagi člena 12(1).

Člen 12

Usklajeno razkrivanje ranljivosti in evropska podatkovna zbirka ranljivosti

1. Vsaka država članica eno od svojih skupin CSIRT imenuje za koordinatorja za usklajeno razkrivanje ranljivosti. Skupina CSIRT, ki je imenovana za koordinatorja, deluje kot zaupanja vredna posrednica, ki po potrebi olajšuje sodelovanje med fizično ali pravno osebo, ki poroča o ranljivostih, in proizvajalcem ali ponudnikom proizvodov IKT ali storitev IKT, ki naj bi zajemali ranljivost, in sicer na pobudo katere koli stranke. Naloge skupine CSIRT, ki je imenovana za koordinatorja, vključujejo:

(a) identifikacijo zadevnih subjektov in vzpostavitev stika z njimi;

(b) podpiranje fizičnih ali pravnih oseb, ki poročajo o ranljivosti, in

(c) pogajanja o časovnicah razkrivanja in obvladovanju ranljivosti, ki vplivajo na več subjektov.

Države članice zagotovijo, da lahko fizične ali pravne osebe, kadar to zahtevajo, skupini CSIRT, ki je imenovana za koordinatorja, ranljivosti poročajo anonimno. Skupina CSIRT, ki je imenovana za koordinatorja, zagotovi skrbno nadaljnje ukrepanje v zvezi s sporočenimi ranljivostmi in anonimnost fizične ali pravne osebe, ki je o ranljivosti poročala. Kadar bi lahko sporočena ranljivost pomembno vplivala na subjekte v več kot eni državi članici, skupina CSIRT, ki je imenovana za koordinatorja, vsake zadevne države članice po potrebi sodeluje z drugimi skupinami CSIRT, ki so imenovane za koordinatorke, v okviru mreže skupin CSIRT.

2. ENISA po posvetovanju s skupino za sodelovanje razvije in vzdržuje evropsko podatkovno zbirko ranljivosti. V ta namen ENISA vzpostavi in vzdržuje ustrezne informacijske sisteme, politike in postopke ter sprejme potrebne tehnične in organizacijske ukrepe, s katerimi zagotovi varnost in celovitost evropske podatkovne zbirke ranljivosti, zlasti z namenom omogočanja subjektom, ne glede na to, ali spadajo na področje uporabe te Direktive, ter njihovim dobaviteljem omrežnih in informacijskih sistemov, da prostovoljno razkrijejo in evidentirajo javno znane ranljivosti proizvodov IKT in storitev IKT. Vsem deležnikom se zagotovi dostop do informacij o ranljivostih v podatkovni zbirki ranljivosti. V podatkovno zbirko se vključijo:

(a) informacije, ki opisujejo ranljivost;

(b) prizadeti proizvodi IKT ali storitve IKT ter resnost ranljivosti v smislu okoliščin, v katerih jo je mogoče izkoristiti;

(c) razpoložljivost povezanih popravkov ter, če popravki niso na voljo, smernice, ki jih določijo pristojni organi ali skupine CSIRT, naslovljene na uporabnike proizvodov IKT in storitev IKT z ranljivostmi, o načinih za zmanjšanje tveganj, ki izhajajo iz razkritih ranljivosti.

Člen 13

Sodelovanje na nacionalni ravni

1. Kadar so pristojni organi, 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 njihove skupine CSIRT ali po potrebi njihovi pristojni organi prejmejo priglasitve pomembnih incidentov v skladu s členom 23 in incidentov, kibernetskih groženj in skorajšnjih incidentov v skladu s členom 30.

3. Države članice zagotovijo, da njihove skupine CSIRT ali po potrebi njihovi pristojni organi obvestijo njihove enotne kontaktne točke o priglasitvah incidentov, kibernetskih groženj in skorajšnjih incidentov v skladu s to direktivo.

4. Za zagotovitev učinkovitega opravljanja nalog in obveznosti pristojnih organov, enotnih kontaktnih točk in skupin CSIRT države članice v največji možni meri zagotovijo ustrezno sodelovanje med temi organi in organi kazenskega pregona, organi za varstvo podatkov, nacionalnimi organi iz Uredb (ES) št. 300/2008 in (EU) 2018/1139, nadzornimi organi iz Uredbe (EU) št. 910/2014, pristojnimi organi iz Uredbe (EU) 2022/2554, nacionalnimi regulativnimi organi v iz Direktive (EU) 2018/1972, pristojnimi organi iz Direktive (EU) 2022/2557 ter pristojnimi organi iz drugih sektorskih pravnih aktov Unije v tej državi članici.

5. Države članice zagotovijo, da njihovi pristojni organi iz te direktive in njihovi pristojni organi iz Direktive (EU) 2022/2557 redno sodelujejo in si izmenjujejo informacije o identifikaciji kritičnih subjektov, o tveganjih, kibernetskih grožnjah in incidentih, pa tudi o nekibernetskih tveganjih, grožnjah in incidentih, ki vplivajo na bistvene subjekte, ki so identificirani kot kritični subjekti na podlagi Direktive (EU) 2022/2557, ter o ukrepih, sprejetih v odziv na takšna tveganja, grožnje in incidente. Države članice tudi zagotovijo, da si njihovi pristojni organi iz te direktive in njihovi pristojni organi iz Uredbe (EU) št. 910/2014, Uredbe (EU) 2022/2554 in Direktive (EU) 2018/1972 redno izmenjujejo informacije, tudi o relevantnih incidentih in kibernetskih grožnjah.

6. Države članice s tehničnimi sredstvi poenostavijo poročanje za priglasitve iz členov 23 in 30.

POGLAVJE III

SODELOVANJE NA RAVNI UNIJE IN MEDNARODNI RAVNI

Člen 14

Skupina za sodelovanje

1. Za podpiranje in olajšanje strateškega sodelovanja ter izmenjave informacij med državami članicami, kot tudi za krepitev zaupanja, se ustanovi skupina za sodelovanje.

2. Skupina za sodelovanje opravlja svoje naloge na podlagi dvoletnih delovnih programov iz odstavka 7.

3. Skupino za sodelovanje sestavljajo predstavniki držav članic, Komisije in ENISA. Evropska služba za zunanje delovanje sodeluje pri dejavnostih skupine za sodelovanje kot opazovalka. Evropski nadzorni organi in pristojni organi iz Uredbe (EU) 2022/2554 lahko sodelujejo pri dejavnostih skupine za sodelovanje v skladu s členom 47(1) navedene uredbe.

Skupina za sodelovanje lahko k sodelovanju pri njenem delu po potrebi povabi Evropski parlament in predstavnike ustreznih deležnikov.

Komisija zagotovi sekretariat.

4. Skupina za sodelovanje ima naslednje naloge:

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

(b) zagotavljanje usmeritev pristojnim organom v zvezi z razvojem in izvajanjem politik za usklajeno razkrivanje ranljivosti iz člena 7(2), točka (c);

(c) izmenjava dobrih praks in informacij v zvezi z izvajanjem te direktive, vključno v zvezi s kibernetskimi grožnjami, incidenti, ranljivostmi, skorajšnjimi incidenti, pobudami za ozaveščanje, usposabljanjem, vajami ter znanji in spretnostmi, krepitvijo zmogljivosti, standardi in tehničnimi specifikacijami, pa tudi v zvezi z identifikacijo bistvenih in pomembnih subjektov na podlagi člena 2(2), točke (b) do (e);

(d) izmenjava nasvetov in sodelovanje s Komisijo pri nastajajočih pobudah politike na področju kibernetske varnosti in splošne skladnosti sektorskih zahtev glede kibernetske varnosti;

(e) izmenjava nasvetov in sodelovanje s Komisijo pri pripravi osnutkov delegiranih ali izvedbenih aktov, sprejetih na podlagi te direktive;

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

(g) izmenjava mnenj o izvajanju sektorskih pravnih aktov Unije, ki vsebujejo določbe o kibernetski varnosti;

(h) po potrebi obravnavanje poročil o medsebojnih strokovnih pregledih iz člena 19(9) ter priprava ugotovitev in priporočil;

(i) izvajanje usklajenih ocen tveganja za varnost za kritične dobavne verige v skladu s členom 22(1);

(j) obravnavanje primerov medsebojne pomoči, tudi izkušenj in rezultatov skupnih čezmejnih nadzornih dejavnosti iz člena 37;

(k) obravnavanje posebnih prošenj za medsebojno pomoč iz člena 37 na zahtevo ene ali več zadevnih držav članic;

(l) zagotavljanje strateških usmeritev mreži skupin CSIRT in mreži EU-CyCLONe o posebnih porajajočih se vprašanjih;

(m) izmenjava mnenj o politiki nadaljnjih ukrepov po kibernetskih incidentih velikih razsežnosti in krizah na podlagi pridobljenih izkušenj mreže skupin CSIRT in mreže EU-CyCLONe;

(n) 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;

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

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

(q) določitev metodologije in organizacijskih vidikov medsebojnih strokovnih pregledov iz člena 19(1) ter določitev metodologije samoocenjevanja za države članice v skladu s členom 19(5), ob pomoči Komisije in ENISA, ter v sodelovanju s Komisijo in ENISA oblikovanje kodeksov ravnanja, na katerih temeljijo delovne metode imenovanih strokovnjakov za kibernetsko varnost v skladu s členom 19(6);

(r) priprava poročil za namene pregleda iz člena 40 o izkušnjah, pridobljenih na strateški ravni in pri medsebojnih strokovnih pregledih;

(s) obravnavanje in redno ocenjevanje stanja kibernetskih groženj ali incidentov, kot je izsiljevalsko programje.

Skupina za sodelovanje predloži poročila iz prvega pododstavka, točka (r), Komisiji, Evropskemu parlamentu in Svetu.

5. Države članice zagotovijo učinkovito, uspešno in varno sodelovanje njihovih predstavnikov v skupini za sodelovanje.

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

7. Skupina za sodelovanje do 1. februarja 2024 in nato vsaki dve leti pripravi delovni program v zvezi z ukrepi, ki jih je treba sprejeti za izpolnitev njenih ciljev in nalog.

8. Komisija lahko sprejme izvedbene akte, s katerimi določi postopkovne ureditve, potrebne za delovanje skupine za sodelovanje.

Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 39(2).

Pri osnutkih izvedbenih aktov iz prvega pododstavka tega odstavka v skladu z odstavkom 4, točka (e), si Komisija s skupino za sodelovanje izmenjuje nasvete in z njo sodeluje.

9. Skupina za sodelovanje se redno, v vsakem primeru pa vsaj enkrat letno, sestane s skupino za odpornost kritičnih subjektov, ustanovljeno na podlagi Direktive (EU) 2022/2557 z namenom spodbujanja in omogočanja strateškega sodelovanja in izmenjave informacij.

Člen 15

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 skupin CSIRT, ki so imenovani ali določeni na podlagi člena 10, in skupina za odzivanje na računalniške grožnje za evropske institucije, organe in agencije Unije (CERT-EU). Komisija sodeluje v mreži skupin CSIRT kot opazovalka. 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) omogočanje souporabe, prenosa in izmenjave tehnologije ter ustreznih ukrepov, politik, orodij, postopkov, primerov dobre prakse in okvirov med skupinami CSIRT;

(c) izmenjava ustreznih informacij o incidentih, skorajšnjih incidentih, kibernetskih grožnjah, tveganjih in ranljivostih;

(d) izmenjava informacij v zvezi s publikacijami in priporočili o kibernetski varnosti;

(e) zagotavljanje interoperabilnosti v zvezi s specifikacijami in protokoli za izmenjavo informacij;

(f) na prošnjo člana mreže skupin CSIRT, na katero bi lahko vplival določen incident, izmenjava in obravnavanje informacij v zvezi s tem incidentom ter z njim povezanimi kibernetskimi grožnjami, tveganji in ranljivostmi;

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

(h) zagotavljanje pomoči državam članicam pri obravnavanju čezmejnih incidentov v skladu s to direktivo;

(i) sodelovanje, izmenjava primerov najboljših praks in zagotavljanje pomoči skupinam CSIRT, imenovanim za koordinatorje na podlagi člena 12(1) v zvezi z upravljanjem razkrivanja ranljivosti, ki bi lahko pomembno vplivale na subjekte v več kot eni državi članici;

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

  (i) kategorij kibernetskih groženj in incidentov;

  (ii) zgodnjega opozarjanja;

  (iii) medsebojne pomoči;

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

  (v) prispevanja k nacionalnemu načrtu odzivanja iz člena 9(4) na kibernetske incidente velikih razsežnosti in krize na zahtevo držav članic;

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

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

(m) na prošnjo posamezne skupine CSIRT obravnavanje zmogljivosti in pripravljenosti te skupine CSIRT;

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

(o) po potrebi obravnavanje poročil o medsebojnih strokovnih pregledih iz člena 19(9);

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

4. Mreža skupin CSIRT do 17. januarja 2025 in nato vsaki dve leti za namene pregleda iz člena 40 oceni napredek, dosežen na področju operativnega sodelovanja, in sprejme poročilo. V poročilu se zlasti oblikujejo sklepi in priporočila na podlagi rezultatov medsebojnih strokovnih pregledov iz člena 19, opravljenih v zvezi z nacionalnimi skupinami CSIRT. To poročilo se predloži skupini za sodelovanje.

5. Mreža skupin CSIRT sprejme svoj poslovnik.

6. Mreža skupin CSIRT in mreža EU-CyCLONe se dogovorita o postopkovnih ureditvah in sodelujeta na njihovi podlagi.

Člen 16

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

1. Mreža EU-CyCLONe se ustanovi za podpiranje usklajenega obvladovanja kibernetskih incidentov velikih razsežnosti in kriz na operativni ravni in za zagotovitev redne izmenjave relevantnih informacij med državami članicami ter institucijami, organi, uradi in agencijami Unije.

2. Mreža EU-CyCLONe je sestavljena iz predstavnikov organov držav članic za obvladovanje kibernetskih kriz, v primerih, ko morebitni ali potekajoči kibernetski incidenti velikih razsežnosti pomembno vplivajo ali bi lahko pomembno vplivali na storitve in dejavnosti, ki spadajo na področje uporabe te direktive, pa tudi predstavnikov Komisije. V drugih primerih Komisija sodeluje pri dejavnostih mreže EU-CyCLONe kot opazovalka.

ENISA zagotovi sekretariat mreže EU-CyCLONe in podpira varno izmenjavo informacij ter zagotavlja potrebna orodja za podporo sodelovanju med državami članicami, s katerimi omogoča varno izmenjavo informacij.

Mreža EU-CyCLONe lahko po potrebi k sodelovanju v vlogi opazovalcev povabi predstavnike ustreznih deležnikov.

3. Mreža EU-CyCLONe ima naslednje naloge:

(a) zviševanje ravni pripravljenosti za obvladovanje kibernetskih incidentov velikih razsežnosti in kriz;

(b) razvoj skupnega situacijskega zavedanja o kibernetskih incidentih velikih razsežnosti in krizah;

(c) ocenjevanje posledic in vpliva relevantnih kibernetskih incidentov velikih razsežnosti in kriz ter predlaganje morebitnih blažilnih ukrepov;

(d) usklajevanje obvladovanja kibernetskih incidentov velikih razsežnosti in kriz ter podpiranje odločanja na politični ravni v zvezi s takimi incidenti in krizami;

(e) obravnavanje nacionalnih načrtov za odzivanje iz člena 9(4) na kibernetske incidente velikih razsežnosti in krize na zahtevo zadevne države članice.

4. Mreža EU-CyCLONe sprejme svoj poslovnik.

5. Mreža EU-CyCLONe redno poroča skupini za sodelovanje o obvladovanju kibernetskih incidentov velikih razsežnosti in kriz, pa tudi o 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 dogovorjenih postopkovnih ureditev iz člena 15(6).

7. Mreža EU-CyCLONe do 17. julija 2024 in nato vsakih 18 mesecev Evropskemu parlamentu in Svetu predloži poročilo o oceni svojega dela.

Člen 17

Mednarodno sodelovanje

Unija v skladu s členom 218 PDEU sklene, kadar je to ustrezno, mednarodne sporazume s tretjimi državami ali mednarodnimi organizacijami, ki omogočajo in urejajo njihovo sodelovanje pri nekaterih dejavnostih skupine za sodelovanje, mreže skupin CSIRT in mreže EU-CyCLONe. Ti sporazumi morajo biti skladni s pravom Unije o varstvu podatkov.

Člen 18

Poročilo o stanju kibernetske varnosti v Uniji

1. ENISA v sodelovanju s Komisijo in skupino za sodelovanje sprejme dvoletno poročilo o stanju kibernetske varnosti v Uniji in ga posreduje in predstavi Evropskemu parlamentu. Poročilo mora med drugim biti na voljo v strojno berljivi obliki in mora vključevati:

(a) oceno tveganja za kibernetsko varnost na ravni Unije, pri čemer se upošteva splošna kibernetska ogroženost;

(b) oceno razvoja zmogljivosti za kibernetsko varnost v javnem in zasebnem sektorju po vsej Uniji;

(c) oceno splošne ravni ozaveščenosti o kibernetski varnosti in kibernetske higiene med državljani in subjekti, vključno z malimi in srednjimi podjetji;

(d) skupno oceno na podlagi rezultatov medsebojnih strokovnih pregledov iz člena 19;

(e) skupno oceno ravni zrelosti zmogljivosti za kibernetsko varnost in sredstev po vsej Uniji, tudi tistih na sektorski ravni, ter stopnjo usklajenosti nacionalnih strategij držav članic za kibernetsko varnost.

2. V poročilo se vključijo posebna priporočila politike za odpravo pomanjkljivosti in zvišanje ravni kibernetske varnosti po vsej Uniji in povzetek ugotovitev za določeno obdobje iz tehničnih poročil o stanju na področju kibernetske varnosti v EU, ki jih izda ENISA v skladu s členom 7(6) Uredbe (EU) 2019/881.

3. ENISA v sodelovanju s Komisijo, skupino za sodelovanje in mrežo skupin CSIRT pripravi metodologijo skupne ocene iz odstavka 1, točka (e), vključno z ustreznimi spremenljivkami, kot so kvantitativni in kvalitativni kazalniki.

Člen 19

Medsebojni strokovni pregledi

1. Skupina za sodelovanje do 17. januarja 2025 s pomočjo Komisije in ENISA ter po potrebi mreže skupin CSIRT določi metodologijo in organizacijske vidike medsebojnih strokovnih pregledov, z namenom učenja iz skupnih izkušenj, okrepitve medsebojnega zaupanja, doseganja visoke skupne ravni kibernetske varnosti ter okrepitve zmogljivosti in politike držav članic na področju kibernetske varnosti, potrebne za izvajanje te direktive. Sodelovanje pri medsebojnih strokovnih pregledih je prostovoljno. Medsebojne strokovne preglede izvede skupina strokovnjakov za kibernetsko varnost. Strokovnjake za kibernetsko varnost imenujeta vsaj dve državi članici, ki nista država članica, v zvezi s katero se izvede pregled.

Medsebojni strokovni pregledi vključujejo vsaj eno od naslednjega:

(a) raven izvajanja zahtev glede obvladovanja tveganj za kibernetsko varnost ter obveznosti poročanja iz členov 21 in 23;

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

(c) operativne zmogljivosti skupin CSIRT;

(d) raven izvajanja medsebojne pomoči iz člena 37;

(e) raven izvajanja dogovorov o izmenjavi informacij o kibernetski varnosti iz člena 29;

(f) posebni čezmejni ali medsektorski vidiki.

2. V metodologijo iz odstavka 1 se vključijo objektivna, nediskriminatorna, pravična in pregledna merila, na podlagi katerih države članice imenujejo strokovnjake za kibernetsko varnost, ki so upravičeni izvajati medsebojne strokovne preglede. Komisija in ENISA sodelujeta v medsebojnih strokovnih pregledih kot opazovalki.

3. Države članice lahko za namene medsebojnega strokovnega pregleda opredelijo posebne vidike iz odstavka 1, točka (f).

4. Države članice pred začetkom medsebojnega strokovnega pregleda iz odstavka 1 sodelujočim državam članicam uradno sporočijo obseg medsebojnega strokovnega pregleda, vključno z vidiki, opredeljenimi na podlagi odstavka 3.

5. Države članice lahko pred začetkom medsebojnega strokovnega pregleda izvedejo samooceno vidikov, ki bodo pregledani, in jo posredujejo imenovanim strokovnjakom za kibernetsko varnost. Skupina za sodelovanje ob pomoči Komisije in ENISA določi metodologijo za samoocenjevanje držav članic.

6. Medsebojni strokovni pregledi obsegajo fizične ali virtualne obiske na kraju samem in izmenjave na daljavo. Države članice, ki so predmet medsebojnega strokovnega pregleda, ob upoštevanju načela dobrega sodelovanja imenovanim strokovnjakom za kibernetsko varnost zagotovijo informacije, potrebne za oceno, brez poseganja v nacionalno pravo ali pravo Unije o varstvu zaupnih ali tajnih podatkov in v zaščito temeljnih državnih funkcij, kot je nacionalna varnost. Skupina za sodelovanje ob pomoči Komisije in ENISA pripravi ustrezne kodekse ravnanja kot podlago za delovne metode imenovanih strokovnjakov za kibernetsko varnost. Vse informacije, pridobljene v okviru medsebojnega strokovnega pregleda, se uporabljajo izključno v ta namen. Strokovnjaki za kibernetsko varnost, ki sodelujejo pri medsebojnem strokovnem pregledu, občutljivih ali zaupnih informacij, pridobljenih med zadevnim pregledom, ne razkrijejo tretjim osebam.

7. Potem ko je bila država članica predmet medsebojnega strokovnega pregleda, isti vidiki, ki so bili v določeni državi članici pregledani, dve leti po zaključku medsebojnega strokovnega pregleda niso predmet nadaljnjih medsebojnih strokovnih pregledov v tej državi članici, razen na zahtevo države članice ali po dogovoru na podlagi predloga skupine za sodelovanje.

8. Države članice zagotovijo, da se drugim državam članicam, skupini za sodelovanje, Komisiji in ENISA pred začetkom postopka medsebojnega strokovnega pregleda razkrijejo vsa tveganja nasprotja interesov v zvezi z imenovanimi strokovnjaki za kibernetsko varnost. Država članica, ki je predmet medsebojnega strokovnega pregleda, lahko nasprotuje imenovanju posameznih strokovnjakov za kibernetsko varnost iz ustrezno utemeljenih razlogov in o tem obvesti državo članico, ki jih je imenovala.

9. Strokovnjaki za kibernetsko varnost, ki sodelujejo v medsebojnih strokovnih pregledih, pripravijo poročila o ugotovitvah in sklepih medsebojnih strokovnih pregledov. Države članice, ki so predmet medsebojnega strokovnega pregleda, lahko predložijo pripombe na osnutke poročil, ki se nanašajo nanje, te pripombe pa se priložijo poročilom. Poročila vsebujejo priporočila za izboljšanje vidikov, vključenih v medsebojni strokovni pregled. Poročila se predložijo skupini za sodelovanje in po potrebi mreži skupin CSIRT. Država članica, ki je predmet medsebojnega strokovnega pregleda, se lahko odloči, da naredi poročilo, ki se nanaša nanjo, ali njegovo redigirano različico javno dostopno.

POGLAVJE IV

OBVEZNOSTI GLEDE UKREPOV ZA OBVLADOVANJE TVEGANJ ZA KIBERNETSKO VARNOST IN POROČANJA

Člen 20

Upravljanje

1. Države članice zagotovijo, da upravljalni organi bistvenih in pomembnih subjektov odobrijo ukrepe za obvladovanje tveganj za kibernetsko varnost, ki jih sprejmejo zadevni subjekti, da izpolnijo člen 21, nadzorujejo njihovo izvajanje in lahko odgovarjajo za kršitve tega člena s strani subjektov.

Pri uporabi tega odstavka se ne sme posegati v nacionalno pravo v zvezi s pravili o odgovornosti, ki se uporabljajo v javnih institucijah, pa tudi ne o odgovornosti javnih uslužbencev ter izvoljenih ali imenovanih uradnikov.

2. Države članice zagotovijo, da se morajo člani upravljalnega organa bistvenih in pomembnih subjektov usposabljati, in spodbujajo bistvene in pomembne subjekte, da podobno usposabljanje redno ponujajo svojim zaposlenim, da pridobijo dovolj znanja in spretnosti, ki jih usposobi za prepoznavanje in ocenjevanje tveganj in za oceno praks obvladovanja tveganj za kibernetsko varnosti ter njihovega vpliva na storitve, ki jih opravlja subjekt.

Člen 21

Ukrepi za obvladovanje tveganj za kibernetsko varnost

1. Države članice zagotovijo, da bistveni in pomembni subjekti sprejmejo ustrezne in sorazmerne tehnične, operativne in organizacijske ukrepe za obvladovanje tveganj za varnost omrežnih in informacijskih sistemov, ki jih ti subjekti uporabljajo za njihovo delovanje ali opravljanje storitev ter za preprečevanje ali zmanjšanje vpliva incidentov na prejemnike svojih storitev in druge storitve.

Ob upoštevanju najsodobnejših in po potrebi ustreznih evropskih in mednarodnih standardov ter stroškov izvajanja morajo ukrepi iz prvega pododstavka zagotavljati raven varnosti omrežnih in informacijskih sistemov, ki ustreza obstoječim tveganjem. Pri ocenjevanju sorazmernosti teh ukrepov je treba ustrezno upoštevati stopnjo izpostavljenosti subjekta tveganjem, velikost subjekta in verjetnost pojava incidentov ter njihovo resnost, vključno z njihovim družbenim in gospodarskim vplivom.

2. Ukrepi iz odstavka 1 morajo temeljiti na pristopu upoštevanja vseh nevarnosti**,** katerega namen je zaščititi omrežne in informacijske sisteme ter njihovo fizično okolje pred incidenti, in vključujejo vsaj naslednje:

(a) politike o analizi tveganja in varnosti informacijskih sistemov;

(b) obvladovanje incidentov;

(c) neprekinjeno poslovanje, kot je upravljanje varnostnih kopij in vnovična vzpostavitev delovanja po nepredvidljivih dogodkih, ter obvladovanje kriz;

(d) varnost dobavne verige, vključno z vidiki, povezanimi z varnostjo, ki se nanašajo na odnose med posameznim subjektom in njegovimi neposrednimi dobavitelji ali ponudniki storitev;

(e) varnost pri pridobivanju, razvoju in vzdrževanju omrežnih in informacijskih sistemov, vključno z obravnavanjem in razkrivanjem ranljivosti;

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

(g) osnovne prakse kibernetske higiene in usposabljanje na področju kibernetske varnosti;

(h) politike in postopke v zvezi z uporabo kriptografije in po potrebi šifriranjem;

(i) varnost človeških virov, politike nadzora dostopa in upravljanje sredstev;

(j) uporaba večfaktorske avtentikacije ali rešitev neprekinjene avtentikacije, varovanih glasovnih, video in besedilnih komunikacij in varnih sistemov za komunikacije v sili znotraj subjekta, kadar je to primerno.

3. Države članice zagotovijo, da subjekti pri preučevanju ustreznih ukrepov iz odstavka 2, točka (d), tega člena, upoštevajo ranljivosti, ki so specifične za posameznega neposrednega 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. Države članice zagotovijo tudi, da morajo subjekti pri ugotavljanju, kateri ukrepi iz navedene točke so ustrezni, upoštevati rezultate usklajenih ocen tveganja za kritične dobavne verige, izvedenih v skladu s členom 22(1).

4. Države članice zagotovijo, da subjekt, ki ugotovi, da ne izpolnjuje ukrepov iz odstavka 2, brez nepotrebnega odlašanja sprejme vse potrebne, ustrezne in sorazmerne popravne ukrepe.

5. Komisija do 17. oktobra 2024 sprejme izvedbene akte, ki določajo tehnične in metodološke zahteve ukrepov iz odstavka 2 v zvezi s ponudniki storitev DNS, registri TLD imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnih centrov, ponudniki omrežij za dostavo vsebine, ponudniki upravljanih storitev, ponudniki upravljanih varnostnih storitev, ponudniki spletnih tržnic, spletnih brskalnikov in platform za storitve družbenega mreženja in ponudniki storitev zaupanja.

Komisija lahko sprejme izvedbene akte, s katerimi določi tehnične in metodološke zahteve ter po potrebi sektorske zahteve za ukrepe iz odstavka 2 v zvezi z bistvenimi in pomembnimi subjekti, ki niso navedeni v prvem pododstavku tega odstavka.

Komisija pri pripravi izvedbenih aktov iz prvega in drugega pododstavka tega odstavka po možnosti upošteva evropske in mednarodne standarde ter ustrezne tehnične specifikacije. Pri osnutkih izvedbenih aktov v skladu s členom 14(4), točka (e), si Komisija izmenjuje nasvete in sodeluje s skupino za sodelovanje in ENISA.

Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 39(2).

Člen 22

Usklajene ocene tveganja za varnost na ravni Unije za kritične dobavne verige

1. Skupina za sodelovanje lahko v sodelovanju s Komisijo in 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 ENISA in po potrebi pomembnimi deležniki identificira specifične kritične storitve IKT, sisteme IKT ali proizvode IKT, ki so lahko predmet usklajene ocene tveganja za varnost iz odstavka 1.

Člen 23

Obveznosti poročanja

1. Vsaka država članica zagotovi, da bistveni in pomembni subjekti njeni skupini CSIRT ali, kadar je to potrebno, njenemu pristojnemu organu brez nepotrebnega odlašanja v skladu z odstavkom 4 priglasijo vse incidente, ki pomembno vplivajo na zagotavljanje njihovih storitev, kot je navedeno v odstavku 3 (pomemben incident). Kadar je ustrezno, zadevni subjekti prejemnike svojih storitev brez nepotrebnega odlašanja uradno obvestijo o pomembnih incidentih, ki bodo verjetno negativno vplivali na zagotavljanje teh storitev. Vsaka država članica zagotovi, da ti subjekti sporočijo, med drugim, vse informacije, ki skupini CSIRT ali, kadar je potrebno, pristojnemu organu omogočajo, da določijo čezmejni vpliv incidenta. Sama priglasitev priglasitvenim subjektom ne sme nalagati dodatne odgovornosti.

Kadar zadevni subjekti pristojnemu organu priglasijo pomemben incident v skladu s prvim pododstavkom, država članica zagotovi, da ta pristojni organ priglasitev po prejemu posreduje skupini CSIRT.

V primeru pomembnega čezmejnega ali medsektorskega pomembnega incidenta države članice zagotovijo, da se njihovim enotnim kontaktnim točkam pravočasno zagotovijo ustrezne informacije, uradno sporočene v skladu z odstavkom 4.

2. Po potrebi države članice zagotovijo, da bistveni in pomembni subjekti brez nepotrebnega odlašanja sporočijo prejemnikom svojih storitev, ki bi jih pomembna kibernetska grožnja lahko prizadela, vse ukrepe ali sredstva, ki jih lahko ti prejemniki sprejmejo v odziv na to grožnjo. Kadar je ustrezno, subjekti zadevne prejemnike obvestijo tudi o sami pomembni kibernetski grožnji.

3. Incident se šteje za pomemben, če:

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

(b) je vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.

4. Države članice zagotovijo, da zadevni subjekti za namen priglasitve iz odstavka 1 skupini CSIRT ali po potrebi pristojnemu organu predložijo:

(a) brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah po seznanitvi z incidentom, zgodnje opozorilo, iz katerega je po potrebi razvidno**,** ali je bil pomemben incident domnevno povzročen z nezakonitim ali zlonamernim dejanjem ali bi lahko imel čezmejni vpliv;

(b) brez nepotrebnega odlašanja, v vsakem primeru pa v 72 urah po seznanitvi s pomembnim incidentom, priglasitev incidenta, s katero se po potrebi posodobijo informacije iz točke (a) in navede začetna ocena pomembnega incidenta, vključno z njegovo resnostjo in vplivom ter, kadar so na voljo, kazalniki ogroženosti;

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

(d) končno poročilo, najpozneje v enem mesecu po predložitvi priglasitve incidenta iz točke (b), ki vključuje naslednje:

(i) podroben opis incidenta, vključno z njegovo resnostjo in vplivom;

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

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

(iv) po potrebi čezmejni vpliv incidenta;

(e) v primeru incidenta, ki je ob predložitvi končnega poročila iz točke (d) še vedno v teku, bi morale države članice poskrbeti, da subjekti takrat predložijo poročilo o napredku, končno poročilo pa najpozneje en mesec po razrešitvi incidenta.

Z odstopanjem od prvega pododstavka, točka (b), ponudnik storitev zaupanja v zvezi s pomembnimi incidenti, ki vplivajo na zagotavljanje njegovih storitev, o tem brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah po seznanitvi s pomembnim incidentom, uradno obvesti skupino CSIRT ali po potrebi pristojni organ.

5. Skupina CSIRT ali pristojni organ brez nepotrebnega odlašanja in po možnosti v 24 urah po prejemu zgodnjega opozorila iz odstavka 4, točka (a), odgovorijo priglasitvenemu subjektu, vključno z začetnimi povratnimi informacijami o pomembnem incidentu in, na zahtevo subjekta, usmeritvami ali operativnim nasvetom glede izvajanja morebitnih blažilnih ukrepov. Kadar skupina CSIRT ni začetni prejemnik priglasitve iz odstavka 1, usmeritve zagotovi pristojni organ v sodelovanju s skupino CSIRT. Skupina CSIRT na zahtevo zadevnega subjekta zagotovi dodatno tehnično podporo. Kadar se za incident sumi, da je kazenske narave, skupina CSIRT ali pristojni organ zagotovi tudi usmeritve o poročanju o pomembnih incidentih organom kazenskega pregona.

6. Kadar je ustrezno in zlasti kadar pomemben incident zadeva dve ali več držav članic, skupina CSIRT, pristojni organ ali enotna kontaktna točka brez nepotrebnega odlašanja obvestijo druge prizadete države članice in ENISA o pomembnem incidentu. Te informacije vključujejo vrsto informacij, prejetih v skladu z odstavkom 4. Skupina CSIRT**,** pristojni organ ali enotne kontaktne točke pri tem v skladu s pravom Unije ali nacionalnim pravom zaščitijo varnost in poslovne interese subjekta ter zaupnost predloženih informacij.

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

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

9. Enotna kontaktna točka ENISA vsake tri mesece predloži zbirno poročilo, vključno z anonimiziranimi in zbirnimi podatki o incidentih, pomembnih kibernetskih grožnjah in skorajšnjih incidentih, priglašenih v skladu z odstavkom 1 tega člena ter členom 30. Da bi se prispevalo k zagotavljanju primerljivih informacij, lahko ENISA sprejme tehnične smernice o parametrih za informacije, ki naj se vključijo v zbirno poročilo. ENISA vsakih šest mesecev obvešča skupino za sodelovanje in mrežo skupin CSIRT o svojih ugotovitvah v zvezi s prejetimi priglasitvami.

10. Skupine CSIRT ali po potrebi pristojni organi zagotovijo pristojnim organom iz Direktive (EU) 2022/2557 informacije o pomembnih incidentih, incidentih, kibernetskih grožnjah in skorajšnjih incidentih, ki so jih v skladu z odstavkom 1 tega člena in členom 30 priglasili bistveni subjekti, identificirani kot kritični subjekti na podlagi Direktive (EU) 2022/2557.

11. Komisija lahko sprejme izvedbene akte, s katerimi se podrobneje določijo vrsta informacij, oblika in postopek priglasitve, predložene v skladu z odstavkom 1 tega člena in členom 30, in obvestila, predloženega v skladu z odstavkom 2 tega člena.

Komisija do 17. oktobra 2024 v zvezi s ponudniki storitev DNS, registri TLD imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnih centrov, ponudniki omrežij za dostavo vsebine, ponudniki upravljanih storitev, ponudniki upravljanih varnostnih storitev, kot tudi ponudniki spletnih tržnic, spletnih brskalnikov in platform za storitve družbenega mreženja sprejme izvedbene akte, v katerih se podrobneje določijo primeri, v katerih se incident šteje za pomembnega, kot je navedeno v odstavku 3. Komisija lahko sprejme te izvedbene akte v zvezi z drugimi bistvenimi in pomembnimi subjekti.

Pri osnutkih izvedbenih aktov iz prvega in drugega pododstavka tega odstavka v skladu s členom 14(4), točka (e), si Komisija izmenjuje nasvete in sodeluje s skupino za sodelovanje.

Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 39(2).

Člen 24

Uporaba evropskih certifikacijskih shem za kibernetsko varnost

1. Države članice lahko za dokaz izpolnjevanja nekaterih zahtev iz člena 21 od bistvenih in pomembnih subjektov zahtevajo, naj zlasti uporabljajo proizvode IKT, storitve IKT in postopke IKT, ki so jih razvili bistveni ali pomembni subjekti ali ki so bili kupljeni pri tretjih straneh, in so certificirani na podlagi evropskih certifikacijskih shem za kibernetsko varnost, sprejetih na podlagi člena 49 Uredbe (EU) 2019/881. Poleg tega države članice bistvene in pomembne subjekte spodbujajo, naj uporabljajo kvalificirane storitve zaupanja.

2. Komisija je pooblaščena za sprejetje delegiranih aktov v skladu s členom 38, da se ta direktiva dopolni z določitvijo kategorij bistvenih in pomembnih subjektov, ki morajo uporabiti nekatere certificirane proizvode IKT, storitve IKT in procese IKT ali pridobiti certifikat na podlagi evropske certifikacijske sheme za kibernetsko varnost, sprejete na podlagi člena 49 Uredbe (EU) 2019/881. Ti delegirani akti se sprejmejo, kadar so bile ugotovljene nezadostne ravni kibernetske varnosti, v njih pa se določi obdobje izvajanja.

Komisija pred sprejetjem delegiranih aktov izvede oceno učinka in posvetovanja v skladu s členom 56 Uredbe (EU) 2019/881.

3. Kadar za namene odstavka 2 tega člena ni na voljo ustrezne evropske certifikacijske sheme za kibernetsko varnost, lahko Komisija po posvetovanju s Skupino za sodelovanje in Evropsko certifikacijsko skupino za kibernetsko varnost od ENISA zahteva, naj pripravi predlogo za shemo v skladu s členom 48(2) Uredbe (EU) 2019/881.

Člen 25

Standardizacija

1. Za zagotovitev skladnega izvajanja člena 21(1) in (2) države članice spodbujajo uporabo evropskih in mednarodnih standardov in tehničnih specifikacij, pomembnih za varnost omrežnih in informacijskih sistemov, ne da bi predpisale uporabo določene vrste tehnologije ali ji dajale prednost.

2. ENISA v sodelovanju z državami članicami ter po posvetovanju z ustreznimi deležniki, kadar je ustrezno, pripravi nasvete in smernice za tehnična področja, ki se upoštevajo v zvezi z odstavkom 1, ter za že obstoječe standarde, vključno z nacionalnimi standardi, s katerimi bi lahko zajeli ta področja.

POGLAVJE V

PRISTOJNOST IN REGISTRACIJA

Člen 26

Pristojnost in teritorialnost

1. Subjekti na podlagi te direktive spadajo v pristojnost države članice, kjer imajo sedež, razen v primeru, da:

(a) se za ponudnike javnih elektronskih komunikacijskih omrežij ali ponudnike javno dostopnih elektronskih komunikacijskih storitev šteje, da spadajo v pristojnost države članice, v kateri zagotavljajo svoje storitve;

(b) se za ponudnike storitev DNS, registre TLD imen, subjekte, ki opravljajo storitve registracije domenskih imen, ponudnike storitev računalništva v oblaku, ponudnike storitev podatkovnih centrov, ponudnike omrežij za dostavo vsebine, ponudnike upravljanih storitev, ponudnike upravljanih varnostnih storitev ter ponudnike spletnih tržnic, spletnih brskalnikov in platform za storitve družbenega mreženja šteje, da spadajo v pristojnost države članice, v kateri imajo glavni sedež v Uniji v skladu z odstavkom 2;

(c) se za subjekte javne uprave šteje, da spadajo v pristojnost države članice, ki jih je ustanovila.

2. Z namene te direktive se za subjekt iz odstavka 1, točka (b), šteje, da ima glavni sedež v Uniji v državi članici, kjer se sprejme večina odločitev v zvezi z ukrepi za obvladovanje tveganj za kibernetsko varnost. Če te države članice ni mogoče določiti ali če se te odločitve ne sprejemajo v Uniji, bi bilo treba šteti, da je glavni sedež v državi članici, kjer se izvajajo operacije v zvezi s kibernetsko varnostjo. Če te države članice ni mogoče določiti, se šteje, da je glavni sedež v državi članici, kjer ima zadevni subjekt sedež z največjim številom zaposlenih v Uniji.

3. Če subjekt iz odstavka 1, točka (b), 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 pristojnostjo države članice, v kateri ima predstavnik sedež. Če ni imenovanega predstavnika v Uniji v skladu s tem odstavkom, lahko katera koli država članica, v kateri subjekt opravlja storitve, uvede sodne postopke proti subjektu zaradi kršitve te direktive.

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

5. Države članice, ki so prejele zahtevek za medsebojno pomoč v zvezi s subjektom iz odstavka 1, točka (b), lahko v mejah zahtevka sprejmejo ustrezne nadzorne in izvršilne ukrepe v zvezi z zadevnim subjektom, ki opravlja storitve ali ima omrežni in informacijski sistem na njihovem ozemlju.

Člen 27

Register subjektov

1. ENISA vzpostavi in vzdržuje register ponudnikov storitev DNS, registrov TLD imen, subjektov, ki opravljajo storitve registracije domenskih imen, ponudnikov storitev računalništva v oblaku, ponudnikov storitev podatkovnih centrov, ponudnikov omrežij za dostavo vsebine, ponudnikov upravljanih storitev, ponudnikov upravljanih varnostnih storitev, kot tudi ponudnikov spletnih tržnic, spletnih brskalnikov in platform za storitve družbenega mreženja na podlagi informacij**,** prejetih od enotnih kontaktnih točk v skladu z odstavkom 4. ENISA na zahtevo ustreznim pristojnim organom omogoči dostop do navedenega registra, pri čemer zagotovi, da je zaupnosti informacij zaščitena kadar je potrebno.

2. Države članice od subjektov iz odstavka 1 zahtevajo, da pristojnim organom do 17. januarja 2025 predložijo naslednje informacije:

(a) ime subjekta;

(b) ustrezni sektor, podsektor in vrsto subjekta iz Priloge I ali II, kadar je to ustrezno;

(c) naslov njegovega glavnega sedeža in njegovih drugih zakonitih sedežev v Uniji ali, če nima sedeža v Uniji, njegovega predstavnika, imenovanega v skladu s členom 26(3);

(d) posodobljene kontaktne podatke, vključno z elektronskimi naslovi in telefonskimi številkami subjekta in po potrebi njegovega zastopnika, imenovanega v skladu s členom 26(3);

(e) države članice, v katerih subjekt opravlja storitve, ter

(f) bloke naslovov IP subjekta.

3. Države članice zagotovijo, da subjekti iz odstavka 1 nemudoma, v vsakem primeru pa v treh mesecih od datuma spremembe, pristojni organ uradno obvestijo o kakršnih koli spremembah informacij, ki so ji predložili v skladu z odstavkom 2.

4. Po prejemu informacij iz odstavkov 2 in 3, razen informacij iz odstavka 2, točka (f), jih enotna kontaktna točka zadevne države članice brez nepotrebnega odlašanja posreduje ENISA.

5. Po potrebi se informacije iz odstavkov 2 in 3 tega člena predložijo prek nacionalnega mehanizma iz člena 3(4), četrti pododstavek.

Člen 28

Podatkovna zbirka o registraciji *domenskih imen*

1. Da bi države članice prispevale k varnosti, stabilnosti in odpornosti DNS, zahtevajo, da registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen, z ustrezno skrbnostjo zbirajo ter vzdržujejo točne in popolne podatke o registraciji domenskih imen v posebni podatkovni zbirki, v skladu s pravom Unije o varstvu podatkov v zvezi s podatki, ki so osebni podatki.

2. Za namene odstavka 1 države članice zahtevajo, da podatkovne zbirke o registraciji domenskih imen vsebujejo potrebne informacije za identifikacijo imetnikov domenskih imen in kontaktnih točk, ki upravljajo domenska imena v okviru vrhnjih domenskih imen, in navezavo stika z njimi. Take informacije vključujejo:

(a) domensko ime;

(b) datum registracije;

(c) ime registratorja, njegov kontaktni elektronski naslov in telefonsko številko;

(d) kontaktni elektronski naslov in telefonsko številko kontaktne točke, ki upravlja domensko ime, če se razlikuje od naslova registratorja.

3. Države članice zahtevajo, da imajo registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen, vzpostavljene politike in postopke, vključno s postopki preverjanja, ki zagotavljajo, da podatkovne zbirke iz odstavka 1 vključujejo točne in popolne informacije. Države članice zahtevajo, da so take politike in postopki javno dostopni.

4. Države članice zahtevajo, da registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen, po registraciji domenskega imena brez nepotrebnega odlašanja podatke o registraciji domenskega imena, ki niso osebni podatki, naredijo javno dostopne.

5. Države članice zahtevajo, da registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen, 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 s pravom Unije o varstvu podatkov. Države članice zahtevajo, da registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen, odgovorijo brez nepotrebnega odlašanja, v vsakem primeru pa v 72 urah od prejema kakršnih koli zahtevkov za dostop. Države članice zahtevajo, da so politike in postopki v zvezi z razkritjem teh podatkov javno dostopni.

6. Izpolnjevanje obveznosti iz odstavkov 1 do 5 ne sme povzročiti podvajanja zbiranja podatkov o registraciji domenskih imen. V ta namen države članice od registrov TLD imen in subjektov, ki opravljajo storitve registracije domenskih imen, zahtevajo, da sodelujejo med seboj.

POGLAVJE VI

IZMENJAVA INFORMACIJ

Člen 29

Dogovori o izmenjavi informacij o kibernetski varnosti

1. Države članice zagotovijo, da si lahko subjekti, ki spadajo na področje uporabe te direktive, ter, kadar je ustrezno, drugi subjekti, ki ne spadajo na področje uporabe te direktive, prostovoljno izmenjujejo ustrezne informacije o kibernetski varnosti, vključno z informacijami, ki se nanašajo na kibernetske grožnje, skorajšnje incidente, ranljivosti, tehnike in postopke, kazalnike ogroženosti, sovražne taktike, specifične informacije o grožnji in akterju, opozorila glede kibernetske varnosti in priporočila glede konfiguracije orodij za kibernetsko varnost za zaznavo kibernetskih napadov, kadar taka izmenjava informacij:

(a) stremi k preprečevanju in odkrivanju incidentov, odzivanju nanje ali okrevanju po njih ali k ublažitvi njihovega vpliva;

(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 ranljivosti, tehnikami odkrivanja, omejevanja in preprečevanja groženj, strategijami za zmanjšanje tveganja ali fazami odzivanja in okrevanja ali spodbujanjem sodelovanja med javnimi in zasebnimi subjekti pri raziskovanju kibernetskih groženj.

2. Države članice zagotovijo, da izmenjava informacij poteka v skupnostih bistvenih in pomembnih subjektov ter, kadar je ustrezno**,** dobaviteljev in ponudnikov storitev. Taka izmenjava se izvaja na podlagi dogovorov o izmenjavi informacij o kibernetski varnosti, ob upoštevanju morebitne občutljive narave informacij, ki se izmenjujejo.

3. Države članice olajšajo sklenitev dogovorov o izmenjavi informacij o kibernetski varnosti iz odstavka 2 tega člena. S takšnimi dogovori se lahko določijo operativni elementi, vključno z uporabo namenskih platform IKT in orodij za avtomatizacijo, vsebina in pogoji dogovorov o izmenjavi informacij. Pri določanju podrobnosti sodelovanja javnih organov pri teh dogovorih, lahko države članice naložijo pogoje glede informacij, ki jih dajo na voljo pristojni organi ali skupine CSIRT. Države članice nudijo podporo za uporabo takih dogovorov v skladu s svojimi politikami iz člena 7(2), točka (h).

4. Države članice zagotovijo, da bistveni in pomembni subjekti obvestijo pristojne organe o svojem sodelovanju pri dogovorih o izmenjavi informacij o kibernetski varnosti iz odstavka 2 po sklenitvi takih dogovorov ali, kadar je potrebno, o odstopu od dogovora, ko odstop začne veljati.

5. ENISA zagotavlja pomoč pri sklenitvi dogovorov o izmenjavi informacij o kibernetski varnosti iz odstavka 2 z izmenjavo najboljših praks in zagotavljanjem smernic.

Člen 30

Prostovoljna priglasitev ustreznih informacij

1. Države članice zagotovijo, da lahko poleg obvezne priglasitve iz člena 23 skupinam CSIRT ali, kadar je potrebno, pristojnim organom, priglasitve prostovoljno predložijo:

(a) bistveni in pomembni subjekti v zvezi z incidenti, kibernetskimi grožnjami in skorajšnjimi incidenti;

(b) subjekti, razen tistih iz točke (a), ne glede na to, ali spadajo na področje uporabe te direktive, v zvezi s pomembnimi incidenti, kibernetskimi grožnjami in skorajšnjimi incidenti.

2. Države članice priglasitve iz odstavka 1 tega člena obravnavajo v skladu s postopkom iz člena 23. Pred prostovoljnimi priglasitvami lahko prednostno obravnavajo obvezne priglasitve.

Skupine CIRT in po potrebi pristojni organi informacije o priglasitvah, prejetih v skladu s tem členom, kadar je potrebno, posredujejo enotnim kontaktnim točkam, pri čemer poskrbijo za zaupnost in ustrezno varstvo informacij, ki jih je posredoval priglasitveni subjekt. Pri prostovoljnem poročanju za priglasitveni subjekt ne veljajo nikakršne dodatne obveznosti, ki zanj ne bi veljale, če ne bi predložil priglasitve, pri čemer se ne posega v preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj.

POGLAVJE VII

NADZOR IN IZVRŠEVANJE

Člen 31

Splošni vidiki, povezani z nadzorom in izvrševanjem

1. Države članice zagotovijo, da njihovi pristojni organi učinkovito nadzorujejo in sprejmejo ukrepe, ki so potrebni za zagotovitev skladnosti s to direktivo.

2. Države članice lahko svojim pristojnim organom dovolijo, da dajo prednost nadzornim nalogam. Ta prednost mora temeljiti na pristopu, ki temelji na tveganju. Pristojni organi lahko za opravljanje svojih nadzornih nalog iz členov 32 in 33 izdelajo nadzorne metodologije, ki omogočajo prednostno razvrščanje teh nalog na podlagi pristopa, ki temelji na tveganju.

3. Pristojni organi pri obravnavi incidentov, katerih posledica je kršitev varstva osebnih podatkov, tesno sodelujejo z nadzornimi organi iz Uredbe (EU) 2016/679, pri čemer se ne posega v pristojnosti in naloge nadzornih organov na podlagi navedene uredbe.

4. Brez poseganja v nacionalni zakonodajni in institucionalni okvir države članice zagotovijo, da imajo pristojni organi, ko izvajajo nadzor subjektov javne uprave pri izpolnjevanju te direktive in naložitvi izvršilnih ukrepov v zvezi s kršitvijo te direktive, ustrezna pooblastila, da lahko te naloge izvajajo operativno neodvisno od nadzorovanih subjektov. V zvezi s temi subjekti se lahko države članice v skladu z nacionalnim zakonodajnim in institucionalnim okvirom odločijo za uvedbo ustreznih, sorazmernih in učinkovitih nadzornih in izvršilnih ukrepov.

Člen 32

Nadzorni in izvršilni ukrepi v zvezi z bistvenimi subjekti

1. Države članice zagotovijo, da so nadzorni in izvršilni ukrepi, naloženi bistvenim subjektom v zvezi z obveznostmi iz te direktive, učinkoviti, sorazmerni in odvračilni, pri čemer upoštevajo okoliščine posameznega primera.

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

(a) opravijo inšpekcijske preglede na kraju samem in nadzor na daljavo, vključno z naključnimi pregledi, ki jih izvedejo usposobljeni strokovnjaki;

(b) opravijo redne in ciljno usmerjene revizije varnosti, ki jih izvede neodvisni subjekt ali pristojni organ;

(c) opravijo priložnostne revizije, tudi ko je to utemeljeno zaradi pomembnega incidenta ali kršitve te direktive s strani bistvenega subjekta;

(d) opravijo varnostne preglede, ki temeljijo na objektivnih, nediskriminatornih, poštenih in preglednih merilih za oceno tveganja, pri čemer po potrebi sodelujejo z zadevnim subjektom;

(e) zahtevajo informacije, ki jih potrebujejo za oceno ukrepov za obvladovanje tveganj za kibernetsko varnost, ki jih je sprejel zadevni subjekt, vključno z dokumentiranimi politikami na področju kibernetske varnosti, in izpolnjevanje obveznosti predložitve informacij pristojnim organom v skladu s členom 27;

(f) zahtevajo dostop do podatkov, dokumentov in informacij, potrebnih za opravljanje njihovih nadzornih nalog;

(g) zahtevajo dokaze o izvajanju politik na področju kibernetske varnosti, kot so rezultati revizij varnosti, ki jih izvede usposobljen revizor, in ustrezni dokazi v zvezi z njimi.

Ciljno usmerjene revizije varnosti iz prvega pododstavka, točka (b), temeljijo na ocenah tveganja, ki jih izvedejo pristojni organi ali subjekt, ki je predmet presoje, ali na drugih razpoložljivih informacijah o tveganju.

Rezultati ciljno usmerjene revizije varnosti se dajo na voljo pristojnemu organu. Stroške ciljno usmerjene revizije varnosti, ki jo opravi neodvisni organ, krije revidirani subjekt, razen v ustrezno utemeljenih primerih, ko pristojni organ odloči drugače.

3. Pristojni organi pri izvajanju svojih pooblastil iz odstavka 2, točka (e), (f) ali (g), navedejo namen zahteve in opredelijo zahtevane informacije.

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

(a) izdajo opozorila o kršitvah te direktive s strani zadevnih subjektov;

(b) sprejmejo zavezujoča navodila, tudi v zvezi z ukrepi za preprečitev ali odpravo incidenta, roki za njihovo izvedbo in poročanjem o tem, ali odredbo, s katero od zadevnih subjektov zahtevajo, da odpravijo ugotovljene pomanjkljivosti ali kršitve te direktive

(c) zadevnim subjektom odredijo, naj prenehajo z ravnanjem, ki krši to direktivo, in naj tega ravnanja ne ponovijo več;

(d) zadevnim subjektom odredijo, naj na določen način in v določenem roku poskrbijo, da bodo njihovi ukrepi za obvladovanje tveganj za kibernetsko varnost v skladu s členom 21, oz. naj izpolnijo obveznosti poročanja iz člena 23;

(e) zadevnim subjektom odredijo, naj obvestijo fizične ali pravne osebe, v zvezi s katerimi opravljajo storitve ali izvajajo dejavnosti, na katere bi lahko vplivala pomembna kibernetska grožnja, o naravi grožnje, pa tudi o vseh mogočih zaščitnih ali popravnih ukrepih, ki jih lahko te fizične ali pravne osebe sprejmejo v odziv na to grožnjo;

(f) zadevnim subjektom odredijo, naj v razumnem roku izvedejo priporočila, dana na podlagi revizije varnosti;

(g) imenujejo uradnika za spremljanje z natančno opredeljenimi nalogami v določenem obdobju, ki spremlja izpolnjevanje členov 21 in 23 s strani zadevnih subjektov;

(h) zadevnim subjektom odredijo, naj na določen način objavijo kršitve te direktive;

(i) naložijo ali zahtevajo, naj ustrezni organi ali sodišča v skladu z nacionalnim pravom naložijo upravno globo na podlagi člena 34, poleg katerega koli od ukrepov iz točk (a) do (h) tega odstavka.

5. Kadar se izvršilni ukrepi, sprejeti v skladu z odstavkom 4, točke (a) do (d) in (f), izkažejo za neučinkovite, države članice zagotovijo, da so njihovi 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 njihovi pristojni organi pooblaščeni, da:

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

(b) zahtevajo, naj ustrezni organi ali sodišča v skladu z nacionalnim pravom začasno prepovejo opravljanje vodstvenih funkcij vsem osebam, ki za bistveni subjekt opravljajo poslovodne naloge na ravni glavnega izvršnega direktorja ali pravnega zastopnika.

Začasni preklic ali prepoved, naložena na podlagi tega odstavka, se uporabljata samo, dokler zadevni subjekt ne sprejme potrebnih ukrepov za odpravo pomanjkljivosti ali izpolni zahtev pristojnega organa, zaradi katerih je bil tak izvršilni ukrep uporabljen. Za uvedbo začasnega preklica ali prepovedi veljajo ustrezni postopkovni zaščitni ukrepi v skladu s splošnimi načeli prava Unije in Listino, vključno s pravico do učinkovitega pravnega sredstva in poštenega sojenja, domnevo nedolžnosti in pravico do obrambe.

Izvršilni ukrepi iz tega odstavka se ne uporabljajo za subjekte javne uprave, za katere velja ta direktiva.

6. Države članice zagotovijo, da ima vsaka fizična oseba, ki je odgovorna za bistveni subjekt ali deluje kot pravni zastopnik bistvenega subjekta na podlagi pooblastila za njegovo zastopanje, odločanje v njegovem imenu ali izvajanje nadzora nad njim, pooblastilo za zagotavljanje skladnosti s to direktivo. Države članice zagotovijo, da lahko te fizične osebe odgovarjajo za kršitev svojih dolžnosti, da bi zagotovile skladnost s to direktivo.

Kar zadeva subjekte javne uprave, ta odstavek ne posega v nacionalno pravo v zvezi z odgovornostjo javnih uslužbencev ter izvoljenih ali imenovanih uradnikov.

7. Pristojni organi pri sprejemanju izvršilnih ukrepov iz odstavka 4 ali 5 spoštujejo pravico do obrambe in upoštevajo okoliščine vsakega posameznega primera ter ustrezno upoštevajo vsaj naslednje:

(a) resnost kršitve in pomembnost kršenih določb, pri čemer se morajo za resne kršitve med drugim v vsakem primeru šteti:

(i) ponavljajoče se kršitve;

(ii) nepriglasitev ali neodprava pomembnih incidentov;

(iii) neodprava pomanjkljivosti v skladu z zavezujočimi navodili pristojnih organov;

(iv) oviranje revizij ali dejavnosti spremljanja, ki jih je odredil pristojni organ po ugotovitvi kršitve;

(v) predložitev napačnih in zelo netočnih informacij v zvezi z ukrepi za obvladovanje tveganj za kibernetsko varnost ali obveznostmi poročanja iz členov 21 in 23;

(b) trajanje kršitve;

(c) vse relevantne predhodne kršitve zadevnega subjekta;

(d) vsako povzročeno premoženjsko ali nepremoženjsko škodo, vključno s finančnimi ali gospodarskimi izgubami, učinki na druge storitve in številom prizadetih uporabnikov;

(e) morebitno naklepnost ali malomarnost storilca kršitve;

(f) vse ukrepe, ki jih je subjekt sprejel za preprečevanje ali zmanjšanje premoženjske ali nepremoženjske škode;

(g) vsako upoštevanje odobrenih kodeksov ravnanja ali odobrenih mehanizmov certificiranja;

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

8. Pristojni organi podrobno utemeljijo svoje izvršilne ukrepe. Pred sprejetjem teh ukrepov zadevne subjekte obvestijo o svojih predhodnih ugotovitvah. Tem subjektom tudi dajo na voljo dovolj časa za predložitev pripomb, razen v ustrezno utemeljenih primerih, ko bi to oviralo takojšnje ukrepanje za preprečitev incidentov ali odziv nanje.

9. Države članice zagotovijo, da njihovi pristojni organi iz te direktive obvestijo ustrezne pristojne organe iste države članice iz Direktive (EU) 2022/2557, kadar izvajajo nadzorna in izvršilna pooblastila, namenjena zagotavljanju, da subjekt, ki je na podlagi Direktive (EU) 2022/2557 identificiran kot kritičen, izpolnjuje obveznosti v skladu s to direktivo. Kadar je ustrezno, lahko pristojni organi iz Direktive (EU) 2022/2557 od pristojnih organov iz te direktive zahtevajo, da izvajajo nadzorna in izvršilna pooblastila v zvezi s subjektom, ki je na podlagi Direktive (EU) 2022/2557 identificiran kot kritičen subjekt.

10. Države članice zagotovijo, da njihovi pristojni organi iz te direktive sodelujejo z ustreznimi pristojnimi organi zadevne države članice iz Uredbe (EU) 2022/2554. Države članice zlasti poskrbijo, da njihovi pristojni organi iz te direktive pri izvajanju nadzornih in izvršilnih pooblastil, katerih cilj je zagotoviti, da obveznosti iz te direktive izpolnjuje bistveni subjekt, ki je imenovan za ključnega tretjega ponudnika storitev IKT na podlagi člena 31 Uredbe (EU) 2022/2554, o tem obvestijo nadzorniški forum, ustanovljen na podlagi člena 32(1) Uredbe (EU) 2022/2554.

Člen 33

Nadzorni in izvršilni ukrepi v zvezi s pomembnimi subjekti

1. Če so jim predloženi dokazi, znaki ali informacije, da pomembni subjekt domnevno ni skladen s to direktivo, zlasti s členoma 21 in 23, države članice zagotovijo, da pristojni organi ukrepajo, po potrebi z naknadnimi nadzornimi ukrepi. Države članice zagotovijo, da so ti ukrepi učinkoviti, sorazmerni in odvračilni, pri čemer upoštevajo okoliščine vsakega posameznega primera.

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

(a) opravijo inšpekcijske preglede na kraju samem in naknadni nadzor na daljavo, ki jih izvedejo usposobljeni strokovnjaki;

(b) opravijo ciljno usmerjene revizije varnosti, ki jih izvede neodvisni subjekt ali pristojni organ;

(c) opravijo revizije varnosti, ki temeljijo na objektivnih, nediskriminatornih, poštenih in preglednih merilih za oceno tveganja, pri čemer po potrebi sodelujejo z zadevnim subjektom;

(d) zahtevajo informacije, ki jih potrebujejo za oceno ukrepov za obvladovanje tveganj za kibernetsko varnost, ki jih je sprejel zadevni subjekt, vključno z dokumentiranimi politikami na področju kibernetske varnosti, in izpolnjevanje obveznosti obveščanja pristojnih organov v skladu s členom 27;

(e) zahtevajo dostop do podatkov, dokumentov in informacij, potrebnih za opravljanje njihovih nadzornih nalog;

(f) zahtevajo dokaze o izvajanju politik na področju kibernetske varnosti, kot so rezultati revizije varnosti, ki jih je izvedel usposobljen revizor, in ustrezni dokazi v zvezi z njimi.

Ciljno usmerjene revizije varnosti iz prvega pododstavka, točka (b), temeljijo na ocenah tveganja, ki jih izvedejo pristojni organi ali subjekt, ki je predmet presoje, ali na drugih razpoložljivih informacijah o tveganju.

Rezultati ciljno usmerjene revizije varnosti se dajo na voljo pristojnemu organu. Stroške ciljno usmerjene revizije varnosti, ki jo opravi neodvisni organ, krije zadevni subjekt, razen v ustrezno utemeljenih primerih, ko pristojni organ odloči drugače.

3. Pristojni organi pri izvajanju svojih pooblastil iz odstavka 2, točke (d), (e) ali (f), 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 vsaj za to, da:

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

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

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

(d) zadevnim subjektom odredijo, naj na določen način in v določenem roku poskrbijo, da bodo njihovi ukrepi za obvladovanje tveganj za kibernetsko varnost v skladu s členom 21, ali naj izpolnijo obveznosti poročanja iz člena 23;

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

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

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

(h) naložijo ali zahtevajo, naj ustrezni organi ali sodišča v skladu z nacionalnim pravom naložijo upravno globo v skladu s členom 34, poleg katerega koli od ukrepov iz točk (a) do (g) tega odstavka.

5. Člen 32(6), (7) in (8) se smiselno uporablja za nadzorne in izvršilne ukrepe, ki so v tem členu določeni za pomembne subjekte.

6. Države članice zagotovijo, da njihovi pristojni organi iz te direktive sodelujejo z ustreznimi pristojnimi organi zadevne države članice iz Uredbe (EU) 2022/2554. Države članice zlasti poskrbijo, da njihovi pristojni organi iz te direktive pri izvajanju nadzornih in izvršilnih pooblastil, katerih cilj je zagotoviti, da obveznosti iz te direktive izpolnjuje pomembni subjekt, ki je na podlagi člena 31 Uredbe (EU) 2022/2554 imenovan za ključnega tretjega ponudnika storitev IKT, o tem obvestijo nadzorniški forum, ustanovljen na podlagi člena 32(1) Uredbe (EU) 2022/2554.

Člen 34

Splošni pogoji za naložitev upravnih glob bistvenim in pomembnim subjektom

1. Države članice zagotovijo, da so upravne globe, ki se v skladu s tem členom naložijo bistvenim in pomembnim subjektom v zvezi s kršitvami te direktive, učinkovite, sorazmerne in odvračilne, pri čemer upoštevajo okoliščine vsakega posameznega primera.

2. Upravne globe se naložijo poleg katerega koli ukrepa iz člena 32(4), točke (a) do (h), člena 32(5) in člena 33(4), točke (a) do (g).

3. Pri odločanju o naložitvi upravne globe in njeni višini se v vsakem posameznem primeru upoštevajo vsaj elementi, določeni v členu 32(7).

4. Države članice zagotovijo, da se bistvenim subjektom za kršitve člena 21 ali 23 v skladu z odstavkoma 2 in 3 tega člena naložijo upravne globe v višini najmanj 10 000 000 EUR ali v višini najmanj 2 % skupnega svetovnega letnega prometa podjetja, ki mu pripada bistveni subjekt, v preteklem proračunskem letu, kateri koli znesek je višji.

5. Države članice zagotovijo, da se pomembnim subjektom za kršitve člena 21 ali 23 v skladu z odstavkoma 2 in 3 tega člena naložijo upravne globe v višini najmanj 7 000 000 EUR ali v višini najmanj 1,4 % skupnega svetovnega letnega prometa podjetja, ki mu pripada pomembni subjekt, v preteklem proračunskem letu, kateri koli znesek je višji.

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

7. Brez poseganja v pooblastila pristojnih organov na podlagi členov 32 in 33 lahko vsaka država članica določi pravila o tem, ali in v kolikšni meri se lahko upravne globe naložijo subjektom javne uprave.

8. Kadar pravni sistem države članice ne določa upravnih glob, ta država članica zagotovi, da se ta člen uporablja tako, da pristojni organ sproži postopek za naložitev globe, pristojna nacionalna sodišča pa jo naložijo, pri čemer mora biti zagotovljeno, da so ta pravna sredstva učinkovita in imajo enak učinek, kot ga imajo upravne globe, ki jih naložijo pristojni organi. V vsakem primeru morajo biti globe učinkovite, sorazmerne in odvračilne. Države članice Komisijo uradno obvestijo o določbah svojih zakonov, ki jih sprejmejo na podlagi tega odstavka do 17. oktobra 2024, brez odlašanja pa tudi o vseh nadaljnjih spremembah teh predpisov ali spremembah, ki vplivajo nanje.

Člen 35

Kršitve, ki pomenijo kršitev varstva osebnih podatkov

1. Kadar se pristojni organi med nadzorom ali izvrševanjem zave, da bi lahko kršitev obveznosti iz členov 21 in 23 te direktive s strani bistvenega ali pomembnega subjekta pomenila kršitev varstva osebnih podatkov, kot je opredeljena v členu 4, točka 12, Uredbe (EU) 2016/679 in o katerem se poda obvestilo v skladu s členom 33 navedene uredbe, o tem brez nepotrebnega odlašanja obvestijo nadzorne organe iz člena 55 ali 56 navedene uredbe.

2. Kadar nadzorni organi iz člena 55 ali 56 Uredbe (EU) 2016/679 naložijo upravno globo na podlagi člena 58(2), točka (i), navedene uredbe, pristojni organi na podlagi člena 34 te direktive ne naložijo upravne globe za kršitev iz odstavka 1 tega člena, naložene zaradi istega ravnanja, zaradi katerega je bila naložena upravna globa na podlagi člena 58(2), točka (i), Uredbe (EU) 2016/679. Vendar lahko pristojni organi naložijo izvršilne ukrepe, določene v členu 32(4), točke (a) do (h), členu 32(5) in členu 33(4), točke (a) do (g), te direktive.

3. Kadar ima nadzorni organ, ki je pristojen v skladu z Uredbo (EU) 2016/679, sedež v drugi državi članici kot pristojni organ, pristojni organ obvesti nadzorni organ, ki ima sedež v njegovi lastni državi članici, o možni kršitvi varstva osebnih podatkov iz odstavka 1.

Člen 36

Sankcije

Države članice določijo pravila o sankcijah, ki se uporabljajo za kršitve nacionalnih predpisov, sprejetih na podlagi te direktive, in sprejmejo vse potrebne ukrepe za zagotovitev, da se te sankcije izvajajo. Te sankcije morajo biti učinkovite, sorazmerne in odvračilne. Države članice o teh pravilih in ukrepih uradno obvestijo Komisijo do 17. januarja 2025 ter jo brez odlašanja uradno obvestijo o vsakršni naknadni spremembi, ki nanje vpliva.

Člen 37

Medsebojna pomoč

1. Kadar subjekt storitve opravlja v več kot eni državi članici ali storitve opravlja v eni ali več državah članicah, omrežni in informacijski sistemi pa so v eni ali več drugih državah članicah, pristojni organi zadevnih 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;

(b) pristojni organ lahko od drugega pristojnega organa zahteva, naj sprejme nadzorne ali izvršilne ukrepe;

(c) pristojni organ po prejemu utemeljenega zahtevka drugega pristojnega organa temu organu zagotovi medsebojno pomoč, sorazmerno s sredstvi, ki jih ima na voljo, da se lahko nadzorni ali izvršilni ukrepi izvajajo učinkovito, uspešno in dosledno.

Medsebojna pomoč iz prvega pododstavka, točka (c), 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, zahtevka ne zavrne, razen če se ugotovi, da organ ni pristojen za zagotavljanje zahtevane pomoči, da zahtevana pomoč ni sorazmerna z nadzornimi nalogami pristojnega organa ali da zahtevek zadeva informacije ali dejavnosti, ki bi bile, če bi bile razkrite ali izvedene, v nasprotju z bistvenimi interesi nacionalne varnosti, javno varnostjo ali obrambo te države članice. Preden pristojni organ zavrne takšen zahtevek, se posvetuje z drugimi zadevnimi pristojnimi organi, na zahtevo katere od zadevnih držav članic pa tudi s Komisijo in ENISA.

2. Po potrebi in na podlagi skupnega dogovora lahko pristojni organi iz različnih držav članic izvajajo skupne nadzorne ukrepe.

POGLAVJE VIII

DELEGIRANI IN IZVEDBENI AKTI

Člen 38

Izvajanje prenosa pooblastila

1. Pooblastilo za sprejemanje delegiranih aktov je preneseno na Komisijo pod pogoji, določenimi v tem členu.

2. Pooblastilo za sprejemanje delegiranih aktov iz člena 24(2) se prenese na Komisijo za obdobje petih let od 16. januarja 2023.

3. Prenos pooblastila iz člena 24(2) lahko kadar koli prekliče Evropski parlament ali Svet. S sklepom o preklicu preneha veljati prenos pooblastila iz navedenega sklepa. Sklep začne učinkovati 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 člena 24(2), začne veljati le, če mu niti Evropski parlament niti Svet ne nasprotuje v roku dveh mesecev od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu ali če pred iztekom tega roka tako Evropski parlament kot Svet obvestita Komisijo, da mu ne bosta nasprotovala. Ta rok se na pobudo Evropskega parlamenta ali Sveta podaljša za dva meseca.

Člen 39

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.

POGLAVJE IX

KONČNE DOLOČBE

Člen 40

Pregled

Komisija do 17. oktobra 2027 in nato vsakih 36 mesecev pregleda delovanje te direktive ter o tem poroča Evropskemu parlamentu in Svetu. V poročilu oceni zlasti pomen velikosti zadevnih subjektov ter sektorjev, podsektorjev in vrst 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. Poročilu po potrebi priloži zakonodajni predlog.

Člen 41

Prenos

1. Države članice sprejmejo in objavijo ukrepe, potrebne za uskladitev s to direktivo, do 17. oktobra 2024. Komisiji takoj sporočijo besedilo teh predpisov.

Države članice te predpise uporabljajo od 18. oktobra 2024.

2. Države članice se pri sprejetju predpisov iz odstavka 1 sklicujejo na to direktivo ali pa sklic nanjo navedejo ob njihovi uradni objavi. Način sklicevanja določijo države članice.

Člen 42

Sprememba Uredbe (EU) št. 910/2014

V Uredbi (EU) št. 910/2014 se člen 19 črta z učinkom od 18. oktobra 2024.

Člen 43

Sprememba Direktive (EU) 2018/1972

V Direktivi (EU) 2018/1972 se člena 40 in 41 črtata z učinkom od 18. oktobra 2024.

Člen 44

Razveljavitev

Direktiva (EU) 2016/1148 se razveljavi z učinkom od 18. oktobra 2024.

Sklicevanje na razveljavljeno direktivo se šteje za sklicevanje na to direktivo in se bere v skladu s korelacijsko tabelo iz Priloge III.

Člen 45

Začetek veljavnosti

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

Člen 46

Naslovniki

Ta direktiva je naslovljena na države članice.

V Strasbourgu, 14. decembra 2022

Za Evropski parlament	*Za Svet*
predsednica	*predsednik*
R. METSOLA	M. BEK

PRILOGA I

VISOKO KRITIČNI SEKTORJI

Sektor	Podsektor	Vrsta subjekta
1. Energija	(a) elektrika	— elektroenergetska podjetja, kot so opredeljena v členu 2, točka 57, Direktive (EU) 2019/944 Evropskega parlamenta in Sveta ([1]), ki opravljajo dejavnosti „dobave“, kot je opredeljena v členu 2, točka 12, navedene direktive
		— operaterji distribucijskega sistema, kot so opredeljeni v členu 2, točka 29, Direktive (EU) 2019/944
		— operaterji prenosnega sistema, kot so opredeljeni v členu 2, točka 35, Direktive (EU) 2019/944
		— proizvajalci, kot so opredeljeni v členu 2, točka 38, Direktive (EU) 2019/944
		— imenovani operaterji trga električne energije, kot so opredeljeni v členu 2, točka 8, Uredbe (EU) 2019/943 Evropskega parlamenta in Sveta ([2]) — udeleženci na trgu, kot so opredeljeni v členu 2, točka 25, Uredbe (EU) 2019/943, ki opravljajo storitve agregiranja, prilagajanja odjema ali shranjevanja energije, kot so opredeljeni v členu 2, točke 18, 20 in 59, Direktive (EU) 2019/944 — upravljavci polnilnega mesta, odgovorni za upravljanje in delovanje polnilnega mesta, ki končnim uporabnikom zagotavlja storitev polnjenja, tudi v imenu in za račun ponudnika mobilnostnih storitev
	(b) daljinsko ogrevanje in hlajenje	— upravljavci daljinskega ogrevanja ali daljinskega hlajenja, kot je opredeljeno v členu 2, točka 19, Direktive (EU) 2018/2001 Evropskega parlamenta in Sveta ([3])
	(c) nafta	— upravljavci naftovodov
		— upravljavci obratov za proizvodnjo, rafiniranje in predelavo nafte ter upravljavci skladišč in transporta nafte
		— osrednji organi za vzdrževanje zalog, kot so opredeljeni v členu 2, točka (f), Direktive Sveta 2009/119/ES ([4])
	(d) plin	— dobavitelji, kot so opredeljeni v členu 2, točka 8, Direktive 2009/73/ES Evropskega parlamenta in Sveta ([5])
		— operaterji distribucijskega sistema, kot so opredeljeni v členu 2, točka 6, Direktive 2009/73/ES
		— operaterji prenosnega sistema, kot so opredeljeni v členu 2, točka 4, Direktive 2009/73/ES
		— operaterji skladiščnega sistema, kot so opredeljeni v členu 2, točka 10, Direktive 2009/73/ES
		— operaterji sistema za UZP, kot so opredeljeni v členu 2, točka 12, Direktive 2009/73/ES
		— podjetja plinskega gospodarstva, kot so opredeljeni v členu 2, točka 1, Direktive 2009/73/ES
		— upravljavci obratov za rafiniranje in predelavo zemeljskega plina
	(e) vodik	— upravljavci proizvodnje, shranjevanja in prenosa vodika

Sektor	Podsektor	Vrsta subjekta
2. Promet	(a) zračni	— letalski prevozniki, kot so opredeljeni členu 3, točka 4, Uredbe (ES) št. 300/2008, ki se uporabljajo v komercialne namene
		— upravni organi letališča, kot so opredeljeni v členu 2, točka 2, Direktive 2009/12/ES Evropskega parlamenta in Sveta ([6]), letališča, kot so opredeljena v členu 2, točka 1, navedene direktive, vključno z jedrnimi letališči iz oddelka 2 Priloge II k Uredbi (EU) št. 1315/2013 Evropskega parlamenta in Sveta ([7]), ter subjekti, ki upravljajo pomožne objekte, naprave in sredstva na letališčih
		— kontrolorji upravljanja prometa, ki zagotavljajo kontrolo zračnega prometa (ATC), kot je opredeljena v členu 2, točka 1, Uredbe (ES) št. 549/2004 Evropskega parlamenta in Sveta ([8])
	(b) železniški	— upravljavci infrastrukture, kot so opredeljeni v členu 3, točka 2, Direktive 2012/34/EU Evropskega parlamenta in Sveta ([9])
		— prevozniki v železniškem prometu, kot so opredeljeni v členu 3, točka 1, Direktive 2012/34/EU, vključno z upravljavci objektov za izvajanje železniških storitev, kot so opredeljeni v členu 3, točka 12, navedene direktive
	(c) vodni	— prevozna podjetja za potniški in tovorni promet po kopenskih vodah, morju in obalnih vodah, kot so za področje vodnega prometa opredeljena v Prilogi I k Uredbi (ES) št. 725/2004 Evropskega parlamenta in Sveta ([10]), brez posameznih plovil, ki jih upravljajo ta podjetja
		— upravni organi pristanišč, kot so opredeljena v členu 3, točka 1, Direktive 2005/65/ES Evropskega parlamenta in Sveta ([11]), vključno z njihovimi pristanišči, kot so opredeljena v členu 2, točka 11, Uredbe (ES) št. 725/2004, ter subjekti, ki izvajajo dela in upravljajo opremo v pristaniščih
		— upravljavci sistemov za nadzor plovbe (VTS), kot so opredeljeni v členu 3, točka (o), Direktive 2002/59/ES Evropskega parlamenta in Sveta ([12])
	(d) cestni	— cestni organi, kot so opredeljeni v členu 2, točka 12, Delegirane uredbe Komisije (EU) 2015/962 ([13]), odgovorni za nadzor upravljanja prometa, razen javnih subjektov, za katere je upravljanje prometa ali upravljanje inteligentnih prometnih sistemov le nebistven del splošne dejavnosti
		— upravljavci inteligentnih prometnih sistemov, kot so opredeljeni v členu 4, točka 1, Direktive 2010/40/EU Evropskega parlamenta in Sveta ([14])
3. Bančništvo		kreditne institucije, kot so opredeljene v členu 4, točka 1, Uredbe (EU) št. 575/2013 Evropskega parlamenta in Sveta ([15])
4. Infrastruktura finančnega trga		— upravljavci mest trgovanja, kot so opredeljena v členu 4, točka 24, Direktive 2014/65/EU Evropskega parlamenta in Sveta ([16])
		— centralne nasprotne stranke (CNS), kot so opredeljene v členu 2, točka 1, Uredbe (EU) št. 648/2012 Evropskega parlamenta in Sveta ([17])

Sektor	Podsektor	Vrsta subjekta
5. Zdravje		— izvajalci zdravstvenega varstva, kot so opredeljeni v členu 3, točka (g), Direktive 2011/24/EU Evropskega parlamenta in Sveta ([18])
		— referenčni laboratoriji EU iz člena 15 Uredbe (EU) 2022/2371 Evropskega parlamenta in Sveta ([19])
		— subjekti, ki izvajajo raziskovalne in razvojne dejavnosti na področju zdravil, kot so opredeljena v členu 1, točka 2, Direktive 2001/83/ES Evropskega parlamenta in Sveta ([20]) — subjekti, ki proizvajajo farmacevtske surovine in preparate s področja C oddelka 21 NACE Rev. 2 — subjekti, ki proizvajajo medicinske pripomočke, ki se štejejo za kritične v času izrednih razmer v javnem zdravju (seznam kritičnih pripomočkov v izrednih razmerah v javnem zdravju) v smislu člena 22 Uredbe (EU) 2022/123 Evropskega parlamenta in Sveta ([21])
6. Pitna voda		dobavitelji in distributerji vode, namenjene za prehrano ljudi, kot je opredeljena v členu 2, točka 1(a), Direktive (EU) 2020/2184 Evropskega parlamenta in Sveta ([22]), razen distributerjev, za katere je distribucija vode za prehrano ljudi le nebistven del splošne dejavnosti distribucije drugih dobrin in blaga
7. Odpadna voda		podjetja, ki zbirajo, odvajajo ali čistijo komunalno odpadno vodo, odpadno vodo iz gospodinjstev ali tehnološko odpadno vodo, kot je opredeljena v členu 2, točke 1, 2 in 3, Direktive Sveta 91/271/EGS ([23]), razen podjetij, za katera je zbiranje, odvajanje ali čiščenje komunalne odpadne vode, odpadne vode iz gospodinjstev ali tehnološke odpadne vode nebistven del splošne dejavnosti
8. Digitalna infrastruktura		— ponudniki stičišča omrežij
		— ponudniki storitev DNS, razen upravljavcev korenskih imenskih strežnikov
		— registri TLD imen
		— ponudniki storitev računalništva v oblaku
		— ponudniki storitev podatkovnih centrov
		— ponudniki omrežij za dostavo vsebin
		— ponudniki storitev zaupanja
		— ponudniki javnih elektronskih komunikacijskih omrežij
		— ponudniki javno dostopnih elektronskih komunikacijskih storitev
9. Upravljanje storitev IKT (med podjetji)		— ponudniki upravljanih storitev — ponudniki upravljanih varnostnih storitev

Sektor	Podsektor	Vrsta subjekta
10. Javna uprava		— subjekti javne uprave enot centralne ravni držav, kot jih opredeli država članica v skladu z nacionalnim pravom
		— subjekti javne uprave enot na regionalni ravni, kot jih opredeli država članica v skladu z nacionalnim pravom
11. Vesolje		upravljavci talne infrastrukture, ki jo imajo v lasti, vodijo in upravljajo države članice ali zasebne stranke, ki podpirajo opravljanje vesoljskih storitev, brez ponudnikov javnih elektronskih komunikacijskih omrežij

([1]) Direktiva (EU) 2019/944 Evropskega parlamenta in Sveta z dne 5. junija 2019 o skupnih pravilih notranjega trga električne energije in spremembi Direktive 2012/27/EU (UL L 158, 14.6.2019, str. 125).
([2]) Uredba (EU) 2019/943 Evropskega parlamenta in Sveta z dne 5. junija 2019 o notranjem trgu električne energije (UL L 158, 14.6.2019, str. 54).
([3]) Direktiva (EU) 2018/2001 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o spodbujanju uporabe energije iz obnovljivih virov (UL L 328, 21.12.2018, str. 82).
([4]) Direktiva Sveta 2009/119/ES z dne 14. septembra 2009 o obveznosti držav članic glede vzdrževanja minimalnih zalog surove nafte in/ali naftnih derivatov (UL L 265, 9.10.2009, str. 9).
([5]) Direktiva 2009/73/ES Evropskega parlamenta in Sveta z dne 13. julija 2009 o skupnih pravilih notranjega trga z zemeljskim plinom in o razveljavitvi Direktive 2003/55/ES (UL L 211, 14.8.2009, str. 94).
([6]) Direktiva 2009/12/ES Evropskega parlamenta in Sveta z dne 11. marca 2009 o letaliških pristojbinah (UL L 70, 14.3.2009, str. 11).
([7]) Uredba (EU) št. 1315/2013 Evropskega parlamenta in Sveta z dne 11. decembra 2013 o smernicah Unije za razvoj vseevropskega prometnega omrežja in razveljavitvi Sklepa št. 661/2010/EU (UL L 348, 20.12.2013, str. 1).
([8]) Uredba (ES) št. 549/2004 Evropskega parlamenta in Sveta z dne 10. marca 2004 o določitvi okvira za oblikovanje enotnega evropskega neba (okvirna uredba) (UL L 96, 31.3.2004, str. 1).
([9]) Direktiva 2012/34/EU Evropskega parlamenta in Sveta z dne 21. novembra 2012 o vzpostavitvi enotnega evropskega železniškega območja (UL L 343, 14.12.2012, str. 32).
([10]) Uredba (ES) št. 725/2004 Evropskega parlamenta in Sveta z dne 31. marca 2004 o povečanju zaščite na ladjah in v pristaniščih (UL L 129, 29.4.2004, str. 6).
([11]) Direktiva Evropskega parlamenta in Sveta 2005/65/ES z dne 26. oktobra 2005 o krepitvi varnosti v pristaniščih (UL L 310, 25.11.2005, str. 28).
([12]) Direktiva 2002/59/ES Evropskega parlamenta in Sveta z dne 27. junija 2002 o vzpostavitvi sistema spremljanja in obveščanja za ladijski promet ter o razveljavitvi Direktive Sveta 93/75/EGS (UL L 208, 5.8.2002, str. 10).
([13]) Delegirana uredba Komisije (EU) 2015/962 z dne 18. decembra 2014 o dopolnitvi Direktive 2010/40/EU Evropskega parlamenta in Sveta v zvezi z opravljanjem storitev zagotavljanja prometnih informacij v realnem času po vsej EU (UL L 157, 23.6.2015, str. 21).
([14]) Direktiva 2010/40/EU Evropskega parlamenta in Sveta z dne 7. julija 2010 o okviru za uvajanje inteligentnih prometnih sistemov v cestnem prometu in za vmesnike do drugih vrst prevoza (UL L 207, 6.8.2010, str. 1).
([15]) Uredba (EU) št. 575/2013 Evropskega parlamenta in Sveta z dne 26. junija 2013 o bonitetnih zahtevah za kreditne institucije in o spremembi Uredbe (EU) št. 648/2012 (UL L 176, 27.6.2013, str. 1).
([16]) Direktiva 2014/65/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o trgih finančnih instrumentov ter spremembi Direktive 2002/92/ES in Direktive 2011/61/EU (UL L 173, 12.6.2014, str. 349).
([17]) Uredba (EU) št. 648/2012 Evropskega parlamenta in Sveta z dne 4. julija 2012 o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov (UL L 201, 27.7.2012, str. 1).
([18]) Direktiva 2011/24/EU Evropskega parlamenta in Sveta z dne 9. marca 2011 o uveljavljanju pravic pacientov pri čezmejnem zdravstvenem varstvu (UL L 88, 4.4.2011, str. 45).

([19]) Uredba (EU) 2022/2371 Evropskega parlamenta in Sveta z dne 23. novembra 2022 o resnih čezmejnih grožnjah za zdravje in o razveljavitvi Sklepa št. 1082/2013/EU (UL L 314, 6.12.2022, str. 26).
([20]) Direktiva 2001/83/ES Evropskega parlamenta in Sveta z dne 6. novembra 2001 o zakoniku Skupnosti o zdravilih za uporabo v humani medicini (UL L 311, 28.11.2001, str. 67).
([21]) Uredba (EU) 2022/123 Evropskega parlamenta in Sveta z dne 25. januarja 2022 o okrepljeni vlogi Evropske agencije za zdravila pri pripravljenosti na krize in kriznem upravljanju na področju zdravil in medicinskih pripomočkov (UL L 20, 31.1.2022, str. 1).
([22]) Direktiva (EU) 2020/2184 Evropskega parlamenta in Sveta z dne 16. decembra 2020 o kakovosti vode, namenjene za prehrano ljudi (UL L 435, 23.12.2020, str. 1).
([23]) Direktiva Sveta 91/271/EGS z dne 21. maja 1991 o čiščenju komunalne odpadne vode (UL L 135, 30.5.1991, str. 40).

PRILOGA II

DRUGI KRITIČNI SEKTORJI

Sektor	Podsektor	Vrsta subjekta
1. Poštne in kurirske storitve		izvajalci poštnih storitev, kot so opredeljeni v členu 2, točka 1a, Direktive 97/67/ES, vključno z izvajalci kurirskih storitev
2. Ravnanje z odpadki		podjetja, ki izvajajo postopke ravnanja z odpadki, kot je opredeljeno v členu 3, točka 9, Direktive 2008/98/ES Evropskega parlamenta in Sveta ([1]), vendar brez podjetij, pri katerih ravnanje z odpadki ni glavna gospodarska dejavnost
3. Izdelava, proizvodnja in distribucija kemikalij		podjetja, ki proizvajajo snovi in distribuirajo snovi ali zmesi iz člena 3, točki 9 in 14, Uredbe (ES) št. 1907/2006 Evropskega parlamenta in Sveta ([2]) in podjetja, ki iz snovi in zmesi proizvajajo izdelke, kot so opredeljeni v členu 3, točka 3, navedene uredbe
4. Pridelava, predelava in distribucija živil		živilske dejavnosti, kot so opredeljene v členu 3, točka 2, Uredbe (ES) št. 178/2002 Evropskega parlamenta in Sveta ([3]), ki se ukvarjajo s prodajo na debelo ter industrijsko pridelavo in predelavo
5. Proizvodnja	(a) proizvodnja medicinskih pripomočkov ter in vitro diagnostičnih medicinskih pripomočkov	subjekti, ki proizvajajo medicinske pripomočke, kot so opredeljeni v členu 2, točka 1, Uredbe (EU) 2017/745 Evropskega parlamenta in Sveta ([4]), in subjekti, ki proizvajajo in vitro diagnostične medicinske pripomočke, kot so opredeljeni v členu 2, točka 2, Uredbe (EU) 2017/746 Evropskega parlamenta in Sveta ([5]), razen subjektov, ki proizvajajo medicinske pripomočke iz Priloge I, točka 5, peta alinea, k tej direktivi
	(b) proizvodnja računalnikov, elektronskih in optičnih izdelkov	podjetja, ki opravljajo katero koli gospodarsko dejavnost s področja C oddelka 26 NACE Rev. 2
	(c) proizvodnja električnih naprav	podjetja, ki opravljajo katero koli gospodarsko dejavnost s področja C oddelka 27 NACE Rev. 2
	(d) proizvodnja drugih strojev in naprav	podjetja, ki opravljajo katero koli gospodarsko dejavnost s področja C oddelka 28 NACE Rev. 2
	(e) proizvodnja motornih vozil, prikolic in polprikolic	podjetja, ki opravljajo katero koli gospodarsko dejavnost s področja C oddelka 29 NACE Rev. 2
	(f) proizvodnja drugih vozil in plovil	podjetja, ki opravljajo katero koli gospodarsko dejavnost s področja C oddelka 30 NACE Rev. 2

Sektor	Podsektor	Vrsta subjekta
6. Digitalni ponudniki		— ponudniki spletnih tržnic
		— ponudniki spletnih iskalnikov
		— ponudniki platform za storitve družbenega mreženja
7. Raziskave		raziskovalne organizacije

([1]) Direktiva 2008/98/ES Evropskega parlamenta in Sveta z dne 19. novembra 2008 o odpadkih in razveljavitvi nekaterih direktiv (UL L 312, 22.11.2008, str. 3).

([2]) Uredba (ES) št. 1907/2006 Evropskega parlamenta in Sveta z dne 18. decembra 2006 o registraciji, evalvaciji, avtorizaciji in omejevanju kemikalij (REACH) ter o ustanovitvi Evropske agencije za kemikalije in o spremembi Direktive 1999/45/ES ter o razveljavitvi Uredbe Sveta (EGS) št. 793/93 in Uredbe Komisije (ES) št. 1488/94 ter Direktive Sveta 76/769/EGS in direktiv Komisije 91/155/EGS, 93/67/EGS, 93/105/ES in 2000/21/ES (UL L 396, 30.12.2006, str. 1).

([3]) Uredba (ES) št. 178/2002 Evropskega parlamenta in Sveta z dne 28. januarja 2002 o določitvi splošnih načel in zahtevah živilske zakonodaje, ustanovitvi Evropske agencije za varnost hrane in postopkih, ki zadevajo varnost hrane (UL L 31, 1.2.2002, str. 1).

([4]) Uredba (EU) 2017/745 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o medicinskih pripomočkih, spremembi Direktive 2001/83/ES, Uredbe (ES) št. 178/2002 in Uredbe (ES) št. 1223/2009 ter razveljavitvi direktiv Sveta 90/385/EGS in 93/42/EGS (UL L 117, 5.5.2017, str. 1).

([5]) Uredba (EU) 2017/746 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o *in vitro* diagnostičnih medicinskih pripomočkih ter razveljavitvi Direktive 98/79/ES in Sklepa Komisije 2010/227/EU (UL L 117, 5.5.2017, str. 176).

PRILOGA III

KORELACIJSKA TABELA

Direktiva (EU) 2016/1148	Ta direktiva
člen 1(1)	člen 1(1)
člen 1(2)	člen 1(2)
člen 1(3)	-
člen 1(4)	člen 2(12)
člen 1(5)	člen 2(13)
člen 1(6)	člen 2(6) in (11)
člen 1(7)	člen 4
člen 2	člen 2(14)
člen 3	člen 5
člen 4	člen 6
člen 5	-
člen 6	-
člen 7(1)	člen 7(1) in (2)
člen 7(2)	člen 7(4)
člen 7(3)	člen 7(3)
člen 8(1) do (5)	člen 8(1) do (5)
člen 8(6)	člen 13(4)
člen 8(7)	člen 8(6)
člen 9(1), (2) in (3)	člen 10(1), (2) in (3)
člen 9(4)	člen 10(9)
člen 9(5)	člen 10(10)
člen 10(1), (2) in (3), prvi pododstavek	člen 13(1), (2) in (3)
člen 10(3), drugi pododstavek	člen 23(9)
člen 11(1)	člen 14(1) in (2)
člen 11(2)	člen 14(3)
člen 11(3)	člen 14(4), prvi pododstavek, točke (a) do (q) in (s), ter odstavek 7
člen 11(4)	člen 14(4), prvi pododstavek, točka (r), in drugi pododstavek
člen 11(5)	člen 14(8)
člen 12(1) do (5)	člen 15(1) do (5)
člen 13	člen 17
člen 14(1) in (2)	člen 21(1) do (4)
člen 14(3)	člen 23(1)
člen 14(4)	člen 23(3)
člen 14(5)	člen 23(5), (6) in (8)

Direktiva (EU) 2016/1148	Ta direktiva
člen 14(6)	člen 23(7)
člen 14(7)	člen 23(11)
člen 15(1)	člen 31(1)
člen 15(2), prvi pododstavek, točka (a)	člen 32(2), točka (e)
člen 15(2), prvi pododstavek, točka (b)	člen 32(2), točka (g)
člen 15(2), drugi pododstavek	člen 32(3)
člen 15(3)	člen 32(4), točka (b)
člen 15(4)	člen 31(3)
člen 16(1) in (2)	člen 21(1) do (4)
člen 16(3)	člen 23(1)
člen 16(4)	člen 23(3)
člen 16(5)	-
člen 16(6)	člen 23(6)
člen 16(7)	člen 23(7)
člen 16(8) in (9)	člen 21(5) in člen 23(11)
člen 16(10)	-
člen 16(11)	člen 2(1), (2) in (3)
člen 17(1)	člen 33(1)
člen 17(2), točka (a)	člen 32(2), točka (e)
člen 17(2), točka (b)	člen 32(4), točka (b)
člen 17(3)	člen 37(1), točki (a) in (b)
člen 18(1)	člen 26(1), točka (b), in odstavek 2
člen 18(2)	člen 26(3)
člen 18(3)	člen 26(4)
člen 19	člen 25
člen 20	člen 30
člen 21	člen 36
člen 22	člen 39
člen 23	člen 40
člen 24	-
člen 25	člen 41
člen 26	člen 45
člen 27	člen 46
Priloga I, točka 1	člen 11(1)
Priloga I, točke 2(a)(i) do (iv)	člen 11(2), točke (a) do (d)

Direktiva (EU) 2016/1148	Ta direktiva
Priloga I, točka 2(a)(v)	člen 11(2), točka (f)
Priloga I, točka 2(b)	člen 11(4)
Priloga I, točki 2(c)(i) in (ii)	člen 11(5), točka (a)
Priloga II	Priloga I
Priloga III, točki 1 in 2	Priloga II, točka 6
Priloga III, točka 3	Priloga I, točka 8