

Bruselj, 26. november 2021
(OR. en)

14337/21

Medinstitucionalna zadeva:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

DOPIS

Pošiljatelj:	Generalni sekretariat Sveta
Prejemnik:	Svet
Št. predh. dok.:	9583/2/21, 11724/21
Št. dok. Kom.:	14150/20
Zadeva:	Predlog direktive Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven kibernetске varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148 – <i>splošni pristop</i>

I. UVOD

1. Komisija je 16. decembra 2020 sprejela predlog direktive o ukrepih za visoko skupno raven kibernetске varnosti v Uniji (v nadaljnjem besedilu: revidirana direktiva o varnosti omrežij in informacij)¹, da bi nadomestila sedanjo direktivo o varnosti omrežij in informacijskih sistemov (v nadaljnjem besedilu: direktiva o varnosti omrežij in informacijskih sistemov)².

¹ Predlog direktive Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven kibernetске varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148.

² 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.

Predlog je bil eden od ukrepov, predvidenih v strategiji EU za kibernetiko varnost v digitalnem desetletju³, da bi zagotovili, da bodo imeli državljani in podjetja koristi od zaupanja vredne digitalne tehnologije.

2. Cilj predloga, ki temelji na členu 114 Pogodbe o delovanju Evropske unije (PDEU), je dodatno izboljšati odpornost javnih in zasebnih subjektov, pristojnih organov in Unije kot celote ter njihove zmogljivosti za odzivanje na incidente.
3. V Evropskem parlamentu je za predlog pristojen Odbor za industrijo, raziskave in energetiko (ITRE). Odbor ITRE je poročilo poročevalca sprejel 28. oktobra 2021.
4. Evropski ekonomsko-socialni odbor je mnenje sprejel 28. aprila 2021.
5. Odbor stalnih predstavnikov je 3. februarja 2021 sklenil, da se bo o predlogu⁴ posvetoval z Evropskim odborom regij. Evropski odbor regij zaenkrat še ni podal mnenja.
6. Evropski nadzornik za varstvo podatkov je mnenje sprejel 11. marca 2021⁵.
7. Svet se je v svojih sklepih⁶ z dne 22. marca 2021 o strategiji EU za kibernetiko varnost v digitalnem desetletju seznanil z novim predlogom, ki temelji na direktivi o varnosti omrežij in informacijskih sistemov, ter ponovno izrazil podporo krepitvi in harmonizaciji nacionalnih okvirov kibernetike varnosti in trajnemu sodelovanju med državami članicami.
8. Evropski svet je v svojih sklepih z dne 21. in 22. oktobra 2021 pozval k nadaljevanju dela v zvezi s predlogom za revidirano direktivo o varnosti omrežij in informacij.

³ 14133/20.

⁴ 5573/21.

⁵ Mnenje 5/2021 o strategiji za kibernetiko varnost in revidirani direktivi o varnosti omrežij in informacij.

⁶ 6722/21.

II. DELO V PRIPRAVLJALNIH TELESIH SVETA

9. Predlog v Svetu obravnava Horizontalna delovna skupina za kibernetika vprašanja (v nadaljnjem besedilu: delovna skupina HWPCI). Predlog je začela preučevati 19. januarja med portugalskim predsedovanjem z natančno obravnavo predloga, med katero so države članice imele priložnost, da postavijo vprašanja in izpostavijo glavne pomisleke ter od Komisije prejmejo podrobna pojasnila o spremembah v revidirani direktivi.
10. Delovna skupina HWPCI je med portugalskim predsedovanjem predstavitvi in obravnavi predloga posvetila 17 sej. Poročilo o napredku pri obravnavi je bilo predloženo Svetu PTE 4. junija 2021.
11. Med slovenskim predsedovanjem se je delo nadaljevalo in okrepilo s ciljem, da bi na seji Sveta (promet, telekomunikacije in energija) 3. decembra 2021 dosegli dogovor o splošnem pristopu. Slovensko predsedstvo je predlogu za revidirano direktivo o varnosti omrežij in informacij namenila 15 sej in številne dvostranske razprave na vseh ravneh.
12. Delovna skupina HWPCI se je pri svojem preoblikovanju besedila predloga osredotočila najprej na interakcijo revidirane direktive o varnosti omrežij in informacij s sektorsko zakonodajo in področjem uporabe, zlasti kar zadeva javno upravo, korenske strežnike DNS in izključitveno klavzulo, nato pa med drugim na medsebojni strokovni pregled, sodne pristojnosti in medsebojno pomoč, usklajeno razkrivanje šibkih točk, podatkovne zbirke domenskih imen in podatke o registraciji ter mednarodnem sodelovanju itd.
13. Prvi kompromisni predlog besedila predlagane direktive je bil objavljen 21. septembra 2021⁷ na podlagi pisnih pripomb in delovnih dokumentov držav članic ter predhodnih kompromisnih predlogov o interakciji revidirane direktive o varnosti omrežij in informacij s sektorsko zakonodajo ter o področju uporabe zadevne direktive.

⁷ 12019/21.

14. Delovna skupina je o zadnji reviziji⁸ kompromisnega predloga predsedstva razpravljala 22. novembra 2021. Delegacije so na splošno pozdravile kompromisno besedilo, nekatere pa so še vedno izrazile preučitvene pridržke ali pripombe o delih kompromisnega predloga. Predlagano je bilo še nekaj tehničnega preoblikovanja določenih delov besedila.

III. VSEBINA

15. Na podlagi razprav delovne skupine so bile kot glavna politična vprašanja opredeljene naslednje točke:

a) Področje uporabe (člen 2)

Od začetka razprav o predlogu revidirane direktive o varnosti omrežij in informacij je bil glavni pomislek držav članic znatno povečanje števila subjektov, ki jih zajema direktiva, in zlasti uvedba pravila omejitve velikosti, v skladu s katerim vsi srednji in veliki subjekti, ki delujejo v sektorjih ali opravljajo storitve, ki jih zajema revidirana direktiva o varnosti omrežij in informacij, spadajo v njeno področje uporabe. Kompromisni predlog ohranja to splošno pravilo, hkrati pa vključuje dodatne določbe za zagotovitev potrebne sorazmernosti, večjo stopnjo obvladovanja tveganj in jasna merila kritičnosti za ugotavljanje, ali subjekti spadajo v področje uporabe direktive. Poleg tega kompromisni predlog vključuje posebne določbe o prednostni razvrstitvi uporabe nadzornih ukrepov na podlagi pristopa, ki temelji na tveganju.

⁸ 12019/5/21 REV 5.

b) Javna uprava (člen 2(2a))

Vključitev javne uprave v področje uporabe revidirane direktive o varnosti omrežij in informacij je bila predmet intenzivnih razprav, saj se sektor javne uprave razlikuje od drugih sektorjev, ki jih zajema revidirana direktiva. Predsedstvo si je prizadevalo za uravnotežen pristop, ki upošteva posebnosti nacionalnih okvirov javne uprave in državam članicam zagotavlja določeno stopnjo prožnosti pri določanju subjektov javne uprave, ki spadajo v področje uporabe revidirane direktive. Zato se v kompromisnem besedilu revidirane direktive ta uporablja za subjekte javne uprave na centralni ravni, države članice pa lahko določijo tudi, da se revidirana direktiva uporablja za subjekte javne uprave na regionalni in lokalni ravni.

c) Izključitvena klavzula (člen 2, točki 3a in 3aa)

Države članice so želele dodatno pojasniti izključitveno klavzulo, saj se direktiva ne uporablja za subjekte, ki opravljajo predvsem dejavnosti na področju obrambe, nacionalne varnosti, javne varnosti ali kazenskega pregona, ali za dejavnosti v zvezi z nacionalno varnostjo ali obrambo. Izključeni so tudi sodstvo, parlamenti in centralne banke.

d) Interakcija s sektorsko zakonodajo

Države članice so poudarile, da je treba revidirano direktivo o varnosti omrežij in informacij uskladiti s sektorsko zakonodajo, zlasti z uredbo o digitalni operativni odpornosti v finančnem sektorju (DORA) in direktivo o odpornosti kritičnih subjektov. Revidirana direktiva o varnosti omrežij in informacij, ki bi morala biti izhodišče za minimalno harmonizacijo na področju kibernetске varnosti, vsebuje poseben člen o sektorskih aktih Unije (člen 2b). Kar zadeva interakcijo z direktivo o odpornosti kritičnih subjektov, kompromisni predlog zagotavlja večjo jasnost glede pristopa, ki vključuje vse nevarnosti. Drugi pomembni dodatki so povezani z dogovori o sodelovanju med organi, pristojnimi na podlagi ustreznih pravnih aktov.

e) Vzajemno učenje (člen 16)

Razen nekaterih izjem so države članice nasprotovale temu, da bi Komisija uvedla obvezne medsebojne strokovne preglede. Predlagani kompromis zagotavlja, da novi mehanizem vzajemnega učenja temelji na vzajemnem zaupanju ter je prostovoljen proces, ki ga vodijo države članice.

f) Sodna pristojnost in teritorialnost (člen 24) ter medsebojna pomoč (člen 34)

Države članice so izrazile pomisleke glede posledic diferenciranja sodnih pristojnosti za subjekte v sektorju IKT, kot je predlagala Komisija. V kompromisnem besedilu je pojasnjena sodna pristojnost glede na vrsto subjektov, poleg tega pa je odločnejše tudi besedilo o medsebojni pomoči.

g) Obveznosti poročanja (člen 20)

Ker so države članice izrazile pomisleke, da bi to preobremenilo subjekte, ki jih zajema revidirana direktiva o varnosti omrežij in informacij, in vodilo v prekomerno poročanje, je bilo obvezno poročanje o pomembnih kibernetiskih grožnjah izključeno iz kompromisnega besedila.

IV. ZAKLJUČEK

16. Odbor stalnih predstavnikov je 24. novembra 2021 dosegel dogovor o kompromisnem besedilu iz priloge in odločil, da ga predloži Svetu (promet, telekomunikacije in energija), da ta sprejme splošni pristop.
17. Svet naj zato na seji 3. decembra 2021 odobri priloženo kompromisno besedilo predsedstva in sprejme splošni pristop.

Predlog

DIREKTIVA EVROPSKEGA PARLAMENTA IN SVETA

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

(Besedilo velja za EGP)

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

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

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora⁹,

ob upoštevanju mnenja Odbora regij¹⁰,

v skladu z rednim zakonodajnim postopkom,

⁹ UL C , , str. .

¹⁰ UL C , , str. .

ob upoštevanju naslednjega:

- (1) Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta¹¹ je bila namenjena razvoju zmogljivosti za kibernetko 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 takšnih storitev pri spoprijemanju s kibernetскими incidenti, s čimer naj bi prispevala k učinkovitemu delovanju gospodarstva in družbe Unije.
- (2) Od začetka veljavnosti Direktive (EU) 2016/1148 je bil dosežen velik napredek pri zviševanju ravni kibernetске odpornosti v Uniji. Pregled navedene direktive je pokazal, da se je uporabljala kot katalizator za institucionalni in regulativni pristop h kibernetски varnosti v Uniji, s čimer je utrla pot do velike spremembe v mišljenju. Direktiva je zagotovila dokončanje nacionalnih okvirov z opredelitvijo nacionalnih strategij za [...] **varnost omrežij in informacijskih sistemov**, vzpostavitev nacionalnih zmogljivosti in izvajanjem regulativnih ukrepov, ki so zajemali bistvene infrastrukture in akterje, ki so jih določile posamezne države članice. Prispevala je tudi k sodelovanju na ravni Unije z ustanovitvijo skupine za sodelovanje¹² in [...] mreže nacionalnih skupin za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: mreža skupin CSIRT)¹³. Kljub navedenim dosežkom pa so bile pri pregledu Direktive (EU) 2016/1148 razkrite pomanjkljivosti, zaradi katerih z navedeno direktivo ni mogoče učinkovito obravnavati sedanjih in nastajajočih izzivov na področju kibernetске varnosti.

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

¹² Člen 11 Direktive (EU) 2016/1148.

¹³ Člen 12 Direktive (EU) 2016/1148.

- (3) Omrežja in informacijski sistemi so se razvili v osrednjo značilnost vsakdanjega življenja s hitro digitalno preobrazbo in medsebojno povezanostjo družbe, vključno s čezmejnimi izmenjavami. Ta razvoj je privedel do razširitve okolja kibernetских groženj, s čimer so se pojavili novi izzivi, ki zahtevajo prilagojene, usklajene in inovativne odzive v vseh državah članicah. Število, obseg, izpopolnjenost, pogostost in vpliv kibernetских incidentov so vse večji ter pomenijo veliko grožnjo delovanju omrežij in informacijskih sistemov. Posledično lahko kibernetски incidenti ovirajo gospodarske dejavnosti na notranjem trgu, ustvarjajo finančne izgube, slabijo zaupanje uporabnikov ter povzročajo veliko škodo gospodarstvu in družbi Unije. Pripravljenost in učinkovitost na področju kibernetiske varnosti sta zato zdaj pomembnejši za ustrezno delovanje notranjega trga kot kdaj koli prej.
- (4) Pravna podlaga Direktive (EU) 2016/1148 je bil člen 114 Pogodbe o delovanju Evropske unije (PDEU), katerega cilj je vzpostavitev in delovanje notranjega trga z okrepitevijo ukrepov za približevanje nacionalnih pravil. Zahteve glede kibernetiske varnosti, ki jih morajo izpolnjevati subjekti, ki opravljajo storitve ali gospodarsko pomembne dejavnosti, se med državami članicami močno razlikujejo v smislu vrste zahtev, njihove ravni podrobnosti in metode nadzora. Te razlike povzročajo dodatne stroške in ustvarjajo težave za podjetja, ki ponujajo blago ali storitve čezmejno. Zahteve, ki jih naloži ena država članica in ki se razlikujejo od zahtev, ki jih naloži druga država članica, ali so celo v nasprotju z njimi, lahko bistveno vplivajo na takšne čezmejne dejavnosti.

Poleg tega bo možnost neoptimalnega oblikovanja ali izvajanja [...] **ukrepov** kibernetске varnosti v eni državi članici verjetno vplivala na raven kibernetске varnosti drugih držav članic, zlasti glede na intenzivne čezmejne izmenjave. Pregled Direktive (EU) 2016/1148 je pokazal velike razlike v njenem izvajanju v državah članicah, tudi v zvezi z njenim področjem uporabe, katerega razmejitev je bila v zelo veliki meri prepuščena presoji držav članic. Direktiva (EU) 2016/1148 je državam članicam zagotovila tudi zelo široko polje proste presoje, kar zadeva izvajanje obveznosti glede varnosti in poročanja o incidentih, določenih v Direktivi. Te obveznosti so se zato na nacionalni ravni izvajale na zelo različne načine. Podobne razlike pri izvajanju so se pojavile tudi v zvezi z določbami Direktive o nadzoru in izvrševanju.

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

- (6) [...] Države članice **bi morale imeti možnost**, da sprejmejo potrebne ukrepe, s katerimi zaščitijo bistvene interese svoje varnosti, javni red in javno varnost ter omogočijo preiskovanje, odkrivanje in pregon kaznivih dejanj[...]. [...] **Direktiva se ne bi smela uporabljati za določene javne ali zasebne subjekte, ki opravljajo dejavnosti na teh področjih. Prav tako se ne bi smela uporabljati za dejavnosti, ki jih subjekti opravljajo na teh področjih. Poleg tega** nobena država članica ni dolžna dajati informacij, katerih razkritje bi bilo v nasprotju z bistvenimi interesi njene javne varnosti. [...] **Pomembni so** nacionalna pravila [...] **ali** pravila Unije za varovanje tajnih podatkov, sporazumi o nerazkritju informacij ali neuradni sporazumi o nerazkritju informacij, kot je semaforski protokol (Traffic Light Protocol)¹⁴.
- (6a) **Pravo Unije o varstvu osebnih podatkov in zasebnosti se uporablja za vsakršno obdelavo osebnih podatkov na podlagi te direktive. Ta direktiva zlasti ne posega v Uredbo (EU) 2016/679 in Direktivo 2002/58/ES Evropskega parlamenta in Sveta ter zato zlasti ne bi smela vplivati na naloge in pooblastila neodvisnih nadzornih organov, pristojnih za spremljanje skladnosti z zadevnim pravom Unije o varstvu podatkov.**

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

- (7) Z razveljavitvijo Direktive (EU) 2016/1148 bi bilo treba področje uporabe po sektorjih razširiti na večji del gospodarstva, ob upoštevanju premislekov iz uvodnih izjav 4 do 6. Sektorje, zajete z Direktivo (EU) 2016/1148, bi bilo torej treba razširiti, da bi se zagotovila celovita pokritost sektorjev in storitev, ki so bistvenega pomena za ključne družbene in gospodarske dejavnosti na notranjem trgu. Pravila se ne bi smela razlikovati glede na to, ali so subjekti izvajalci bistvenih storitev ali ponudniki digitalnih storitev. Takšno razlikovanje se je izkazalo za zastarelo, saj ne odraža dejanskega pomena sektorjev ali storitev za družbene in gospodarske dejavnosti na notranjem trgu.
- (8) V skladu z Direktivo (EU) 2016/1148 so bile države članice odgovorne za določanje, kateri subjekti izpolnjujejo merila, v skladu s katerimi se štejejo za izvajalce bistvenih storitev („postopek določitve“). Za odpravo velikih razlik med državami članicami v zvezi s tem in zagotovitev pravne varnosti za zahteve glede obvladovanja tveganj in obveznosti poročanja za vse ustrezne subjekte bi bilo treba določiti enotno merilo, ki bi določalo, kateri subjekti spadajo na področje uporabe te direktive. Navedeno merilo bi moralo vključevati uporabo pravila omejitve velikosti, v skladu s katerim na področje uporabe te direktive spadajo vsa srednja in velika podjetja, kot so opredeljena v Priporočilu Komisije 2003/361/ES¹⁵, ki delujejo v sektorjih ali opravljajo vrsto storitev, zajetih s to direktivo. [...]

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

- (8a) **Da se zagotovi jasen pregled nad subjekti, ki spadajo na področje uporabe te direktive, bi morale imeti države članice možnost vzpostaviti nacionalne mehanizme za samopriglasitev, ki od subjektov, za katere velja ta direktiva, zahtevajo, da organom, pristojnim na podlagi te direktive, ali organom, ki jih za ta namen imenujejo države članice, predložijo vsaj svoje ime, naslov in kontaktne podatke, pa tudi sektor, v katerem delujejo, ali vrsto storitve, ki jo opravljajo, ter po potrebi seznam držav članic, v katerih subjekt opravlja svoje storitve. Kadar registri obstajajo na nacionalni ravni, se lahko države članice odločijo za ustrezne mehanizme, ki omogočajo določitev subjektov, ki spadajo na področje uporabe te direktive.**
- (9) [...] S to direktivo bi morali biti zajeti tudi **mikro- ali mali subjekti**, ki izpolnjujejo nekatera merila, ki kažejo na ključno vlogo za gospodarstvo ali družbo držav članic ali za določene sektorje ali vrste storitev. Države članice bi morale biti odgovorne, **da [...] Komisiji [...] predložijo vsaj ustrezne informacije o številu določenih subjektov, sektorju, ki mu pripadajo, ali vrsti storitve, ki jo ponujajo, ter specifičnih meril, na podlagi katerih so bili določeni. Države članice se lahko v skladu z nacionalnimi varnostnimi predpisi odločijo, da Komisiji predložijo imena teh subjektov.**
- (9a) **Subjekti javne uprave, ki opravljajo dejavnosti na področjih nacionalne varnosti, obrambe, javne varnosti, kazenskega pregona ter sodstva, parlamenti in centralne banke so izključeni iz področja uporabe te direktive. Za namene te direktive se za subjekte z regulativno pristojnostjo ne šteje, da opravljajo dejavnosti na področju kazenskega pregona, zato niso izključeni iz področja uporabe te direktive iz tega razloga. Poleg tega subjekti javne uprave na centralni ravni, ki so ustanovljeni skupaj s tretjo državo v skladu z mednarodnim sporazumom, ne spadajo na področje uporabe te direktive.**

- (9aa) **Države članice bi morale imeti možnost določiti, 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.**
- (9aaa) **Ta direktiva se ne uporablja za diplomatska in konzularna predstavništva držav članic v tujini ter za njihovo infrastrukturo IKT, ki jo uporabljajo ta predstavništva, če se ta infrastruktura nahaja v tujini ali se uporablja za uporabnike v tujini.**
- (10) Komisija lahko v sodelovanju s skupino za sodelovanje izda usmeritve o izvajanju meril, ki se uporabljajo za mikro- in mala podjetja.
- (11) [...] **Subjekti, ki spadajo na področje uporabe te direktive, bi morali biti razvrščeni v dve kategoriji: bistveni in pomembni, pri čemer se upoštevata raven kritičnosti sektorja ali vrste storitev, ki jih opravljajo, ter njihova velikost. V zvezi s tem bi bilo treba po potrebi ustrezno upoštevati tudi vse ustrezne sektorske ocene tveganja ali usmeritve pristojnih organov.** Za bistvene in pomembne subjekte bi morale veljati [...] zahteve glede obvladovanja tveganj in obveznosti poročanja. Pri teh dveh kategorijah subjektov bi bilo treba razlikovati med ureditvijo nadzora in ureditvijo kazni, da bi se zagotovilo ustrezno ravnovesje med zahtevami **na podlagi tveganj** in obveznostmi na eni strani ter upravnim bremenom, ki izhaja iz nadzora nad izpolnjevanjem zahtev in obveznosti, na drugi strani.

- (12) **Ta direktiva določa izhodišče za ukrepe za obvladovanje tveganj za kibernetško varnost in obveznosti poročanja v vseh sektorjih, ki spadajo na njeno področje uporabe. Da bi preprečili razdrobljenost določb pravnih aktov Unije o kibernetški varnosti, bi morala Komisija, kadar se šteje, da so za zagotavljanje visoke ravni kibernetške varnosti potrebne dodatne sektorske določbe glede obvladovanja tveganj za kibernetško varnost in obveznosti poročanja, oceniti, ali bi se takšne določbe lahko določile v izvedbenem aktu na podlagi pooblastila iz te direktive. Če takšni akti ne bi bili primerni za to, bi sektorska zakonodaja lahko prispevala k zagotavljanju visoke ravni [...] kibernetške varnosti, ob polnem upoštevanju posebnosti in kompleksnosti zadevnih sektorjev. Če izvedbeni akt na podlagi pooblastila iz te direktive ni ustrezen, je treba to utemeljiti v sektorski zakonodaji. Hkrati bi bilo treba pri takšnih sektorskih določbah pravnih aktov Unije ustrezno upoštevati potrebo po celovitem in harmoniziranem okviru za kibernetško varnost. [...] To ne posega v obstoječa izvedbena pooblastila, ki so bila podeljena Komisiji v številnih sektorjih, vključno s prometnim in energetske.**

(12a) Če sektorski pravni akt Unije vsebuje določbe[...], ki od bistvenih ali pomembnih subjektov zahtevajo, da sprejmejo ukrepe, ki so po učinku vsaj enakovredne obveznostim iz te direktive v zvezi z ukrepi za obvladovanje tveganja za kibernetško varnost [...] in obveznostmi prigrasitve pomembnih incidentov ali pomembnih kibernetških groženj[...], bi se morale uporabljati navedene sektorske določbe, vključno z določbami o nadzoru in izvrševanju. Pri določanju enakovrednega učinka obveznosti iz sektorskih določb pravnega akta Unije bi bilo treba upoštevati naslednje vidike: (i) ukrepe za obvladovanje tveganj za kibernetško varnost bi morali sestavljati ustrezni in sorazmerni tehnični in organizacijski ukrepi za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih zadevni subjekti uporabljajo pri opravljanju svojih storitev, vključevati pa bi morali vsaj vse elemente iz te direktive; (ii) obveznost prigrasitve pomembnih incidentov in kibernetških groženj bi morala biti vsaj enakovredna obveznostim iz te direktive, kar zadeva vsebino, obliko in časovnico prigrasitev; (iii) načini poročanja subjektov in ustreznih organov o sektorskih pravnih aktih Unije bi morali biti vsaj enakovredni zahtevam iz te direktive glede njihove vsebine, oblike in časovnic ter bi morali upoštevati vlogo skupin CSIRT; (iv) zahteve za čezmejno sodelovanje za zadevne organe bi morale biti vsaj enakovredne zahtevam iz te direktive. Če sektorske določbe pravnega akta Unije ne zajemajo 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 niso zajeti v teh sektorskih določbah.

- (12aa)** Komisija bi morala redno pregledovati, kako se uveljavlja zahteva po enakovrednem učinku v zvezi s sektorskimi določbami pravnih aktov Unije[...]. Komisija se mora pri pripravi rednega pregleda posvetovati s skupino za sodelovanje.
- (12aaa)** Prihodnji sektorski pravni akti Unije bi morali ustrezno upoštevati opredelitve pojmov iz člena 4 te direktive ter nadzorni in izvršilni okvir iz poglavja VI te direktive.
- (12ab)** Kadar sektorske določbe pravnih aktov Unije od bistvenih ali pomembnih subjektov zahtevajo, da sprejmejo ukrepe, ki imajo vsaj enakovreden učinek kot obveznosti poročanja iz te direktive, bi se bilo treba izogibati prekrivanju obveznosti poročanja ter zagotoviti skladnost in učinkovitost obravnave prigrasitev kibernetičkih groženj ali incidentov. V ta namen lahko navedene sektorske določbe državam članicam omogočijo, da vzpostavijo skupen, samodejen in neposreden mehanizem poročanja za prigrasitev pomembnih incidentov in kibernetičkih groženj organom, katerih naloge so določene v zadevnih sektorskih določbah, in pristojnim organom, vključno z enotno kontaktno točko in skupinami CSIRT, kot je ustrezno, ki so odgovorni za naloge na področju kibernetičke varnosti iz te direktive, ali mehanizem, ki zagotavlja sistematično in takojšnjo izmenjavo informacij in sodelovanje med ustreznimi organi in skupinami CSIRT v zvezi z obravnavanjem takšnih prigrasitev. Za poenostavitev poročanja in izvajanje skupnega, samodejnega in neposrednega mehanizma poročanja lahko države članice v skladu s sektorsko zakonodajo uporabljajo enotno vstopno točko, ki jo vzpostavijo v skladu s členom 11(5a) te direktive. Za zagotovitev harmonizacije bi bilo treba obveznosti poročanja v sektorskih pravnih aktih Unije uskladiti s tistimi, ki so določene v tej direktivi. Države članice lahko v skladu s sektorsko zakonodajo določijo, da so naslovniki poročanja organi, pristojni na podlagi te direktive, ali nacionalne skupine CSIRT .

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

(13a) Da bi se izognili vrzelim in podvajanju obveznosti glede kibernetске varnosti, ki veljajo za subjekte v letalskem sektorju iz točke 2(a) Priloge I, bi morali nacionalni organi, imenovani v skladu z uredbama (ES) št. 300/2008¹⁶ in (EU) 2018/1139¹⁷ Evropskega parlamenta in Sveta, ter organi, pristojni na podlagi te direktive, sodelovati pri izvajanju ukrepov za obvladovanje tveganj za kibernetско varnost in nadzoru teh ukrepov na nacionalni ravni. Nacionalni organi, imenovani v skladu z uredbama (ES) št. 300/2008 in (EU) 2018/1139, [...] bi lahko šteli, da s tem, ko subjekt izpolnjuje ukrepe za obvladovanje tveganj za kibernetско varnost iz te direktive, izpolnjuje tudi zahteve iz navedenih uredb ter iz ustreznih delegiranih in izvedbenih aktov, sprejetih na podlagi navedenih uredb.

¹⁶ 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).

¹⁷ 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).

- (14) Glede na prepletenost kibernetске varnosti in fizične varnosti subjektov bi bilo treba zagotoviti skladen pristop med Direktivo (EU) XXX/XXX Evropskega parlamenta in Sveta in to direktivo. Za dosego tega bi morale države članice zagotoviti, da se kritični subjekti [in enakovredni subjekti] v skladu z Direktivo (EU) XXX/XXX štejejo [...] za bistvene subjekte po tej direktivi. Države članice bi morale tudi zagotoviti, da njihove strategije za kibernetско varnost določajo okvir politike za okrepljeno usklajevanje med organom, pristojnim na podlagi te direktive, in organom, pristojnim na podlagi Direktive (EU) XXX/XXX, v okviru izmenjave informacij o incidentih in kibernetских grožnjah ter izvajanje nadzornih nalog.
- Pristojni o[...]rgani iz obeh direktiv bi morali sodelovati in si izmenjevati informacije, zlasti v zvezi z določanjem kritičnih subjektov, kibernetскими grožnjami, tveganji za kibernetско varnost in incidenti na področju kibernetске varnosti **ter nekibernetскими tveganji, grožnjami in incidenti**, ki vplivajo na kritične subjekte [ali subjekte, ki so jim enakovredni], [...] vključno z ukrepi za kibernetско varnost in fizičnimi ukrepi, ki jih sprejmejo kritični subjekti, **ter rezultati nadzornih dejavnosti, opravljenih v zvezi s takšnimi subjekti. Poleg tega bi si morali pristojni organi za racionalizacijo nadzornih dejavnosti med pristojnimi organi, imenovanimi v skladu z obema direktivama, in za zmanjšanje upravnega bremena za zadevne subjekte prizadevati za harmonizacijo predlog za prigrasitev incidentov in nadzornih postopkov.**** [...] Organi, pristojni na podlagi Direktive (EU) XXX/XXX,[...] **lahko po potrebi zahtevajo**, da organi, pristojni na podlagi te direktive,[...] izvajajo svoja nadzorna in izvršilna pooblastila v zvezi z bistvenim subjektom, ki je določen kot kritičen.[...] [...]

- (14a) Subjekti, ki spadajo v sektor digitalne infrastrukture, v bistvu temeljijo na omrežjih in informacijskih sistemih, zato bi morale obveznosti, ki jih tem subjektom nalaga ta direktiva, celovito obravnavati fizično varnost takšnih sistemov kot del njihovih obveznosti obvladovanja tveganj za kibernetско varnost in poročanja. Ker so te zadeve zajete v tej direktivi, se obveznosti iz poglavij III do VI Direktive (EU) XXX/XXX [direktiva o odpornosti kritičnih subjektov] ne uporabljajo za takšne subjekte.
- (15) Podpiranje in ohranjanje zanesljivega, odpornega in varnega sistema domenskih imen (DNS) sta ključna dejavnika pri ohranjanju celovitosti interneta ter bistvena za njegovo neprekinjeno in stabilno delovanje, od katerega sta odvisna digitalno gospodarstvo in družba. Zato bi se morala ta direktiva uporabljati za [...] ponudnike storitev sistema domenskih imen vzdolž verige **zagotavljanja DNS in** razreševanja DNS, **ki so pomembni za notranji trg**, vključno z [...] **registri** vrhnjih domenskih imen[...], **subjekti, ki zagotavljajo storitve registracije domenskih imen, upravljavci** krovnih imenskih strežnikov za domenska imena in **upravljavci** rekurzivnih razreševalnikov. **Izraz „ponudnik storitev sistema domenskih imen (DNS)“ se ne bi smel uporabljati za storitve sistema domenskih imen, ki se izvajajo za lastne namene zadevnega subjekta in njegovih pridruženih subjektov.** Obveznosti glede kibernetске varnosti, ki izhajajo iz te direktive za to kategorijo ponudnikov, so strogo omejene na ukrepe za obvladovanje tveganj za kibernetско varnost in poročanje, zato ne posegajo v to, kako skupnost več zainteresiranih strani upravlja globalni DNS .

- (16) Storitve računalništva v oblaku bi morale zajemati storitve, ki omogočajo upravljanje na zahtevo in širok oddaljeni dostop do prožnega in po obsegu prilagodljivega nabora deljivih in porazdeljenih računalniških virov. Ti računalniški viri obsegajo vire, kot so omrežja, strežniki ali druga infrastruktura, operacijski sistemi, programska oprema, pomnilniki, aplikacije in storitve. **Modeli 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. Zgoraj navedene storitve in modeli uvajanja imajo enak pomen kot izrazi za storitve in modele uvajanja, opredeljeni v standardu ISO/IEC 17788:2014. Zmožnost uporabnika računalništva v oblaku, da enostransko sam sebi 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 takšne 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 takšne računalniške vire, ki se zagotavljajo več uporabnikom, ki imajo skupen dostop do storitve, vendar obdelava poteka ločeno za vsakega uporabnika, čeprav se storitev zagotavlja z isto elektronsko opremo. Izraz „porazdeljeni“ se uporablja za opis računalniških virov, ki so na različnih omrežnih računalnikih ali napravah ter ki medsebojno komunicirajo in se usklajujejo z izmenjevanjem sporočil.

- (17) Zaradi pojava inovativnih tehnologij in novih poslovnih modelov se pričakuje, da se bodo na trgu pojavili novi modeli uvajanja in storitev računalništva v oblaku v odziv na razvijajoče se potrebe strank. V tem okviru se lahko storitve računalništva v oblaku zagotavljajo v zelo porazdeljeni obliki, še bližje lokaciji, kjer se podatki pridobivajo ali zbirajo, kar pomeni premik s tradicionalnega modela na zelo porazdeljen model („računalništvo na robu“).
- (18) Storitve, ki jih ponujajo ponudniki storitev podatkovnih centrov, se morda ne zagotavljajo vedno v obliki storitve računalništva v oblaku. Zato podatkovni centri morda niso vedno del infrastrukture računalništva v oblaku. Za obvladovanje vseh tveganj za varnost omrežij in informacijskih sistemov bi morala ta direktiva zajemati tudi ponudnike takšnih storitev podatkovnih centrov, ki niso storitve računalništva v oblaku. V tej direktivi bi moral izraz „storitev podatkovnega centra“ zajemati opravljanje storitve, ki vključuje strukture ali skupine struktur, namenjene centralizirani namestitvi, medsebojnemu povezovanju in delovanju opreme za informacijsko tehnologijo in omrežne opreme, za shranjevanje, obdelavo in prenos podatkov skupaj z vsemi zmogljivostmi in infrastrukturami za distribucijo električne energije in okoljski nadzor. Izraz „storitev podatkovnega centra“ se ne nanaša na podatkovne centre v podjetjih, ki so v lasti zadevnega subjekta, ki jih upravlja za lastne namene.
- (19) Ponudniki poštnih storitev v smislu Direktive 97/67/ES Evropskega parlamenta in Sveta¹⁸, [...] **tudi** [...] ponudniki [...] kurirskih storitev, bi morali biti predmet te direktive, če zagotavljajo vsaj en korak v verigi poštne dostave ter zlasti sprejem, usmerjanje ali dostavo, vključno s storitvami prevzema. Storitve prenosa, ki se ne izvajajo v povezavi z enim od navedenih korakov, ne bi smele spadati v obseg poštnih storitev.

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

- (20) Navedene vse večje medsebojne odvisnosti so rezultat vse bolj čezmejne in medsebojno odvisne mreže opravljanja storitev z uporabo ključnih infrastruktur po vsej Uniji v sektorjih energije, prometa, digitalne infrastrukture, pitne in odpadne vode, zdravja, nekaterih vidikov javne uprave in vesolja, kar zadeva opravljanje nekaterih storitev, ki so odvisne od talne infrastrukture, ki jih imajo v lasti, jih upravljajo in vodijo bodisi države članice bodisi zasebni subjekti, s čimer torej niso zajete infrastrukture, ki jih ima v lasti, jih upravlja ali vodi Unija ali ki so v lasti, se upravljajo ali vodijo v imenu Unije v okviru njenih vesoljskih programov. Te medsebojne odvisnosti pomenijo, da ima lahko kakršna koli motnja, tudi takšna, ki je prvotno omejena na en subjekt ali en sektor, širše kaskadne učinke, ki imajo lahko daljnosežne in dolgotrajne negativne učinke na opravljanje storitev na notranjem trgu. Pandemija COVID-19 je razkrila šibko točko naših vse bolj medsebojno odvisnih družb zaradi tveganj z majhno verjetnostjo.
- (20a) Za doseganje in ohranjanje visoke ravni kibernetске varnosti bi morali nacionalne strategije za kibernetско varnost, ki jih zahteva ta direktiva, sestavljati skladni okviri za upravljanje na področju kibernetске varnosti. Te strategije so lahko sestavljene iz enega ali več zakonodajnih ali nezakonodajnih dokumentov.**
- (21) Glede na razlike v nacionalnih strukturah upravljanja in zaradi varovanja že obstoječih sektorskih dogovorov ali nadzornih in regulativnih organov Unije bi morale imeti države članice možnost imenovati več kot en nacionalni pristojni organ, odgovoren za izvajanje nalog, povezanih z varnostjo omrežij in informacijskih sistemov bistvenih in pomembnih subjektov po tej direktivi. Države članice bi morale imeti možnost, da to vlogo dodelijo obstoječemu organu.

- (22) Za zagotavljanje lažjega čezmejnega sodelovanja in komunikacije med organi ter za učinkovito izvajanje te direktive je nujno, da vsaka država članica imenuje nacionalno enotno kontaktno točko, odgovorno za usklajevanje vprašanj v zvezi z varnostjo omrežij in informacijskih sistemov ter za čezmejno sodelovanje na ravni Unije.
- (23) Pristojni organi ali skupine CSIRT bi morali od subjektov učinkovito in uspešno prejeti priglasitve incidentov, **med drugim zato, da bi po potrebi olajšali pravočasen odziv na incidente in priglasitelju zagotovili odziv**. Enotne kontaktne točke bi morale biti zadolžene za posredovanje priglasitev incidentov enotnim kontaktnim točkam drugih prizadetih držav članic. [...]

- (23a) S sektorskimi pravnimi akti Unije, ki zahtevajo ukrepe za obvladovanje tveganj za kibernetško varnost ali obveznosti poročanja, ki so po učinku vsaj enakovredni tistim iz te direktive, bi se lahko določalo, da imenovani pristojni organi iz teh aktov izvajajo svoja nadzorna in izvršilna pooblastila v zvezi s takšnimi ukrepi ali obveznostmi s pomočjo pristojnih organov, imenovanih v skladu s to direktivo. Zadevni pristojni organi lahko v ta namen sklenejo dogovore o sodelovanju. V takšnih dogovorih bi lahko med drugim določili postopke 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 med pristojnimi organi o nadzoru in izvrševanju, vključno z dostopom do informacij v zvezi s kibernetško varnostjo, ki jih zahtevajo pristojni organi, imenovani v skladu s to direktivo.
- (24) Države članice bi morale imeti ustrezne tehnične in organizacijske zmogljivosti za preprečevanje, odkrivanje in ublažitev incidentov in tveganj v omrežjih in informacijskih sistemih ter za odzivanje nanje. Zato bi morale države članice zagotoviti, da imajo dobro delujoče skupine CSIRT, znane tudi kot skupine za odzivanje na računalniške grožnje (v nadaljnjem besedilu: skupine CERT), ki izpolnjujejo osnovne zahteve, da bi se tako zagotovile učinkovite in združljive zmogljivosti za obvladovanje incidentov in tveganj ter zagotovilo učinkovito sodelovanje na ravni Unije. Za okrepitev odnosa zaupanja med subjekti in skupinami CSIRT v primerih, ko je skupina CSIRT del pristojnega organa, [...] **lahko** države članice razmislijo o funkcionalnem ločevanju med operativnimi nalogami, ki jih opravljajo skupine CSIRT, zlasti v zvezi z izmenjavo informacij in podporo subjektom, in nadzornimi dejavnostmi pristojnih organov.

- (25) Kar zadeva osebne podatke, bi morale biti skupinam CSIRT omogočeno, da v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta¹⁹ v imenu in na zahtevo subjekta po tej direktivi zagotovijo proaktivni pregled omrežij in informacijskih sistemov, ki se uporabljajo za opravljanje storitev subjektov. **Po potrebi** bi si morale države članice prizadevati za zagotovitev enake ravni tehničnih zmogljivosti za vse sektorske skupine CSIRT. Države članice lahko pri oblikovanju nacionalnih skupin CSIRT zaprosijo za pomoč Agencijo Evropske unije za kibernetско varnost (ENISA).
- (26) Mednarodno sodelovanje na področju kibernetске varnosti je pomembno, zato bi morali skupinam CSIRT poleg sodelovanja v mreži skupin CSIRT, vzpostavljeni s to direktivo, omogočiti tudi sodelovanje v mrežah mednarodnega sodelovanja. **Skupine CSIRT in pristojni organi bi zato lahko izmenjali informacije, vključno z osebnimi podatki, s skupinami CSIRT tretjih držav ali njihovimi organi za namene izvajanja njihovih nalog v skladu z Uredbo (EU) 2016/679. Če ni sprejet sklep o ustreznosti v skladu s členom 45 Uredbe (EU) 2016/679 ali ni ustreznih zaščitnih ukrepov v skladu s členom 46 navedene uredbe, bi se lahko izmenjava osebnih podatkov, ki se šteje za potrebno za namene blažitve pomembnih kibernetских groženj in odzivanja na tekoč pomemben incident, štela za pomemben javni interes v smislu člena 49(1)(d) Uredbe (EU) 2016/679.**

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

- (27) V skladu s Prilogo k Priporočilu Komisije (EU) 2017/1548 o usklajenem odzivu na velike kibernetiske incidente in krize („načrt“)²⁰ bi moral velik incident pomeniti incident, ki pomembno vpliva na vsaj dve državi članici ali ki povzroči motnje, ki presegajo zmožnost države članice za odziv nanje. Glede na njihov vzrok in vpliv se lahko veliki incidenti stopnjujejo in sprevržejo v popolno krizo, ki ne omogoča ustreznega delovanja notranjega trga. Glede na velik obseg in večinoma čezmejno naravo takšnih incidentov bi morali države članice ter ustrezne institucije, organi in agencije Unije sodelovati na tehnični, operativni in politični ravni za ustrezno usklajevanje odziva po vsej Uniji.
- (28) Ker lahko izkoriščanje šibkih točk v omrežjih in informacijskih sistemih povzroči hude motnje in škodo, sta hitro odkrivanje in odpravljanje takšnih šibkih točk pomemben dejavnik pri zmanjševanju tveganj za kibernetisko varnost. Subjekti, ki razvijajo **ali upravljajo** takšne sisteme, bi morali zato vzpostaviti ustrezne postopke za obravnavanje šibkih točk, ko jih odkrijejo. Ker šibke točke pogosto odkrijejo in o njih poročajo (jih razkrijejo) tretje osebe (poročajoči subjekti), bi moral proizvajalec ali ponudnik proizvodov ali storitev IKT vzpostaviti tudi potrebne postopke za prejemanje informacij o šibkih točkah od tretjih oseb. V zvezi s tem mednarodna standarda ISO/IEC 30111 in ISO/IEC [...] **29147** določata usmeritve o obravnavanju oziroma razkrivanju šibkih točk. Kar zadeva razkrivanje šibkih točk, je pomembno zlasti usklajevanje med poročajočimi subjekti in proizvajalci ali ponudniki proizvodov ali storitev IKT. Usklajeno razkrivanje šibkih točk določa strukturiran postopek, s katerim se šibke točke organizacijam sporočijo tako, da lahko organizacija diagnosticira in odpravi šibko točko, preden se podrobne informacije o šibki točki razkrijejo tretji osebi ali javnosti. Usklajeno razkrivanje šibkih točk bi moralo vključevati tudi usklajevanje med poročajočim subjektom in organizacijo v zvezi s časovnim okvirom za odpravo in objavo šibkih točk.

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

- (29) Države članice bi morale zato sprejeti ukrepe za olajšanje usklajenega razkrivanja šibkih točk z vzpostavitvijo ustrezne nacionalne politike. **Države članice bi si morale v okviru svoje nacionalne politike prizadevati, da v skladu s svojim nacionalnim pravnim redom čim bolj obravnavajo izzive, s katerimi se soočajo raziskovalci šibkih točk, vključno z njihovo morebitno izpostavljenostjo kazenski odgovornosti.** [...] Države članice bi morale imenovati skupino CSIRT, ki bi prevzela vlogo „koordinatorke“ in ki bi po potrebi delovala kot posrednica med poročajočimi subjekti in proizvajalci ali ponudniki proizvodov ali storitev IKT. Naloge skupine CSIRT koordinatorke bi morale vključevati zlasti določitev zadevnih subjektov in vzpostavitev stika z njimi, podpiranje poročajočih subjektov, pogajanja o časovnicah razkrivanja in upravljanje razkrivanja šibkih točk, ki vplivajo na več organizacij (**usklajeno** razkrivanje šibkih točk več strani). Če **bi sporočene** šibke točke **lahko potencialno pomembno vplivale na subjekte** [...] v več državah članicah, bi morale imenovane skupine CSIRT [...] **po potrebi** sodelovati v okviru mreže skupin CSIRT.
- (30) Dostop do točnih in pravočasnih informacij o šibkih točkah, ki vplivajo na proizvode in storitve IKT, prispeva k okrepljenemu obvladovanju tveganj za kibernetско varnost. V zvezi s tem so viri javno dostopnih informacij o šibkih točkah pomembno orodje za subjekte in njihove uporabnike, pa tudi za nacionalne pristojne organe in skupine CSIRT. Zato bi morala agencija ENISA vzpostaviti register šibkih točk, kjer bi bistveni in pomembni subjekti ter njihovi dobavitelji, pa tudi subjekti, ki ne spadajo na področje uporabe te direktive, **ali imenovane skupine CSIRT** lahko prostovoljno razkrivali šibke točke in zagotavljali informacije o šibkih točkah, ki bi uporabnikom omogočale sprejetje ustreznih blažilnih ukrepov.

- (31) Čeprav podobni registri ali zbirke podatkov o šibkih točkah obstajajo, te upravljajo in vodijo subjekti, ki nimajo sedeža v Uniji. Evropski register šibkih točk, ki bi ga vodila agencija ENISA, bi zagotovil večjo preglednost v zvezi s postopkom objave pred uradnim razkritjem šibke točke in odpornost v primerih motenj ali prekinitev pri opravljanju podobnih storitev. Da bi preprečila podvajanje prizadevanj in poskušala zagotoviti čim večje dopolnjevanje, bi morala agencija ENISA preučiti možnost sklenitve sporazumov o strukturnem sodelovanju s podobnimi registri v jurisdikcijah tretjih držav. **Agencija ENISA bi morala zlasti preučiti možnost tesnega sodelovanja z upravljavci sistema splošnih šibkih točk in izpostavljenosti (CVE), pa tudi možnost, da postane organ za dodeljevanje korenskih števil CVE.**
- (32) **Skupina za sodelovanje bi morala še naprej podpirati in lajšati strateško sodelovanje in izmenjavo informacij ter krepiti zaupanje med državami članicami.** Skupina za sodelovanje bi morala vsaki dve leti pripraviti delovni program, ki bi vključeval ukrepe, ki bi jih skupina sprejela za izvajanje svojih ciljev in nalog. Časovni okvir prvega programa, sprejetega v skladu s to direktivo, bi moral biti usklajen s časovnim okvirom zadnjega programa, sprejetega v skladu z Direktivo (EU) 2016/1148, da bi se preprečile morebitne motnje pri delu skupine.
- (33) Skupina za sodelovanje bi morala pri pripravi usmeritev dosledno: evidentirati nacionalne rešitve in izkušnje, oceniti vpliv svojih dosežkov na nacionalne pristope, razpravljati o izzivih v zvezi z izvajanjem in oblikovati posebna priporočila, ki bi se obravnavala z boljšim izvajanjem obstoječih pravil.

- (34) Skupina za sodelovanje bi morala ostati prilagodljiv forum in biti sposobna odzivati se na spreminjajoče se in nove prednostne naloge politike in izzive, ob upoštevanju razpoložljivosti virov. Organizirati bi morala redne skupne sestanke z ustreznimi zasebnimi zainteresiranimi stranmi iz vse Unije, na katerih bi se razpravljalo o dejavnostih, ki jih izvaja skupina, in zbirale informacije o nastajajočih izzivih politike. Za okrepitev sodelovanja na ravni Unije bi morala skupina razmisliti o tem, da bi k sodelovanju pri svojem delu povabila organe in agencije Unije, vključene v politiko na področju kibernetске varnosti, kot so Evropski center za boj proti kibernetски kriminaliteti (EC3), Agencija Evropske unije za varnost v letalstvu (EASA) in Agencija Evropske unije za vesoljski program (EUSPA).
- (35) Pristojni organi in skupine CSIRT bi morali biti pooblaščeni za sodelovanje v programih izmenjave uradnikov iz drugih držav članic, da bi izboljšali sodelovanje. Pristojni organi bi morali sprejeti potrebne ukrepe, s katerimi bi uradnikom iz drugih držav članic omogočili učinkovito sodelovanje v dejavnostih pristojnega organa gostitelja.
- (35a) 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 kibernetске varnosti, kot je Europol.**
- (36) [...]

- (36a) Da bi države članice olajšale učinkovito izvajanje določb te direktive, kot so obvladovanje šibkih točk, obvladovanje tveganj za kibernetško varnost, ukrepi poročanja in dogovori o izmenjavi informacij, lahko sodelujejo s tretjimi državami in izvajajo dejavnosti, ki se štejejo kot ustrezne za ta namen, vključno z izmenjavo informacij o grožnjah, incidentih, šibkih točkah, orodjih in metodah, taktikah, tehnikah in postopkih, pripravljenostjo za obvladovanje kibernetских kriz in povezanimi vajami, usposabljanjem, vzpostavljanjem zaupanja in ureditvami za strukturirano izmenjavo informacij. Takšni dogovori o sodelovanju bi morali biti skladni s pravom Unije o varstvu podatkov.
- (37) Države članice bi morale prispevati k vzpostavitvi okvira EU za odzivanje na krize na področju kibernetške varnosti, določenega v Priporočilu (EU) 2017/1584, z obstoječimi mrežami za sodelovanje, zlasti **evropsko** organizacijsko mrežo za povezovanje v kibernetški krizi (EU-CyCLONe), mrežo skupin CSIRT in skupino za sodelovanje. Mreža EU-CyCLONe in mreža skupin CSIRT bi morali sodelovati na podlagi postopkovnih ureditev, v katerih so opredeljeni načini navedenega sodelovanja, **in se izogibati kakršnemu koli podvajanju nalog**. V poslovniku mreže EU-CyCLONe bi morali biti podrobneje opredeljeni načini delovanja mreže, med drugim z vlogami, načini sodelovanja, stiki z drugimi ustreznimi akterji in predlogami za izmenjavo informacij ter sredstvi komuniciranja. Za obvladovanje krize na **politični** ravni Unije bi se morale ustrezne strani zanašati na enotne ureditve za politično odzivanje na krize (IPCR). Komisija bi morala v ta namen uporabljati postopek medsektorskega kriznega usklajevanja na visoki ravni v okviru sistema ARGUS. Če bo imela kriza znaten vpliv na zunanjo ali skupno varnostno in obrambno politiko (SVOP), bi bilo treba sprožiti mehanizem Evropske službe za zunanje delovanje (ESZD) za krizno odzivanje.

- (37a) **Mreža EU-CyCLONe bi morala delovati kot posredniška mreža med tehnično in politično ravno v primeru obsežnih kibernetičnih incidentov in kriz. Okrepiti bi morala operativno sodelovanje, in sicer na podlagi ugotovitev mreže skupin CSIRT ter z uporabo lastnih zmogljivosti za pripravo analize učinka obsežnih incidentov in kriz ter podporo odločanju na politični ravni. Institucije, organi in agencije EU bi morali imenovati pristojni organ, odgovoren za upravljanje obsežnih varnostnih incidentov in kriz, da postane član mreže EU-CyCLONe.**
- (38) [...]
- (39) [...]
- (39a) **Za zagotavljanje varnosti omrežij 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 varnostnih ukrepov, ki ustrezajo trenutnim tveganjem.**
- (40) **Pri ukrepih za obvladovanje tveganj bi bilo treba upoštevati stopnjo odvisnosti subjekta od omrežij in informacijskih sistemov, mednje pa bi morali spadati ukrepi za prepoznavanje tveganj incidentov, preprečevanje, odkrivanje in obvladovanje incidentov ter ublažitev njihovega vpliva. Varnost omrežij in informacijskih sistemov bi morala obsegati varnost shranjenih, prenesenih in obdelanih podatkov.**

- (40a) Ker imajo lahko grožnje za varnost omrežij in informacijskih sistemov različen izvor, se v tej direktivi uporablja pristop, ki vključuje vse nevarnosti, tj. zaščito omrežij in informacijskih sistemov ter njihovega fizičnega okolja pred kakršnimi koli dogodki, kot so kraja, požar, poplave, izpadi telekomunikacij ali električne energije ali pred kakršnim koli nepooblaščenim fizičnim dostopom in poškodbami ali poseganjem v informacije 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 omrežij in informacijskih sistemov. Ukrepi za obvladovanje tveganj bi zato morali obravnavati tudi fizično in okoljsko varnost z vključitvijo ukrepov za zaščito omrežja in informacijskih sistemov subjekta pred okvarami sistemov, človeškimi napakami, zlonamernimi dejanji ali naravnimi pojavi v skladu z evropskimi ali mednarodno priznanimi standardi, kot so tisti iz serije ISO 27000. V zvezi s tem bi morali subjekti v okviru svojih ukrepov za obvladovanje tveganj obravnavati tudi varnost človeških virov in imeti vzpostavljene ustrezne politike za nadzor dostopa. Navedeni ukrepi bi morali biti skladni z Direktivo XXXX [direktiva o odpornosti kritičnih subjektov].**
- (40b) Če ni ustreznih evropskih certifikacijskih shem za kibernetsko varnost, sprejetih v skladu z Uredbo (EU) 2019/881, bi lahko države članice od subjektov zahtevale, da uporabljajo certificirane izdelke, storitve in postopke IKT ali pridobijo certifikat v okviru razpoložljivih nacionalnih shem za kibernetsko varnost za namene izpolnjevanja zahtev glede obvladovanja tveganj za kibernetsko varnost iz te direktive.**

- (41) Da bistvenim in pomembnim subjektom ne bi bilo naloženo nesorazmerno finančno in upravno breme, bi morale biti zahteve glede obvladovanja tveganj za kibernetško varnost sorazmerne s tveganjem [...] **za zadevno omrežje in informacijski sistem, pri čemer bi bilo treba upoštevati dovršenost takšnih ukrepov in stroške njihovega izvajanja. Ustrezno bi bilo treba upoštevati tudi velikost subjekta ter verjetnost pojava incidentov in njihovo resnost.**
- (41a) **Da bi zmanjšali regulativna bremena, bi morale biti zahteve za izvajanje ukrepov za obvladovanje tveganj za kibernetško varnost za srednje, male ali mikrosubjekte načeloma manj stroge, razen če bi merila kritičnosti ali nacionalne ocene tveganja upravičile strožje zahteve, zlasti v zvezi s subjekti, ki izpolnjujejo merila v zvezi s kritičnostjo iz te direktive.**
- (42) Bistveni in pomembni subjekti bi morali zagotoviti varnost omrežij in informacijskih sistemov, ki jih uporabljajo pri svojih dejavnostih. To so predvsem zasebna omrežja in informacijski sistemi, ki jih upravlja njihovo notranje osebje za IT ali za varnost katerih skrbi zunanji izvajalec. Zahteve glede obvladovanja tveganj za kibernetško varnost in poročanja v skladu s to direktivo bi se morale uporabljati za ustrezne bistvene in pomembne subjekte ne glede na to, ali vzdrževanje svojih omrežij in informacijskih sistemov izvajajo notranje ali ga oddajajo zunanjim izvajalcem.
- (42aa) **Ponudniki storitev sistema domenskih imen, registri vrhnjih domenskih imen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnih centrov, ponudniki omrežij za dostavo vsebine, ponudniki upravljanih storitev ter ponudniki upravljanih varnostnih storitev bi morali biti zaradi svoje čezmejne narave bolj harmonizirani na ravni Unije. Izvajanje ukrepov za kibernetško varnost bi bilo zato treba olajšati z izvedbenim aktom.**

- (43) Obravnavanje tveganj za kibernetško varnost, ki izhajajo iz dobavne verige subjekta in njegovega razmerja z njegovimi dobavitelji, je še zlasti pomembno glede na razširjenost incidentov, v katerih so bili subjekti žrtve kibernetških napadov in v katerih so bili zlonamerni akterji sposobni ogroziti varnost omrežij in informacijskih sistemov subjekta z izkoriščanjem šibkih točk, ki vplivajo na proizvode in storitve tretje osebe. Subjekti bi morali zato oceniti in upoštevati splošno kakovost proizvodov ter praks svojih dobaviteljev in ponudnikov storitev na področju kibernetške varnosti, vključno z njihovimi varnimi razvojnimi postopki.
- (44) Med ponudniki storitev imajo ponudniki upravljanih varnostnih storitev na področjih, kot so odzivanje na incidente, penetracijsko testiranje, varnostne presoje in svetovanje, še posebno pomembno vlogo pri zagotavljanju pomoči subjektom pri njihovih prizadevanjih za odkrivanje incidentov in odzivanje nanje. Vendar pa so bili takšni ponudniki upravljanih varnostnih storitev tudi sami tarče kibernetških napadov in zaradi svoje tesne vključenosti v delovanje izvajalcev pomenijo posebno tveganje za kibernetško varnost. Subjekti bi morali biti zato še bolj skrbni pri izbiri ponudnika upravljanih varnostnih storitev.
- (44a) Tudi nacionalni pristojni organi lahko v okviru svojih nadzornih nalog uporabljajo storitve kibernetške varnosti, kot so varnostne presoje in penetracijsko testiranje ali odzivanje na incidente. Da bi subjektom in nacionalnim pristojnim organom pomagali pri izbiri usposobljenih in zanesljivih ponudnikov storitev kibernetške varnosti, bi morala Komisija ob pomoči skupine za sodelovanje in agencije ENISA razmisliti o možnosti, da zahteva evropsko certifikacijsko shemo za kibernetško varnost v skladu s členom 48 Uredbe (EU) 2019/881.**

- (45) Subjekti bi morali obravnavati tudi tveganja za kibernetško varnost, ki izhajajo iz njihovih stikov in odnosov z drugimi zainteresiranimi stranmi v okviru širšega ekosistema. Subjekti bi morali zlasti sprejeti ustrezne ukrepe za zagotovitev, da njihovo sodelovanje z akademskimi in raziskovalnimi ustanovami poteka v skladu z njihovimi politikami na področju kibernetške varnosti, ob upoštevanju dobrih praks v zvezi z varnim dostopom in razširjanjem informacij na splošno ter še posebno z varstvom intelektualne lastnine. Podobno bi morali subjekti glede na pomen in vrednost podatkov za dejavnosti subjektov pri uporabi storitev pretvorbe podatkov in podatkovne analitike, ki jih opravljajo tretje osebe, sprejeti vse ustrezne ukrepe za kibernetško varnost.
- (46) Za nadaljnje obravnavanje ključnih tveganj za dobavno verigo ter zagotavljanje pomoči subjektom, ki delujejo v sektorjih, zajetih s to direktivo, pri ustreznem obvladovanju tveganj za kibernetško varnost, povezanih z dobavno verigo in dobavitelji, bi morala skupina za sodelovanje, ki vključuje ustrezne nacionalne organe, v sodelovanju s Komisijo in agencijo ENISA izvesti usklajene sektorske ocene tveganj v zvezi z dobavno verigo, kot je že storila za omrežja 5G na podlagi Priporočila (EU) 2019/534 o kibernetški varnosti omrežij 5G²¹, da bi za posamezne sektorje opredelila kritične storitve, sisteme ali proizvode IKT, zadevne grožnje in šibke točke.

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

- (47) Pri ocenah tveganj v zvezi z dobavno verigo bi bilo treba glede na značilnosti zadevnega sektorja upoštevati tehnične in, kjer je ustrezno, netehnične dejavnike, vključno z dejavniki, opredeljenimi v Priporočilu (EU) 2019/534, iz usklajene ocene tveganj za varnost omrežij 5G na ravni EU in nabora orodij EU za kibernetsko varnost omrežij 5G, o katerem se je dogovorila skupina za sodelovanje. Za opredelitev dobavnih verig, ki bi morale biti predmet usklajene ocene tveganja, bi bilo treba upoštevati naslednja merila: (i) obseg, v katerem bistveni in pomembni subjekti uporabljajo določene kritične storitve, sisteme ali proizvode IKT in se zanašajo nanje; (ii) pomembnost posameznih kritičnih storitev, sistemov ali proizvodov IKT za izvajanje kritičnih ali občutljivih funkcij, vključno z obdelavo osebnih podatkov; (iii) razpoložljivost alternativnih storitev, sistemov ali proizvodov IKT; (iv) odpornost celotne dobavne verige storitev, sistemov ali proizvodov IKT proti dogodkom, ki povzročajo motnje v delovanju, in (v) morebiten prihodnji pomen nastajajočih storitev, sistemov ali proizvodov IKT za dejavnosti subjektov.
- (48) Za racionalizacijo pravnih obveznosti, naloženih ponudnikom javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev in ponudnikom storitev zaupanja, povezanih z varnostjo njihovih omrežij in informacijskih sistemov, ter za omogočanje zadevnim subjektom in njihovim ustreznim pristojnim organom, da izkoristijo pravni okvir, vzpostavljen s to direktivo (vključno z imenovanjem skupine CSIRT, odgovorne za obvladovanje tveganj in incidentov, sodelovanje pristojnih organov pri delu skupine za sodelovanje in mreže skupin CSIRT), bi jih bilo treba vključiti na področje uporabe te direktive. Zato bi bilo treba razveljaviti ustrezne določbe iz Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta²² ter Direktive (EU) 2018/1972 Evropskega parlamenta in Sveta²³, ki se nanašajo na uvedbo zahtev glede varnosti in priglasitve za tovrstne subjekte.

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

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

(48a) Za obveznosti glede varnosti iz te direktive bi bilo treba šteti, da dopolnjujejo zahteve, naložene ponudnikom storitev zaupanja na podlagi Uredbe (EU) št. 910/2014 (uredba eIDAS). 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 varnostnih incidentih v skladu s to direktivo. Takšne obveznosti glede varnosti in poročanja bi se morale nanašati tudi na fizično zaščito opravljenih storitev. Še naprej se uporablja člen 24 Uredbe (EU) št. 910/2014.

(48aa) Države članice lahko vlogo pristojnih organov za storitve zaupanja dodelijo nadzornim organom eIDAS, da zagotovijo nadaljevanje sedanjih praks ter nadgradijo znanje in izkušnje, pridobljene pri uporabi uredbe eIDAS. Kadar je ta vloga dodeljena drugemu organu, bi morali nacionalni pristojni organi na podlagi te direktive pravočasno tesno sodelovati in si izmenjati ustrezne informacije, da se zagotovita učinkovit nadzor in skladnost ponudnikov storitev zaupanja z zahtevami iz te direktive in Uredbe [XXXX/XXXX].

Nacionalni pristojni organi na podlagi te direktive bi morali, kjer je ustrezno, nemudoma obvestiti nadzorni organ eIDAS o vsaki priglašeni pomembni kibernetiski grožnji ali incidentu, ki vpliva na storitve zaupanja, ter o vsakem primeru, ko ponudnik storitev zaupanja ne izpolnjuje zahtev na podlagi te direktive. 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 eIDAS in pristojnemu organu na podlagi te direktive. Pravila o obveznostih poročanja ne bi smela vplivati na Uredbo (EU) 2016/679 in Direktivo 2002/58/ES Evropskega parlamenta in Sveta²⁴.

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

- (49) Kjer je ustrezno in da bi se izognili nepotrebnim motnjam, bi bilo treba obstoječe nacionalne smernice, [...] sprejete za prenos pravil, povezanih z varnostnimi ukrepi, določenimi v členih 40 [...] in 41 Direktive (EU) 2018/1972 [...], **upoštevati pri ureditvah za prenos, ki jih izvedejo države članice v zvezi s to direktivo, pri tem pa graditi na že pridobljenem znanju in spretnostih v zvezi z ukrepi za obvladovanje varnostnih tveganj in prigrisativjo incidentov na podlagi Direktive (EU) 2018/1972. Da bi se olajšala harmonizacija in prehod ter bi bile motnje čim manjše, lahko agencija ENISA pripravi tudi usmeritve v zvezi z zahtevami glede varnosti in 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, da zagotovijo nadaljevanje sedanjih praks ter nadgradijo znanje in izkušnje, pridobljene na podlagi Direktive (EU) 2018/1972.**
- (50) Glede na vedno večji pomen medosebnih komunikacijskih storitev, neodvisnih od številke, je treba zagotoviti, da se tudi za take storitve uporabljajo ustrezne varnostne zahteve, ob upoštevanju njihove posebne narave in gospodarskega pomena. Ponudniki takih storitev bi torej prav tako morali zagotoviti raven varnosti omrežij in informacijskih sistemov, primerno obstoječemu tveganju. Ker ponudniki medosebnih komunikacijskih storitev, neodvisnih od številke, običajno nimajo dejanskega nadzora nad prenosom signalov prek omrežja, je mogoče raven tveganja za take storitve v nekaterih pogledih šteti za manjšo kot pri tradicionalnih elektronskih komunikacijskih storitvah. Enako velja za medosebne komunikacijske storitve, ki uporabljajo številke in nimajo dejanskega nadzora nad prenosom signalov.

- (51) Notranji trg je bolj odvisen od delovanja interneta kot kdaj koli prej. Storitve praktično vseh bistvenih in pomembnih subjektov so odvisne od storitev, ki se opravljajo prek interneta. Za zagotovitev nemotenega opravljanja storitev bistvenih in pomembnih subjektov je pomembno, da imajo javna elektronska komunikacijska omrežja, kot so na primer hrbtenična internetna omrežja ali podmorski komunikacijski kabli, vzpostavljene ustrezne ukrepe za kibernetško varnost in da poročajo o incidentih v zvezi z njo.
- (52) **Kjer je ustrezno, [...]** bi morali subjekti prejemnike svoje storitve obvestiti o specifičnih [...] ukrepih, ki jih lahko sprejmejo za ublažitev tveganja, **ki je posledica pomembne kibernetške groženje** njim samim. **Subjekti bi morali po potrebi in zlasti v primerih, ko se pomembna kibernetška grožnja lahko uresniči, o sami grožnji hkrati s pristojnimi organi ali skupinami CSIRT obvestiti tudi prejemnike svoje storitve.** Zahteva glede obveščanja zadevnih prejemnikov o takih grožnjah subjektov ne bi smela odvezati obveznosti, da na svoje stroške sprejmejo ustrezne in takojšnje ukrepe za preprečevanje ali odpravo vseh kibernetških groženj in ponovno vzpostavitev običajne ravni varnosti storitve. Zagotavljanje takih informacij o **kibernetških** [...] grožnjah prejemnikom bi moralo biti brezplačno.
- (53) Zlasti bi morali ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev prejemnike storitve obvestiti o specifičnih in pomembnih kibernetških grožnjah ter ukrepih, ki jih lahko sprejmejo za zagotovitev varnosti svojih komunikacij, na primer z uporabo posebnih vrst programske opreme ali tehnologij šifriranja.

- (54) Za zaščito varnosti elektronskih komunikacijskih omrežij in storitev bi bilo treba spodbujati uporabo šifriranja, zlasti šifriranja od konca do konca, ki bi moralo biti po potrebi obvezno za ponudnike takih storitev in omrežij v skladu z načeloma privzete in vgrajene varnosti ter zasebnosti za namene člena 18. Uporabo šifriranja od konca do konca bi bilo treba uskladiti s pooblastili države članice, da zagotovi zaščito svojih bistvenih varnostnih interesov in javne varnosti ter dovoli preiskovanje, odkrivanje in pregon kaznivih dejanj v skladu s pravom Unije. Pri rešitvah za zakonit dostop do informacij v komunikacijah, šifriranih od konca do konca, bi se morala ohraniti učinkovitost šifriranja pri varovanju zasebnosti in varnosti komunikacij ter hkrati zagotoviti učinkovit odziv na kazniva dejanja.
- (55) Direktiva določa dvostopenjski pristop k poročanju o incidentih za vzpostavitev ustreznega ravnovesja med, na eni strani, hitrim poročanjem, ki pomaga blažiti morebitno širjenje incidentov in omogoča subjektom, da zaprosijo za podporo, ter, na drugi strani, podrobnim poročanjem, pri katerem se pridobivajo dragocene izkušnje iz posameznih incidentov ter sčasoma poveča odpornost posameznih podjetij in celotnega sektorja proti kibernetiskim grožnjam. Kadar se subjekti seznanijo z incidentom, bi se moralo od njih zahtevati, da v 24 urah predložijo začetno priglasitev, ki ji najpozneje čez en mesec sledi končno poročilo. Začetna priglasitev bi morala vključevati le informacije, ki so nujno potrebne za seznaniitev pristojnih organov z incidentom in ki subjektu omogočajo, da po potrebi zaprosi za pomoč. V taki priglasitvi bi moralo biti, kjer je ustrezno, navedeno, ali je bil incident domnevno povzročen z nezakonitim ali zlonamernim dejanjem. Države članice bi morale zagotoviti, da se z zahtevo po predložitvi začetne priglasitve viri poročajočega subjekta ne preusmerijo z dejavnosti, povezanih z obvladovanjem incidentov, ki bi moralo biti prednostna naloga. Da bi države članice nadalje preprečile, da bi se zaradi obveznosti poročanja o incidentih bodisi viri preusmerili z upravljanja odzivov na incidente bodisi kako drugače ogrozila prizadevanja subjektov v zvezi s tem, bi morale tudi zagotoviti, da lahko zadevni subjekt v ustrezno utemeljenih primerih in v dogovoru s pristojnimi organi ali skupino CSIRT odstopa od rokov, tj. 24 ur za začetno priglasitev in enega meseca za končno poročilo.

- (55a) **Proaktiven pristop h kibernetским grožnjam je bistven element obvladovanja tveganj za kibernetško varnost, ki bi moral pristojnim organom omogočiti, da učinkovito preprečijo, da bi se kibernetške grožnje udeležile v dejanskih incidentih, ki lahko povzročijo znatne materialne ali nematerialne izgube. V ta namen je prigrasitev pomembnih kibernetških grožnjah ključnega pomena.**
- (56) Bistveni in pomembni subjekti so pogosto v položaju, ko je treba zaradi obveznosti prigrasitve, vključenih v različne pravne instrumente, o določenem incidentu zaradi njegovih značilnosti poročati različnim organom. Taki primeri ustvarjajo dodatna bremena in lahko tudi privedejo do negotovosti v zvezi z obliko in postopki takih prigrasitev. Glede na navedeno in za poenostavitev poročanja o varnostnih incidentih bi [...] **lahko** države članice vzpostavile *enotno vstopno točko* za vse prigrasitve, ki se zahtevajo na podlagi te direktive in tudi drugega prava Unije, kot sta Uredba (EU) 2016/679 in Direktiva 2002/58/ES. Agencija ENISA bi morala skupaj s skupino za sodelovanje s pomočjo smernic oblikovati skupne predloge prigrasitev, s katerimi bi se poenostavile in racionalizirale informacije za poročanje, ki se zahtevajo s pravom Unije, ter zmanjšala bremena za podjetja.
- (57) V primeru suma, da je incident povezan s hudimi kaznivimi dejanji po pravu Unije ali nacionalnem pravu, bi morale države članice bistvene in pomembne subjekte na podlagi veljavnih pravil o kazenskem postopku v skladu s pravom Unije spodbujati, da incident, za katerega sumijo, da je hudo kaznivo dejanje, prijavijo ustreznim organom kazenskega pregona. Kjer je ustrezno in brez poseganja v pravila o varstvu osebnih podatkov, ki se uporabljajo za Europol, je zaželeno, da Evropski center za boj proti kibernetški kriminaliteti (EC3) in agencija ENISA olajšata usklajevanje med pristojnimi organi in organi kazenskega pregona različnih držav članic.

- (58) V številnih primerih je zaradi incidentov ogrožena varnost osebnih podatkov. V tem okviru bi morali pristojni organi v skladu z Direktivo 2002/58/ES sodelovati in si izmenjevati informacije o vseh pomembnih zadevah z organi za varstvo podatkov in nadzornimi organi.
- (59) Vzdrževanje točnih in popolnih podatkovnih zbirk domenskih imen in podatkov o registraciji (tako imenovani podatki „WHOIS“) ter omogočanje zakonitega dostopa do takih podatkov sta bistveni za zagotavljanje varnosti, stabilnosti in odpornosti sistema domenskih imen, kar posledično prispeva k višji skupni ravni kibernetske varnosti v Uniji. Če obdelava vključuje osebne podatke, mora biti taka obdelava skladna s pravom Unije o varstvu podatkov.
- (60) Razpoložljivost in pravočasna dostopnost teh podatkov za javne organe, vključno s pristojnimi organi na podlagi prava Unije ali nacionalnega prava za preprečevanje, preiskovanje ali pregon kaznivih dejanj, skupine CERT [...] in skupine CSIRT ter, kar zadeva podatke njihovih strank, ponudnike elektronskih komunikacijskih omrežij in storitev ter ponudnike tehnologij in storitev kibernetske varnosti, ki delujejo v imenu zadevnih strank, sta bistveni za preprečevanje zlorab sistema domenskih imena in boj proti njim, zlasti za preprečevanje in odkrivanje kibernetskih incidentov ter odzivanje nanje. Pri takem dostopu bi bilo treba spoštovati pravo Unije o varstvu podatkov, če je povezan z osebnimi podatki.
- (61) Da bi zagotovili razpoložljivost točnih in popolnih podatkov o registraciji domenskih imen, bi morali registri vrhnjih domen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene (tako imenovani regulatorji), zbirati podatke o registraciji domenskih imen ter zagotavljati njihovo celovitost in razpoložljivost. **Kar zadeva podatke o registraciji, bi morali subjekti zlasti preveriti ime in elektronski naslov regulatorja.** [...] Registri vrhnjih domen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene, bi morali vzpostaviti politike in postopke za zbiranje in vzdrževanje točnih in popolnih podatkov o registraciji ter za preprečevanje in popravljanje netočnih podatkov o registraciji v skladu s pravili Unije o varstvu podatkov.

(62) Registri vrhnjih domen in subjekti, ki opravljajo storitve registracije domenskih imen zanje, bi morali objaviti podatke o registraciji domenskih imen, ki ne spadajo na področje uporabe pravil Unije o varstvu podatkov, kot so podatki, ki se nanašajo na pravne osebe²⁵. Registri vrhnjih domen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene, bi morali v skladu s pravom Unije o varstvu podatkov zakonit dostop do podatkov o registraciji posameznih domenskih imen v zvezi s fizičnimi osebami omogočiti tudi osebam, ki imajo upravičen razlog za dostop. Države članice bi morale zagotoviti, da se registri vrhnjih domen in subjekti, ki opravljajo storitve registracije domenskih imen zanje, brez nepotrebnega odlašanja odzovejo na zahteve [...] po razkritju podatkov o registraciji domenskih imen **s strani oseb, ki imajo upravičen razlog za dostop, kot so pristojni organi na podlagi prava Unije ali nacionalnega prava na področju nacionalne varnosti in kazenskega pravosodja ali skupine CSIRT**. Registri vrhnjih domen in subjekti, ki zanje opravljajo storitve registracije domenskih imen, bi morali vzpostaviti politike in postopke za objavo in razkritje podatkov o registraciji, vključno s sporazumi o ravni storitve, za obravnavanje zahtev oseb za dostop, ki imajo upravičen razlog za dostop. Postopek dostopa lahko vključuje tudi uporabo vmesnika, portala ali drugih tehničnih orodij za zagotovitev učinkovitega sistema za predložitev zahtev in dostopanje do podatkov o registraciji. **Države članice bi morale zagotoviti, da so vse vrste dostopa do podatkov o registraciji domenskih imen (osebnih in neosebnih podatkov) brezplačne**. Komisija lahko za spodbujanje harmoniziranih praks na notranjem trgu, brez poseganja v pristojnosti Evropskega odbora za varstvo podatkov, sprejme smernice o takih postopkih, ki bodo **skladni in komplementarni z mednarodnimi standardi, ki jih razvije večdeležniška skupnost**.

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

- (63) [...] **Bistveni in pomembni subjekti na podlagi te direktive bi morali spadati v sodno pristojnost države članice, kjer opravljajo svoje storitve. Subjekti iz Priloge I, točke 1 do 7 in 10, ponudniki storitev zaupanja in ponudniki stičišča omrežij iz Priloge I, točka 8, ter subjekti iz Priloge II, točke 1 do 5 te direktive, bi morali spadati v sodno pristojnost države članice, na ozemlju katere imajo sedež.** Če subjekt opravlja storitve ali ima sedež v več kot eni državi članici, bi moral spadati v ločeno in sočasno sodno pristojnost vsake od teh držav članic. Pristojni organi teh držav članic bi morali sodelovati, si medsebojno pomagati in, kjer je ustrezno, izvajati skupne nadzorne ukrepe. **Kadar se države članice odločijo za izvrševanje sodne pristojnosti, bi se morale izogibati temu, da bi bilo isto ravnanje zaradi kršitve obveznosti iz te direktive sankcionirano več kot enkrat.**
- (64) Da bi se upoštevala čezmejna narava storitev in postopkov ponudnikov storitev sistema domenskih imen, registrov vrhnjih domenskih imen, **subjektov, ki opravljajo storitve registracije domenskih imen za vrhnje domene**, ponudnikov omrežij za dostavo vsebine, ponudnikov storitev računalništva v oblaku, ponudnikov storitev podatkovnih centrov in ponudnikov digitalnih storitev, bi morala biti za te subjekte pristojna samo ena država članica. Sodno pristojnost bi bilo treba dodeliti državi članici, v kateri ima zadevni subjekt glavni sedež v Uniji. Merilo sedeža za namene te direktive pomeni dejansko izvajanje dejavnosti na podlagi stabilnih ureditev. Pravna oblika takih ureditev, bodisi prek izpostave bodisi prek podružnice, ki je pravna oseba, v tem pogledu ni odločujoči dejavnik.

Izpolnjevanje tega merila ne bi smelo biti odvisno od tega, ali so omrežja in informacijski sistemi fizično locirani na tistem mestu; prisotnost in uporaba teh sistemov sami po sebi ne pomenita tega glavnega sedeža in zato nista odločilni merili za ugotavljanje glavnega sedeža. Glavni sedež bi moral biti kraj, kjer se v Uniji **po večini** sprejemajo odločitve v zvezi z ukrepi za obvladovanje tveganj za kibernetno varnost. To običajno ustreza kraju osrednje uprave podjetij v Uniji. Če **kraja, kjer se takšne odločitve po večini sprejemajo, ni mogoče določiti ali** se take odločitve ne sprejemajo v Uniji, bi se moralo šteti, da je glavni sedež v državi članici, v kateri je sedež subjekta z največjim številom zaposlenih v Uniji. Kadar storitve opravljajo povezane družbe, bi bilo treba glavni sedež obvladujoče družbe šteti za glavni sedež povezanih družb.

- (64a) **Kadar rekurzivno storitev sistema domenskih imen (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 sodni pristojnosti vseh držav članic, v katerih se opravljajo njegove storitve.**
- (64aa) **Da se zagotovi jasen pregled ponudnikov storitev domenskih imen, registrov imen vrhnjih domen, subjektov, ki opravljajo storitve registracije domenskih imen za vrhnje domene, ponudnikov omrežij za zagotavljanje vsebin, ponudnikov storitev računalništva v oblaku, ponudnikov storitev podatkovnih centrov in digitalnih ponudnikov, ki opravljajo storitve po vsej Uniji v okviru področja uporabe te direktive, bi morala agencija ENISA vzpostaviti in vzdrževati register takih subjektov, in sicer na podlagi prigrasitev, ki jih prejmejo države članice, če je ustrezno, prek njihovih nacionalnih mehanizmov za samoprigrasitev. Za zagotovitev točnosti in popolnosti informacij, ki bi jih bilo treba vključiti v ta register, bi morale države članice agenciji ENISA predložiti informacije o teh subjektih, ki so na voljo v njihovih nacionalnih registrih. Agencija ENISA in države članice bi morale sprejeti ukrepe za lajšanje interoperabilnosti takšnih registrov, hkrati pa zagotoviti varstvo zaupnih ali tajnih informacij.**

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

- (66) Če se podatki, ki se v skladu z nacionalnim pravom ali pravom Unije štejejo za tajne, izmenjujejo, sporočajo ali drugače souporabljaajo v skladu z določbami te direktive, bi se morala uporabljati ustrezna posebna pravila o ravnanju s tajnimi podatki.
- (67) Ker so kibernetiske grožnje vse bolj zapletene in izpopolnjene, so dobri ukrepi za odkrivanje in preprečevanje večinoma odvisni od redne izmenjave obveščevalnih podatkov o grožnjah in šibkih točkah med subjekti. Izmenjava informacij prispeva k večji ozaveščenosti o kibernetiskih grožnjah, kar posledično krepi sposobnost subjektov za preprečevanje, da bi se grožnje spremenile v dejanske incidente, in subjektom omogoča, da boljše omejijo učinke incidentov in si učinkoviteje opomorejo. Videti je, da ob odsotnosti usmeritev na ravni Unije več dejavnikov ovira tako izmenjavo obveščevalnih podatkov, zlasti negotovost glede združljivosti s pravili o konkurenci in odgovornosti.
- (68) Subjekte bi bilo zato treba spodbuditi, naj skupaj izkoristijo svoje individualno znanje in praktične izkušnje na strateški, taktični in operativni ravni, da bi tako okrepili svoje zmogljivosti za ustrezno ocenjevanje in spremljanje kibernetiskih groženj, zaščito pred njimi in odzivanje nanje. Zato je treba omogočiti, da se na ravni Unije vzpostavijo mehanizmi za prostovoljne dogovore o izmenjavi informacij. V ta namen bi morale države članice dejavno podpirati in spodbujati tudi ustrezne subjekte, ki niso zajeti v področje uporabe te direktive, naj sodelujejo v takih mehanizmih za izmenjavo informacij. Taki mehanizmi bi se morali izvajati ob polnem spoštovanju pravil Unije o konkurenci in pravil prava Unije o varstvu podatkov.

- (69) [...] **Obdelava osebnih podatkov** v obsegu, nujno potrebnem in sorazmernem za zagotovitev varnosti omrežja in informacij, ki jo izvajajo **bistveni in pomembni** subjekti [...] ter ponudniki varnostnih tehnologij in storitev, **bi se lahko štela kot potrebna za izpolnjevanje pravne obveznosti ali bi lahko** [...] pomenila zakoniti interes zadevnega[...] upravljavca podatkov, kot je navedeno v Uredbi (EU) 2016/679. To bi **lahko** [...] vključevalo ukrepe, povezane s preprečevanjem, odkrivanjem in analizo incidentov ter odzivanjem nanje, ukrepe za ozaveščanje v zvezi s konkretnimi kibernetскими grožnjami, izmenjavo informacij v okviru odpravljanja in usklajenega razkrivanja šibkih točk ter prostovoljno izmenjavo informacij o takih incidentih, [...] kibernetских grožnjah in šibkih točkah, kazalnikih ogroženosti, taktikah, tehnikah in postopkih, opozorilih glede kibernetiske varnosti in orodjih za konfiguracijo. Taki ukrepi lahko zahtevajo obdelavo [...] **različnih** vrst osebnih podatkov, **kot so:** naslovi IP, enotni naslovi vira (URL), domenska imena in elektronski naslovi. **Obdelava osebnih podatkov, ki jo izvajajo pristojni organi, enotne kontaktne točke in skupine CSIRT, bi morala biti določena v nacionalnem pravu in bi se morala šteti kot potrebna za izpolnjevanje pravne obveznosti ali za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu podatkov, kot je navedeno v členu 6(1), točka (c) ali (e), Uredbe (EU) 2016/679.**
- (69a) S pravom držav članic se lahko določijo pravila, ki pristojnim organom, enotnim kontaktnim točkam in skupinam CSIRT – kolikor je to nujno potrebno in sorazmerno za namen zagotavljanja varnosti omrežja in informacijskih sistemov bistvenih in pomembnih subjektov – omogočajo obdelavo posebnih kategorij osebnih podatkov v skladu s členom 9[...] Uredbe (EU) 2016/679, zlasti z določitvijo ustreznih in posebnih ukrepov za zaščito temeljnih pravic in interesov fizičnih oseb, vključno s tehničnimi omejitvami glede ponovne uporabe takih podatkov in uporabe najsodobnejših varnostnih ukrepov in ukrepov za varovanje zasebnosti, kot je psevdonimizacija ali šifriranje, kadar bi anonimizacija lahko pomembno vplivala na želeni namen.

- (70) Za okrepitev nadzornih pooblastil in ukrepov, ki pomagajo zagotavljati dejansko izpolnjevanje zahtev, bi bilo treba v tej direktivi določiti minimalni seznam nadzornih ukrepov in sredstev, s katerimi **lahko** [...] pristojni organi nadzorujejo bistvene in pomembne subjekte. Poleg tega bi bilo treba s to direktivo vzpostaviti razlikovanje nadzorne ureditve med bistvenimi in pomembnimi subjekti, da bi se zagotovilo ustrezno ravnovesje med obveznostmi subjektov in pristojnih organov. Tako bi morala za bistvene subjekte veljati celovita ureditev nadzora (predhodni in naknadni nadzor), medtem ko bi morala za pomembne subjekte veljati manj stroga ureditev nadzora, to je le naknadni nadzor. To pomeni, da se od pomembnih subjektov [...] **ne bi smelo zahtevati**, da sistematično **dokumentirajo** izpolnjevanje zahtev glede obvladovanja tveganj za kibernetško varnost, pristojni organi pa bi morali uporabljati reaktivni naknadni pristop k nadzoru in tako ne bi imeli splošne obveznosti nadzorovanja teh subjektov. **Za pomembne subjekte se lahko naknadni nadzor sproži na podlagi dokazov ali kakršnih koli znakov ali informacij, s katerimi se seznanijo pristojni organi in za katere ti organi menijo, da kažejo na morebitno neizpolnjevanje obveznosti iz 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, javno dostopne informacije, ali pa lahko izhajajo iz drugih dejavnosti, ki jih izvajajo pristojni organi pri izpolnjevanju svojih nalog.**

- (70a) Pri izvajanju predhodnega nadzora bi morali imeti pristojni organi možnost, da se sorazmerno 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 ali ciljno usmerjene varnostne presoje ali varnostni pregledi, vrsta informacij, ki jih je treba zahtevati, in raven podrobnosti teh informacij. Takšne metodologije za nadzor lahko spremljajo tudi delovni programi ter se redno ocenjujejo in pregledujejo, tudi glede vidikov, kot so dodeljevanje sredstev in potrebe.**
- (70aa) V zvezi s subjekti javne uprave bi bilo treba nadzorna pooblastila izvajati v skladu z nacionalnimi okviri in pravnim redom. Države članice bi morale imeti možnost, da se odločijo za uvedbo ustreznih, sorazmernih in učinkovitih ukrepov za nadzor in izvrševanje v zvezi s temi subjekti.**
- (70aaa) Da bi bistveni in pomembni subjekti dokazali skladnost z nekaterimi ukrepi za obvladovanje tveganja za kibernetško varnost, bi države članice od njih lahko zahtevale uporabo kvalificiranih storitev zaupanja ali priglašeni shem elektronske identifikacije v skladu z Uredbo (EU) št. 910/2014.**

- (71) Da bi bilo izvrševanje učinkovito, bi bilo treba določiti minimalni seznam upravnih sankcij za kršitve obveznosti glede obvladovanja tveganj za kibernetko varnost in poročanja iz te direktive ter vzpostaviti jasen in skladen okvir za take sankcije po vsej Uniji. Ustrezno bi bilo treba upoštevati naravo, težo in trajanje kršitve, dejansko povzročeno škodo ali nastale izgube ali morebitno škodo ali izgube, ki bi lahko nastale, ali je kršitev namerna ali posledica malomarnosti, ukrepe, sprejete za preprečevanje ali omilitev nastale škode in/ali izgub, stopnjo odgovornosti ali vse zadevne predhodne kršitve, stopnjo sodelovanja s pristojnim organom in morebitne druge oteževalne ali olajševalne dejavnike. Za naložitev sankcij, vključno z upravnimi globami, bi morali veljati ustrezni postopkovni zaščitni ukrepi v skladu s splošnimi načeli prava Unije in Listine Evropske unije o temeljnih pravicah, vključno z učinkovitim sodnim varstvom in ustreznimi postopki.
- (71a) Določbe, povezane z odgovornostjo fizičnih oseb, ki imajo določene odgovornosti znotraj subjekta, za kršitev njihove dolžnosti zagotavljanja skladnosti z obveznostmi, določenimi v tej direktivi, od držav članic ne zahtevajo, da morajo zagotoviti kazenski pregon ali civilno odgovornost za škodo, ki jo taka kršitev povzroči tretjim stranem.**
- (72) Za zagotovitev učinkovitega izvrševanja obveznosti, določenih v tej direktivi, bi morali biti vsi pristojni organi pooblaščen, da naložijo ali zahtevajo naložitev upravnih glob.

- (73) Kadar se upravne globe naložijo podjetjem, bi se podjetje v te namene moralo razumeti kot podjetje v skladu s členoma 101 in 102 PDEU. Kadar se upravne globe naložijo osebam, ki niso podjetje, bi moral nadzorni organ pri določanju ustreznega zneska globe upoštevati splošno raven dohodka v državi članici in ekonomski položaj osebe. Države članice bi morale določiti, ali bi se morale upravne globe uporabljati tudi za javne organe in v kakšnem obsegu. Naložitev upravne globe ne vpliva na uporabo drugih pooblastil pristojnih organov ali drugih sankcij, določenih v nacionalnih pravilih, s katerimi je prenesena ta direktiva.
- (74) Države članice [...] **lahko** določijo pravila o kazenskih sankcijah za kršitve nacionalnih pravil, s katerimi je prenesena ta direktiva. Naložitev kazenskih sankcij zaradi kršitev takih nacionalnih pravil in z njimi povezanih upravnih kazni pa ne bi smela voditi h kršitvi načela *ne bis in idem*, kakor ga razlaga Sodišče.
- (75) Kadar ta direktiva ne zagotavlja harmonizacije upravnih kazni ali po potrebi v drugih primerih, denimo v primerih hudih kršitev obveznosti, določenih v tej direktivi, bi morale države članice uporabiti sistem, ki zagotavlja učinkovite, sorazmerne in odvračilne sankcije. Narava takšnih sankcij, kazenskih ali upravnih, bi morala biti določena s pravom držav članic.

- (76) Za nadaljnjo krepitev učinkovitosti in odvračilnosti sankcij, ki se uporabljajo za kršitve obveznosti, določenih v skladu s to direktivo, bi morali biti pristojni organi pooblaščen za uporabo sankcij, ki vključujejo začasni preklic certifikata ali dovoljenja za del storitev ali vse storitve, ki jih opravlja bistveni subjekt, in začasno prepoved opravljanja vodstvenih funkcij za fizično osebo. Glede na njihovo resnost in vpliv na dejavnosti subjektov ter končno na potrošnike bi se morale take sankcije uporabljati le sorazmerno z resnostjo kršitve in ob upoštevanju posebnih okoliščin posameznega primera, vključno s tem, ali je kršitev namerna ali posledica malomarnosti, ter ukrepi, sprejetimi za preprečevanje ali ublažitev škode in/ali izgub. Take sankcije bi se morale uporabljati le kot ultima ratio, kar pomeni šele potem, ko so bili uporabljeni vsi drugi ustrezni izvršilni ukrepi, določeni v tej direktivi, in le dokler subjekti, za katere se uporabijo, ne sprejmejo potrebnih ukrepov za odpravo pomanjkljivosti ali izpolnitev zahtev pristojnega organa, zaradi katerih so bile takšne sankcije naložene. Za uvedbo takšnih sankcij bi morali veljati ustrezni postopkovni zaščitni ukrepi v skladu s splošnimi načeli prava Unije in Listine Evropske unije o temeljnih pravicah, vključno z učinkovitim sodnim varstvom, ustreznimi postopki, domnevo nedolžnosti in pravico do obrambe.
- (76a) Za zagotovitev učinkovitega nadzora in izvrševanja, zlasti v primerih 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 omrežje in informacijski sistem na njihovem ozemlju.**

- (77) S to direktivo bi bilo treba določiti pravila sodelovanja med pristojnimi in nadzornimi organi v skladu z Uredbo (EU) 2016/679 za obravnavanje kršitev, povezanih z osebnimi podatki.
- (78) Ta direktiva bi morala biti namenjena zagotavljanju visoke ravni odgovornosti za ukrepe za obvladovanje tveganj za kibernetško varnost in obveznosti poročanja na ravni organizacij. Zato bi morali upravni organi subjektov, ki spadajo na področje uporabe te direktive, odobriti ukrepe za obvladovanje tveganj za kibernetško varnost in nadzorovati njihovo izvajanje.
- (79) Vzpostaviti bi bilo treba [...] **sistem vzajemnega učenja, da bi pripomogli h krepitvi medsebojnega zaupanja in pridobivanju spoznanj iz dobrih praks in izkušenj**, ki bo omogočal [...] **izmenjave** strokovnjakov, ki jih imenujejo države članice, [...] za izvajanje politik kibernetške varnosti [...]. **Pri izvajanju sistema vzajemnega učenja bi bilo treba posebno pozornost nameniti zagotavljanju, da sistem ne bi po nepotrebnem ali nesorazmerno obremenil zadevnih organov držav članic. Komisija bi morala preučiti vse možnosti, da bi morda lahko zagotovila kritje stroškov, ki bi lahko nastali zaradi organizacije misij vzajemnega učenja. Poleg tega bi moral sistem vzajemnega učenja upoštevati rezultate podobnih mehanizmov, kot je sistem medsebojnega strokovnega pregleda mreže skupin CSIRT, dodati vrednost in preprečiti podvajanje. Izvajanje sistema vzajemnega učenja ne bi smelo posegati v nacionalno pravo ali pravo Unije o varstvu zaupnih in tajnih podatkov. Pred začetkom krogov vzajemnega učenja lahko države članice izvedejo samooceno ustreznih vidikov. Agencija ENISA lahko na zahtevo skupine za sodelovanje po potrebi zagotovi usmeritve za samooceno in ustrezne predloge. Države članice bi se lahko odločile, da svoja poročila objavijo.**

- (80) [...]
- (81) Da bi se zagotovili enotni pogoji za izvajanje ustreznih določb te direktive v zvezi s postopkovnimi ureditvami, potrebnimi za delovanje skupine za sodelovanje, tehničnimi elementi, povezanimi z ukrepi za obvladovanje tveganj, ali vrsto informacij, obliko in postopkom priglasitev incidentov, **kategorijami subjektov, od katerih se bo zahtevala uporaba določenih certificiranih proizvodov, storitev in postopkov IKT**, bi bilo treba na Komisijo prenesti izvedbena pooblastila. Ta pooblastila bi bilo treba izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta²⁶.
- (82) Komisija bi morala redno v posvetovanju z zainteresiranimi stranmi pregledovati to direktivo, zlasti da bi ugotovila, ali jo je treba prilagoditi spremenjenim družbenim, političnim, tehnološkim ali tržnim razmeram.

²⁶ 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).

- (83) Ker cilja te direktive, in sicer doseganja visoke skupne ravni kibernetске varnosti v Uniji, države članice ne morejo zadovoljivo doseči, temveč se zaradi učinkov ukrepov lažje doseže na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 Pogodbe o Evropski uniji. V skladu z načelom sorazmernosti iz navedenega člena ta direktiva ne presega tistega, kar je potrebno za doseganje navedenega cilja.
- (84) Ta direktiva upošteva temeljne pravice in načela Listine Evropske unije o temeljnih pravicah, zlasti pravico do spoštovanja zasebnega življenja in komunikacij, varstvo osebnih podatkov, svobodo gospodarske pobude, lastninsko pravico, pravico do učinkovitega pravnega sredstva in nepristranskega sodišča in pravico do izjave. To direktivo bi bilo treba izvajati v skladu s temi pravicami in načeli –

SPREJELA NASLEDNJO DIREKTIVO:

POGLAVJE I

Splošne določbe

Člen 1

Predmet urejanja

1. Ta direktiva določa ukrepe za zagotovitev visoke skupne ravni kibernetске varnosti v Uniji,
da bi se izboljšalo delovanje notranjega trga.
2. V ta namen ta direktiva:
 - (a) določa obveznosti za države članice, da sprejmejo nacionalne strategije za kibernetско varnost, imenujejo pristojne nacionalne organe, enotne kontaktne točke in skupine za odzivanje na incidente na področju računalniške varnosti (CSIRT);
 - (b) določa obveznosti glede obvladovanja tveganj za kibernetско varnost in poročanja za vrste subjektov [...] iz prilog **I in II**[...];
 - (c) določa **pravila in** obveznosti glede izmenjave informacij o kibernetски varnosti.

Člen 2

Področje uporabe

1. Ta direktiva se uporablja za javne in zasebne **vrste** subjektov, [...] **navedene** v [...] prilogah **I in II**, [...] **ki dosegajo ali presegajo zgornje meje za srednja podjetja** [...] v smislu Priporočila Komisije 2003/361/ES²⁷. **Za namene te direktive se ne uporabljata člen 3(4) in člen 6(2), drugi in tretji pododstavki, iz Priloge k navedenemu priporočilu.**
2. [...]Ne glede na [...] velikost **subjektov iz odstavka 1** se ta direktiva uporablja tudi, **kadar:**
[...]
 - (a) storitve opravlja eden ali več naslednjih subjektov:
 - (i) **ponudniki** javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev iz Priloge I, točka 8;
 - (ii) **ponudniki kvalificiranih storitev zaupanja iz Priloge I, točka XX;**
 - (iii) **ponudniki nekvalificiranih storitev zaupanja iz Priloge I, točka XX;**
 - (iv) registri vrhnjih domenskih imen [...] iz Priloge I, točka 8;
 - (b) [...]

²⁷ 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).

- (c) je subjekt edini ponudnik storitve, [...] **ki je bistvena za ohranjanje kritičnih družbenih ali gospodarskih dejavnosti, v državi članici;**
- (d) bi morebitna motnja pri opravljanju storitve subjekta lahko [...] **pomembno** vplivala na javni red, javno varnost ali javno zdravje;
- (e) bi morebitna motnja pri opravljanju storitve subjekta lahko povzročila [...] **pomembna** sistemska tveganja, zlasti za sektorje, v katerih bi lahko taka motnja imela čezmejni vpliv;
- (f) [...];
- (g) je subjekt določen kot kritični subjekt v skladu z Direktivo (EU) XXXX/XXXX Evropskega parlamenta in Sveta²⁸ [direktiva o odpornosti kritičnih subjektov] ali [kot subjekt, enakovreden kritičnemu subjektu v skladu s členom 7 navedene direktive].

2a. Ta direktiva se ne glede na njihovo velikost uporablja tudi za subjekte javne uprave centralnih vlad, ki so kot taki priznani v državi članici v skladu z nacionalnim pravom in navedeni v Prilogi I, točka 9. Države članice lahko določijo, da se ta direktiva uporablja tudi za subjekte javne uprave na regionalni in lokalni ravni.

²⁸ [vstaviti polni naslov in sklic na objavo v UL, ko bosta znana].

3. [...]

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

3a. (1) Ta direktiva se ne uporablja za:

- (a) subjekte, ki ne spadajo v področje uporabe prava Unije, in v vsakem primeru vse subjekte, ki predvsem izvajajo dejavnosti na področju obrambe, nacionalne varnosti ali javne varnosti ali kazenskega pregona, ne glede na to, kateri subjekt izvaja te dejavnosti in ali gre za javni subjekt ali zasebni subjekt, brez poseganja v točko (2);**

(b) subjekte, ki izvajajo dejavnosti v sodstvu, parlamentih ali centralnih bankah.[...]

(2) Kadar subjekti javne uprave izvajajo dejavnosti na teh področjih samo kot del svojih celotnih dejavnosti, so v celoti izključeni iz področja uporabe te direktive.

3aa. Ta direktiva se ne uporablja za:

- (i) dejavnosti subjektov, ki ne spadajo v področje uporabe prava Unije, in v vsakem primeru vse dejavnosti, ki zadevajo nacionalno varnost ali obrambo, ne glede na to, kateri subjekt izvaja te dejavnosti in ali gre za javni subjekt ali zasebni subjekt;
- (ii) dejavnosti subjektov v sodstvu, parlamentih, centralnih bankah in na področju javne varnosti, vključno s subjekti javne uprave, ki izvajajo dejavnosti kazenskega pregona za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij.

3aaa. 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.

3aaaa. Ta direktiva ne posega v pravo Unije o varstvu osebnih podatkov, zlasti Uredbo (EU) 2016/679 in Direktivo 2002/58/ES.

3b. Ta direktiva se ne uporablja za subjekte, ki so izvzeti iz Uredbe (EU) XXXX/XXXX Evropskega parlamenta in Sveta [uredba o digitalni operativni odpornosti v finančnem sektorju] v skladu s členom 2, odstavek 4, uredbe o digitalni operativni odpornosti v finančnem sektorju.

4. Ta direktiva se uporablja brez poseganja v [...] ²⁹ direktivi 2011/93/EU ³⁰ in 2013/40/EU ³¹ Evropskega parlamenta in Sveta.

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

²⁹ [...]

³⁰ 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).

³¹ 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).

Člen 2a

Bistveni in pomembni subjekti

1. Med subjekti, za katere se uporablja ta direktiva, se kot bistveni štejejo:
 - (i) subjekti vrste, ki je opredeljena v Prilogi I, točke 1 do 8a in 10, k tej direktivi, ki presegajo zgornje meje za srednja podjetja, kot so opredeljena v Priporočilu Komisije 2003/361/ES;
 - (ii) srednje veliki subjekti iz člena 2(2), točka(a)(i);
 - (iii) subjekti iz člena 2(2), točka (a)(ii) in (iv), te direktive, ne glede na velikost;
 - (iv) subjekti iz člena 2(2), točka (g), in člena 2(2a) te direktive, ne glede na velikost;
 - (v) če so jih ustanovile države članice, subjekti, ki so jih države članice pred začetkom veljavnosti te direktive določile za izvajalce bistvenih storitev v skladu z Direktivo (EU) 2016/1148 ali nacionalnim pravom;
 - (vi) subjekti vrste, ki je določena v Prilogi II, ki presegajo zgornje meje za srednja podjetja, kot so opredeljena v Priporočilu Komisije 2003/361/ES, ki jih države članice opredelijo kot bistvene na podlagi meril iz člena 2(2), točke (c) do (e);

- (vii) srednje veliki subjekti v smislu Priporočila Komisije 2003/361/ES, ki jih države članice opredelijo kot bistvene na podlagi meril iz člena 2(2), točke (c) do (e);
- (viii) mikro ali mala podjetja v smislu Priporočila Komisije 2003/361/ES, kot so določena v odstavku 2, točka (a)(i), ali določena v skladu z odstavkom 2, točke (c) do (e), tega člena, ki jih države članice opredelijo kot bistvene na podlagi nacionalnih ocen tveganja.

2. Med subjekti, za katere se uporablja ta direktiva, se kot pomembni štejejo:

- (i) subjekti vrste, ki je določena v Prilogi I k tej direktivi, ki izpolnjujejo pogoje za srednja podjetja v smislu Priporočila Komisije 2003/361/ES, in subjekti vrste, ki je določena v Prilogi II, ki dosegajo ali presegajo zgornje meje za srednja podjetja v smislu Priporočila Komisije 2003/361/ES³²;
- (ii) subjekti iz člena 2(2), točka (iii), te direktive, ne glede na velikost;
- (iii) mali in mikro subjekti iz člena 2(2), točka(a)(i);
- (iv) mali in mikro subjekti, ki jih države članice opredelijo kot pomembne subjekte na podlagi člena 2, odstavek 2, točke (c) do (e).

³² 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).

Člen 2a

Mehanizmi za prigrasitev

1. **Države članice lahko vzpostavijo nacionalni mehanizem za samoprigrasitev, v skladu s katerim morajo vsi subjekti, za katere se uporablja ta direktiva, pristojnim organom na podlagi te direktive ali organom, ki jih v ta namen določijo države članice, predložiti vsaj svoje ime, naslov, kontaktne podatke, sektor, v katerem delujejo, ali vrsto storitve, ki jo opravljajo, ter po potrebi seznam držav članic, kjer opravljajo storitve, za katere se uporablja ta direktiva.**
2. **Države članice [...] v zvezi s subjekti, ki jih določijo na podlagi člena 2(2), točke (b) do (e), [12 mesecev po roku za prenos te direktive] Komisiji predložijo vsaj relevantne informacije o številu opredeljenih subjektov, sektorju, v katerem delujejo, ali vrsti storitev, ki jo opravljajo glede na priloge, ter posebno določbo ali določbe člena 2(2), na podlagi katerih so bili določeni. Države članice redno oziroma vsaj vsaki dve leti pregledajo [...] te informacije [...] ter jih po potrebi posodobijo.**

Člen 2b

Sektorski akti Unije

1. Kadar se s [...] sektorskimi **pravnimi akti Unije** zahteva, da bistveni ali pomembni subjekti bodisi sprejmejo ukrepe za obvladovanje tveganj za kibernetško varnost bodisi priglasijo **pomembne** incidente ali [...] kibernetške grožnje, 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 VI, za take subjekte ne uporabljajo**. Če sektorski pravni akti Unije ne zajemajo vseh subjektov v določenem sektorju, ki spadajo v področje uporabe te direktive, se ustrezne določbe te direktive še naprej uporabljajo za subjekte, ki niso zajeti v teh sektorskih določbah.
2. Za zahteve iz odstavka 1 tega člena se šteje, da so po učinku enakovredne obveznostim iz te direktive, če zadevni sektorski akt Unije zagotavlja takojšen dostop, kadar je ustrezno, samodejen in neposreden, do priglasitev incidentov s strani pristojnih organov v skladu s to direktivo ali imenovanih skupin CSIRT in če:
 - (a) imajo ukrepi za obvladovanje tveganj za kibernetško varnost vsaj enakovreden učinek kot ukrepi iz člena 18(1) in (2) te direktive; ali
 - (b) imajo zahteve za priglasitev pomembnih incidentov vsaj enakovreden učinek kot zahteve iz člena 20(1) do (6).

3. Komisija redno pregleduje, kako se uveljavljajo zahteve glede enakovrednega učinka iz odstavkov 1 in 2 tega člena v zvezi s sektorskimi določbami pravnih aktov Unije. Komisija se pri pripravi tovrstnih rednih pregledov posvetuje s skupino za sodelovanje in agencijo ENISA.

Člen 3

Minimalna harmonizacija

Države članice lahko brez poseganja v svoje druge obveznosti na podlagi prava Unije [...] sprejmejo ali ohranijo določbe, ki zagotavljajo višjo raven kibernetске varnosti, **na področjih, ki jih zajema ta direktiva.**

Člen 4

Opredelitev pojmov

V tej direktivi se uporabljajo naslednje opredelitve pojmov:

- (1) „omrežje in informacijski sistem“ pomeni:
- (a) elektronsko komunikacijsko omrežje v smislu člena 2(1) Direktive (EU) 2018/1972;
 - (b) vsako napravo ali skupino med seboj povezanih ali sorodnih naprav, od katerih ena ali več na podlagi programa opravlja samodejno obdelavo digitalnih podatkov;
 - (c) digitalne podatke, ki jih elementi iz točk (a) in (b) shranjujejo, obdelujejo, pridobivajo ali prenašajo za namene njihovega delovanja, uporabe, varovanja in vzdrževanja;

- (2) „varnost omrežij in informacijskih sistemov“ pomeni zmožnost omrežij in informacijskih sistemov, da na določeni ravni zaupanja preprečijo vsak **dogodek**, ki **lahko** [...] ogrozi razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki jih navedena omrežja in informacijski sistemi zagotavljajo ali so prek njih dostopni;
- (2a) „elektronske komunikacijske storitve“ pomenijo [...] elektronske komunikacijske storitve v smislu člena 2(4) Direktive (EU) 2018/172;**
- (3) „kibernetska varnost“ pomeni kibernetiko varnost v smislu člena 2(1) Uredbe (EU) št. 2019/881 Evropskega parlamenta in Sveta³³;
- (4) „nacionalna strategija za **kibernetiko varnost**“ [...] pomeni skladen okvir države članice, ki določa strateške cilje in prednostne naloge **na področju kibernetike varnosti** [...] v zadevni državi članici;
- (5) „incident“ pomeni vsak dogodek, ki ogroža razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali [...] storitev, ki jih navedena omrežja in informacijski sistemi zagotavljajo ali so prek njih dostopni;
- (5a) „velik kibernetiki incident“ pomeni incident, ki pomembno vpliva na vsaj dve državi članici ali katerega motnja presega zmožnost države članice, da se nanje odzove;**

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

- (6) „obvladovanje incidentov“ pomeni vsa dejanja in postopke, namenjene odkrivanju, analizi in zaježitvi incidentov ter odzivanju nanje;
- (6a) „tveganje“ pomeni možnost izgube ali motnje zaradi incidenta ter je izraženo kot kombinacija razsežnosti take izgube ali motnje in verjetnosti, da bi do zadevnega incidenta prišlo;**
- (7) „kibernetska grožnja“ pomeni kibernetško grožnjo v smislu člena 2(8) Uredbe 2019/881;
- (7a) „pomembna kibernetška grožnja“ pomeni kibernetško grožnjo, za katero se glede na njene tehnične značilnosti lahko domneva, da bi lahko resno vplivala na omrežje in informacijske sisteme subjekta ali njegovih uporabnikov, tako da bi povzročila znatne materialne ali nematerialne izgube;**
- (8) „šibka točka“ pomeni pomanjkljivost, dovzetnost ali napako IKT sredstva ali sistema [...], ki jo kibernetška grožnja lahko izkoristi;
- (8a) „skorajšnji dogodek“ pomeni dogodek, ki bi lahko povzročil škodo omrežju in informacijskim sistemom subjekta ali njegovih uporabnikov, vendar je bilo uspešno preprečeno, da bi se v celoti uresničil;**
- (9) „predstavnik“ pomeni vsako fizično ali pravno osebo s sedežem v Uniji, ki je izrecno imenovana, da deluje v imenu (i) ponudnika storitev sistema domenskih imen (DNS), registra vrhnjih domenskih imen (TLD), ponudnika storitev računalništva v oblaku, ponudnika storitev podatkovnega centra, ponudnika omrežja za dostavo vsebine iz točke 8 Priloge I ali (ii) subjektov iz točke [...] 6 Priloge II, ki nimajo sedeža v Uniji, s katerim lahko nacionalni pristojni organ ali skupina CSIRT vzpostavi stik namesto z zadevnim subjektom, kar zadeva obveznosti tega subjekta na podlagi te direktive;

- (10) „standard“ pomeni standard v smislu člena 2(1) Uredbe (EU) št. 1025/2012 Evropskega parlamenta in Sveta³⁴;
- (11) „tehnična specifikacija“ pomeni tehnično specifikacijo v smislu člena 2(4) Uredbe (EU) št. 1025/2012;
- (12) „stičišče omrežij“ pomeni omrežno zmogljivost, ki omogoča medsebojno povezavo več kot dveh neodvisnih omrežij (avtonomnih sistemov), predvsem zaradi izmenjave internetnega prometa; stičišče omrežij zagotavlja medsebojno povezavo le avtonomnih sistemov; stičišče omrežij omogoča izmenjavo internetnega prometa med katerima koli sodelujočima avtonomnima sistemoma, brez prehoda prek tretjega avtonomnega sistema, prav tako pa ne spreminja takšnega prometa ali kako drugače posega vanj;
- (13) „sistem domenskih imen (DNS)“ pomeni hierarhičen porazdeljen sistem dodeljevanja imen, ki končnim uporabnikom omogoča dostop do storitev in virov na internetu;
- (14) „ponudnik storitev sistema domenskih imen (DNS)“ pomeni subjekt, ki opravlja storitve rekurzivnega ali avtoritativnega razreševanja domenskih imen **za [...] uporabo s strani tretjih oseb, z izjemo korenskih imenskih strežnikov**;

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

- (15) „register vrhnjih domenskih imen“ pomeni subjekt, ki mu je bila dodeljena določena vrhnja domena in ki je odgovoren za upravljanje vrhnje domene, vključno z registracijo domenskih imen pod vrhno domeno in tehničnim upravljanjem vrhnje domene, vključno z upravljanjem njenih imenskih strežnikov, vzdrževanjem njenih podatkovnih zbirk in porazdelitvijo območnih datotek vrhnje domene po imenskih strežnikih, **z izjemo primerov, ko register vrhnja domenska imena uporablja le za lastno uporabo;**
- (15a) „subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene“ pomenijo registre imen vrhnjih domen, registratorje za vrhnje domene in agente registratorjev, kot so preprodajalci in ponudniki posredniških storitev;
- (16) „digitalna storitev“ pomeni storitev v smislu člena 1(1)(b) Direktive (EU) 2015/1535 Evropskega parlamenta in Sveta³⁵;
- (16a) „storitev zaupanja“ pomeni storitev zaupanja v smislu člena 3(16) Uredbe (EU) št. 910/2014;

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

- (16b) „ponudnik kvalificiranih storitev zaupanja“ pomeni ponudnika kvalificiranih storitev zaupanja v smislu člena 3(20) Uredbe (EU) št. 910/2014;
- (17) „spletna tržnica“ pomeni digitalno storitev v smislu člena 2(n) Direktive 2005/29/ES Evropskega parlamenta in Sveta³⁶;
- (18) „spletni iskalnik“ pomeni digitalno storitev v smislu člena 2(5) Uredbe (EU) 2019/1150 Evropskega parlamenta in Sveta³⁷;
- (19) „storitev računalništva v oblaku“ pomeni digitalno storitev, ki omogoča upravljanje na zahtevo in širok oddaljeni dostop do prožnega in po obsegu prilagodljivega nabora deljivih [...] računalniških virov, **tudi kadar so ti porazdeljeni na več lokacijah**;
- (20) „storitev podatkovnega centra“ pomeni storitev, ki vključuje strukture ali skupine struktur, namenjene centralizirani namestitvi, medsebojnemu povezovanju in delovanju opreme za informacijsko tehnologijo in omrežne opreme za storitve shranjevanja, obdelave in prenosa podatkov skupaj z vsemi zmogljivostmi in infrastrukturami za distribucijo električne energije in okoljski nadzor;

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

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

- (21) „omrežje za dostavo vsebin“ pomeni mrežo geografsko porazdeljenih strežnikov za zagotavljanje visoke razpoložljivosti, dostopnosti ali hitre dostave digitalnih vsebin in storitev uporabnikom interneta v imenu ponudnikov vsebin in storitev;
- (22) „platforma za storitve družbenega mreženja“ pomeni platformo, ki končnim uporabnikom omogoča, da se povezujejo, si izmenjujejo vsebine, se spoznavajo in komunicirajo med seboj prek več naprav ter zlasti prek klepetov, objav, videoposnetkov in priporočil[...];
- (23) „subjekt javne uprave“ pomeni subjekt, **ki je v skladu z nacionalnim pravom kot tak priznan v državi članici** [...] 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) ga večinoma financirajo država, regionalni organ ali druge osebe javnega prava; ali je pod upravljavskim nadzorom takih organov ali oseb; ali ima upravni, vodstveni ali nadzorni odbor, katerega več kot polovico članov imenujejo država, regionalni organi ali druge osebe javnega prava;
 - (d) ima pooblastilo, da na fizične ali pravne osebe naslovi upravne ali regulativne odločbe, ki vplivajo na njihove pravice na področju čezmejnega gibanja oseb in pretoka blaga, storitev ali kapitala.
- (24) „subjekt“ pomeni vsako fizično ali pravno osebo, ki je ustanovljena in priznana kot taka po nacionalnem pravu njenega kraja sedeža ter lahko v svojem imenu uveljavlja pravice in prevzema obveznosti;

- (25) „bistveni subjekt“ pomeni subjekt vrste [...] iz Priloge I, ki je določen kot „bistven“ v skladu s členom 2a(1);
- (26) „pomembni subjekt“ pomeni subjekt vrste [...] iz prilog I in II, ki je določen kot „pomemben“ v skladu s členom 2a(2);
- (26a) „proizvod IKT“ pomeni proizvod IKT v smislu člena 2(12) Uredbe (EU) št. 2019/881;
- (26aa) „storitev IKT“ pomeni storitev IKT v smislu člena 2(13) Uredbe (EU) št. 2019/881;
- (26ab) „postopek IKT“ pomeni postopek IKT v smislu člena 2(14) Uredbe 2019/881;
- (26ac) „ponudnik upravljanih storitev“ pomeni vsak subjekt, ki opravlja storitve, kot so omrežje, aplikacija, infrastruktura in varnost, prek stalnega in rednega upravljanja, podpore in aktivnega upravljanja v prostorih strank, v lastnem podatkovnem centru (gostovanje) ali v podatkovnem centru tretje osebe;
- (26ad) „ponudnik upravljanih varnostnih storitev“ pomeni kateri koli subjekt, ki zagotavlja zunanje spremljanje in upravljanje varnostnih naprav in sistemov. Skupne storitve vključujejo upravljan požarni zid, odkrivanje vdorov, virtualno zasebno omrežje, pregled šibkih točk in protivirusne storitve.

Vključuje tudi uporabo visoko dostopnih centrov za varnostne operacije (bodisi iz lastnih objektov ali objektov drugih ponudnikov podatkovnih centrov) za zagotavljanje storitev 24 ur na dan in 7 dni v tednu, da bi se zmanjšalo število operativnega varnostnega osebja, ki ga mora podjetje najeti, usposablјati in obdržati, da bi ohranilo sprejemljivo varnostno držo.

POGLAVJE II

Usklajeni regulativni okviri za kibernetiko varnost

Člen 5

Nacionalna strategija za kibernetiko varnost

1. Vsaka država članica sprejme nacionalno strategijo za kibernetiko varnost, v kateri so opredeljeni strateški cilji ter ustrezni ukrepi politike in regulativni ukrepi za doseganje in ohranjanje visoke ravni kibernetiske varnosti. Nacionalna strategija za kibernetiko varnost vključuje zlasti naslednje:
 - (a) [...] cilje in prednostne naloge strategije držav članic za kibernetiko varnost;
 - (b) okvir upravljanja za doseganje navedenih ciljev in prednostnih nalog, vključno s politikami iz odstavka 2 ter vlogami in odgovornostmi [...] različnih organov in akterjev, vključenih v izvajanje strategije;
 - (c) [...] **usmeritve** za opredelitev ustreznih sredstev in **oceno** tveganj za kibernetiko varnost v zadevni državi članici;
 - (d) opredelitev ukrepov za zagotovitev pripravljenosti na incidente, odzivanja nanje in okrevanja po njih, vključno s sodelovanjem med javnim in zasebnim sektorjem;
 - (e) [...]

(f) okvir politike za okrepljeno usklajevanje med organi, pristojnimi na podlagi te direktive in direktive (EU) XXXX/XXXX Evropskega parlamenta in Sveta³⁸ [direktiva o odpornosti kritičnih subjektov] za izmenjavo informacij o **tveganjih za kibernetško varnost**, [...] kibernetških grožnjah **in incidentih ter nekibernetških tveganjih, grožnjah in incidentih** ter izvajanje nadzornih nalog, **kot je ustrezno**;

(fa) **okvir politike za usklajevanje in sodelovanje med organi, pristojnimi na podlagi te direktive, in pristojnimi organi, imenovanimi na podlagi sektorske zakonodaje.**

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

- (a) politiko za obravnavanje kibernetške varnosti v dobavni verigi proizvodov in storitev IKT, ki jih [...] subjekti uporabljajo za opravljanje svojih storitev;
- (b) **politiko** [...] v zvezi z vključitvijo in specifikacijo zahtev za proizvode in storitve IKT pri javnem naročanju, povezanih s kibernetško varnostjo, **vključno s certificiranjem za kibernetško varnost**;
- (c) politiko **o obvladovanju šibkih točk, ki vključuje spodbujanje in olajševanje prostovoljnega** usklajenega razkrivanja šibkih točk v smislu člena 6(1);
- (d) politiko, povezano z ohranjanjem splošne razpoložljivosti, [...] celovitosti **in zaupnosti** javnega jedra odprtega interneta;
- (e) politiko za spodbujanje in razvoj **izobraževanja in usposabljanja**, znanj in spretnosti, ozaveščanja ter raziskovalnih in razvojnih pobud na področju kibernetške varnosti;

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

- (f) politiko za podpiranje akademskih in raziskovalnih institucij pri razvoju orodij in varne omrežne infrastrukture za kibernetiko varnost;
 - (g) politiko, ustrezne postopke in ustrezna orodja za izmenjavo informacij za podpiranje prostovoljne izmenjave informacij o kibernetiki varnosti med podjetji v skladu s pravom Unije;
 - (h) politiko za obravnavanje posebnih potreb MSP, zlasti tistih, ki so izključena s področja uporabe te direktive, v zvezi z usmeritvami in podporo pri povečevanju njihove odpornosti proti kibernetičnim grožnjam.
3. Države članice Komisiji priglasijo svoje nacionalne strategije za kibernetiko varnost v treh mesecih od njihovega sprejetja. **Pri tem lahko** države članice [...] izključijo [...] **elemente strategije, ki se nanašajo na nacionalno** varnost.
4. Države članice **redno in** vsaj vsakih [...] **pet** let ocenijo svoje nacionalne strategije za kibernetiko varnost na podlagi ključnih kazalnikov uspešnosti in jih po potrebi spremenijo. Agencija Evropske unije za kibernetiko varnost (ENISA) na **njihovo** zahtevo pomaga državam članicam pri razvoju nacionalne strategije in ključnih kazalnikov uspešnosti za oceno strategije.

Člen 6

Usklajeno razkrivanje šibkih točk in evropski register šibkih točk

1. Vsaka država članica imenuje eno od svojih skupin CSIRT iz člena 9 za koordinatorko za usklajeno razkrivanje šibkih točk. Imenovana skupina CSIRT deluje kot zaupanja vredna posrednica, ki po potrebi olajšuje sodelovanje med poročajočim subjektom, **lastnikom potencialnih šibkih točk** in proizvajalcem ali ponudnikom proizvodov ali storitev IKT. **Vsaka fizična ali pravna oseba lahko imenovani skupini CSIRT poroča o šibkih točkah iz člena 4(8), po možnosti anonimno. Imenovana skupina CSIRT zagotovi natančno spremljanje tega poročanja in zaupnost identitete osebe, ki poroča o šibkih točkah. Če bi sporočena šibka točka [...] lahko potencialno pomembno vplivala na subjekte v več kot eni državi članici, imenovana skupina CSIRT vsake zadevne države članice po potrebi sodeluje z drugimi imenovanimi skupinami CSRT v okviru mreže skupin CSIRT.**
2. Agencija ENISA razvije in vzdržuje evropski register šibkih točk **ter se pri tem posvetuje s skupino za sodelovanje.** V ta namen agencija ENISA vzpostavi in vzdržuje ustrezne informacijske sisteme, politike in postopke, zlasti z namenom omogočanja pomembnim in bistvenim subjektom ter njihovim dobaviteljem omrežnih in informacijskih sistemov, da **prostovoljno** razkrijejo in evidentirajo **javno znane** šibke točke proizvodov in storitev IKT ter zagotovijo dostop do informacij o šibkih točkah, vsebovanih v registru, vsem zainteresiranim stranem. Register vključuje zlasti informacije, ki opisujejo šibko točko, prizadeti proizvod ali storitev IKT ter resnost šibke točke v smislu okoliščin, v katerih jo je mogoče izkoristiti, razpoložljivost povezanih popravkov ter, če popravki niso na voljo, usmeritve, **ki jih izdajo nacionalni pristojni organi ali skupine CSIRT in so naslovljene na uporabnike proizvodov in storitev s šibkimi točkami, o načinih za zmanjšanje tveganj, ki izhajajo iz razkritih šibkih točk. Agencija ENISA zagotovi, da evropski register šibkih točk uporablja varno in odporno komunikacijsko in informacijsko infrastrukturo.**

Člen 7

Nacionalni okviri za krizno upravljanje kibernetске varnosti

1. Vsaka država članica imenuje enega ali več pristojnih organov, odgovornih za upravljanje velikih **kibernetских** incidentov in kriz. Države članice zagotovijo, da imajo pristojni organi ustrezne vire za učinkovito in uspešno opravljanje nalog, ki so jim bile dodeljene. **Države članice zagotovijo skladnost z obstoječimi okviri za splošno krizno upravljanje.**
2. Vsaka država članica določi zmogljivosti, sredstva in postopke, ki se lahko uporabijo v primeru krize za namene te direktive.
3. Vsaka država članica sprejme nacionalni načrt odzivanja na kibernetске incidente in krize, v katerem so opredeljeni cilji in načini upravljanja velikih kibernetских incidentov in kriz. V načrtu se določijo zlasti:
 - (a) cilji nacionalnih ukrepov in dejavnosti za pripravljenost;
 - (b) naloge in odgovornosti nacionalnih pristojnih organov;
 - (c) postopki za krizno upravljanje kibernetске varnosti, **vključno z njihovo vključitvijo v splošni nacionalni okvir za krizno upravljanje**, in kanali za izmenjavo informacij;
 - (d) ukrepi za pripravljenost, vključno z **rednimi** vajami in dejavnostmi usposabljanja;
 - (e) ustrezne vključene javne in zasebne [...] strani ter infrastruktura;
 - (f) nacionalni postopki in ureditve med ustreznimi nacionalnimi organi za zagotovitev učinkovitega sodelovanja države članice pri usklajenem upravljanju velikih kibernetских incidentov in kriz na ravni Unije ter njegove podpore.

4. Države članice Komisijo obvestijo o imenovanju svojih pristojnih organov iz odstavka 1 ter predložijo **ustrezne informacije v zvezi z zahtevami iz odstavka 3 tega člena o** svojih nacionalnih načrtih odzivanja na kibernetске incidente in krize [...] v treh mesecih od zadevnega imenovanja in sprejetja navedenih načrtov. Države članice lahko [...] izključijo določene informacije, če in kolikor je to [...] potrebno za njihovo nacionalno varnost, **javno varnost ali obrambo**.

Člen 8

Nacionalni pristojni organi in enotne kontaktne točke

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

5. Države članice zagotovijo, da imajo pristojni organi iz odstavka 1 in enotne kontaktne točke ustrezne vire, da učinkovito in uspešno opravljajo dodeljene naloge ter tako izpolnjujejo cilje te direktive. Države članice zagotovijo učinkovito, uspešno in varno sodelovanje imenovanih predstavnikov v skupini za sodelovanje iz člena 12.
6. Vsaka država članica Komisijo brez nepotrebnega odlašanja uradno obvesti o imenovanju pristojnega organa iz odstavka 1 in enotne kontaktne točke iz odstavka 3, njunih nalogah in vseh poznejših spremembah, povezanih z določitvijo in nalogami. Vsaka država članica njihovo imenovanje objavi. Komisija objavi seznam imenovanih enotnih kontaktnih točk.

Člen 9

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

1. Vsaka država članica imenuje eno ali več skupin CSIRT, ki izpolnjujejo zahteve iz člena 10(1) ter so pristojne za obvladovanje incidentov v skladu z natančno določenim postopkom, pri čemer zajame vsaj sektorje, podsektorje ali subjekte iz prilog I in II. Skupina CSIRT se lahko ustanovi v okviru pristojnega organa iz člena 8.
2. Države članice zagotovijo, da ima vsaka skupina CSIRT ustrezne vire za učinkovito izvajanje svojih nalog iz člena 10(2). **Skupine CSIRT lahko pri izvajanju teh nalog dajo prednost zagotavljanju določenih storitev subjektom na podlagi pristopa, ki temelji na tveganju.**
3. Države članice zagotovijo, da ima vsaka skupina CSIRT na voljo ustrezno, varno in odporno komunikacijsko in informacijsko infrastrukturo za izmenjavo informacij z bistvenimi in pomembnimi subjekti ter drugimi ustreznimi zainteresiranimi stranmi. V ta namen države članice zagotovijo, da skupine CSIRT prispevajo k uvajanju orodij za varno izmenjavo informacij.

4. Skupine CSIRT sodelujejo in si, kjer je ustrezno, v skladu s členom 26 izmenjujejo ustrezne informacije z zaupanja vrednimi sektorskimi ali medsektorskimi skupnostmi bistvenih in pomembnih subjektov.
5. Skupine CSIRT sodelujejo pri **vzajemnem učenju** [...], organiziranem v skladu s členom 16.
6. Države članice zagotovijo učinkovito, uspešno in varno sodelovanje svojih skupin CSIRT v mreži skupin CSIRT iz člena 13.
7. Države članice brez nepotrebnega odlašanja obvestijo Komisijo o skupinah CSIRT, imenovanih v skladu z odstavkom 1, skupini CSIRT koordinatorki, imenovani v skladu s členom 6(1), in njihovih ustreznih nalogah, določenih v zvezi s subjekti iz prilog I in II.
8. Države članice lahko pri oblikovanju nacionalnih skupin CSIRT zaprosijo za pomoč agencijo ENISA.

Člen 10

Zahteve in naloge skupin CSIRT

1. Skupine CSIRT izpolnjujejo naslednje zahteve:
 - (a) skupine CSIRT zagotavljajo visoko stopnjo razpoložljivosti svojih komunikacijskih [...] **kanalov**, tako da preprečujejo posamezne točke odpovedi in vzpostavijo več kanalov, po katerih se drugi lahko kadar koli obrnejo nanje in one obrnejo na druge. Skupine CSIRT jasno opredelijo komunikacijske kanale ter o njih obvestijo uporabnike in partnerje;
 - (b) uradi skupin CSIRT in podporni informacijski sistemi se nahajajo na varnih krajih;

- (c) skupine CSIRT imajo ustrezen sistem za upravljanje in usmerjanje zahtevkov, zlasti da se poenostavi njihova učinkovita in uspešna predaja;
- (d) skupine CSIRT imajo ustrezno osebje, s katerim lahko zagotovijo stalno razpoložljivost;
- (e) skupine CSIRT imajo redundantne sisteme in nadomestni delovni prostor, da se zagotovi neprekinjeno izvajanje njihovih storitev;
- (f) skupine CSIRT imajo možnost, da sodelujejo v mednarodnih mrežah za sodelovanje.

2. Skupine CSIRT imajo naslednje naloge:

- (a) spremljanje kibernetских groženj, šibkih točk in incidentov na nacionalni ravni;
- (b) zagotavljanje zgodnjega opozarjanja, opozoril, obvestil in razširjanja informacij o kibernetских grožnjah, šibkih točkah in incidentih bistvenim in pomembnim subjektom ter **pristojnim organom in** drugim ustreznim zainteresiranim stranem;
- (c) odzivanje na incidente;
- (d) **zbiranje in analiziranje forenzičnih podatkov in** opravljanje dinamičnih analiz tveganja in incidentov ter situacijsko zavedanje na področju kibernetiske varnosti;
- (e) opravljanje[...] proaktivnega pregleda omrežij in informacijskih sistemov[...], **da se odkrijejo šibke točke s potencialnim pomembnim vplivom, pod pogojem, da ne pride do vdora v omrežja ali informacijske sisteme ali do negativnega vpliva na njihovo delovanje, v primeru, da ni privolitve subjekta;**

- (f) sodelovanje v mreži skupin CSIRT in zagotavljanje medsebojne pomoči **skladno z zmožnostmi in pristojnostmi** drugim članicam mreže na njihovo zahtevo;
 - (fa) **po potrebi so v vlogi koordinatorja za namene postopka usklajenega razkrivanja šibkih točk v skladu s členom 6(1), ki vključuje zlasti olajševanje interakcije med poročajočimi subjekti, lastnikom potencialnih šibkih točk in proizvajalcem ali ponudnikom proizvodov IKT ali storitev IKT, kadar je to potrebno, identifikacijo zadevnih subjektov in stik z njimi, podporo poročajočim subjektom, pogajanja o rokih za razkrivanje in obvladovanje šibkih točk, ki vplivajo na več organizacij (večstransko usklajeno razkrivanje šibkih točk).**
- 3. Skupine CSIRT sodelujejo z ustreznimi akterji v zasebnem sektorju, da bi bolje dosegle cilje Direktive.
 - 3a. **Skupine CSIRT lahko vzpostavijo sodelovanje z nacionalnimi skupinami CSIRT tretjih držav. V okviru tega sodelovanja si lahko izmenjujejo ustrezne informacije, vključno z osebnimi podatki, v skladu s pravom Unije o varstvu podatkov.**
 - 4. Za olajšanje sodelovanja skupine CSIRT spodbujajo sprejetje in uporabo skupnih ali standardiziranih praks, sistemov razvrščanja in taksonomij v zvezi z naslednjim:
 - (a) postopki obvladovanja incidentov;
 - (b) kriznim upravljanjem kibernetike varnosti;
 - (c) usklajenim razkrivanjem šibkih točk.

Člen 11

Sodelovanje na nacionalni ravni

1. Kadar so pristojni organi iz člena 8, enotna kontaktna točka in skupine CSIRT iste države članice ločeni subjekti, med seboj sodelujejo pri izpolnjevanju obveznosti, ki jih določa ta direktiva.
2. Države članice zagotovijo, da bodisi njihovi pristojni organi bodisi skupine CSIRT prejmejo priglasiťve incidentov ter pomembnih kibernetiskih groženj in skorajšnjih dogodkov, predloženih v skladu s to direktivo. Kadar država članica sklēne, da njene skupine CSIRT ne prejēmajō takih priglasiťev, se tem skupinam v obsegu, potrebnem za opravljanje njihovih nalog, zagotovi dostop do podatkov o incidentih, ki jih v skladu s členom 20 priglasiťjo bistveni ali pomembni subjekti.
3. Vsaka država članica zagotovi, da njeni pristojni organi ali skupine CSIRT obvestijo njeno enotno kontaktno točko o priglasiťvah incidentov, pomembnih kibernetiskih groženj in skorajšnjih dogodkov v skladu s to direktivo.

4. Če je to potrebno za učinkovito opravljanje nalog in izpolnjevanje obveznosti, določenih v tej direktivi, države članice zagotovijo ustrezno sodelovanje med pristojnimi organi, **skupinami CSIRT**, enotnimi kontaktnimi točkami, organi kazenskega pregona, organi za varstvo podatkov in **pristojnimi organi, imenovanimi [...]** v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov], **pristojnimi organi v skladu z Izvedbeno uredbo Komisije 2019/1583, nacionalnimi regulativnimi organi, imenovanimi v skladu z Direktivo (EU) 2018/1972, nacionalnimi organi, imenovanimi v skladu s členom 17 Uredbe (EU) št. 910/2014, [...]** nacionalnimi finančnimi organi, imenovanimi v skladu z Uredbo (EU) XXXX/XXXX Evropskega parlamenta in Sveta [uredba o digitalni operativni odpornosti v finančnem sektorju], **ter pristojnimi organi, imenovanimi v skladu z drugimi sektorskimi pravnimi akti Unije, v zadevni državi članici.**
5. Države članice zagotovijo, da njihovi organi, pristojni na podlagi te direktive, **in pristojni organi, imenovani v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov]**, redno [...] **izmenjujejo** informacije o **opredelitvi kritičnih subjektov, tveganjih za kibernetško varnost, kibernetških grožnjah in incidentih ter nekibernetških tveganjih, grožnjah in incidentih**, ki vplivajo na bistvene subjekte, ki so opredeljeni kot kritični [ali kot subjekti, enakovredni kritičnim subjektom], v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov], ter o ukrepih, sprejetih [...] v odziv na taka tveganja in incidente. **Države članice zagotovijo tudi, da organi, pristojni na podlagi te direktive, [...] in pristojni organi, imenovani v skladu z Uredbo XXXX/XXXX [uredba o digitalni operativni odpornosti v finančnem sektorju], Direktivo 2018/1972 in Uredbo (EU) št. 910/2014 redno izmenjujejo ustrezne informacije.**

V zvezi s ponudniki storitev zaupanja in [...]zlasti [...]v primerih, ko je nadzorna vloga na podlagi te direktive dodeljena drugemu organu kot nadzornim organom, imenovanim v skladu z Uredbo (EU) št. 910/2014, nacionalni pristojni organi na podlagi te direktive pravočasno tesno sodelujejo tako, da izmenjujejo ustrezne informacije, da se zagotovita učinkovit nadzor in skladnost ponudnikov storitev zaupanja z zahtevami iz te direktive in Uredbe [XXXX/XXXX], in, kjer je ustrezno, nacionalni pristojni organ na podlagi te direktive brez nepotrebnega odlašanja obvesti nadzorni organ eIDAS o vseh priglasenih pomembnih kibernetičnih grožnjah ali incidentih, ki vplivajo na storitve zaupanja.

- 5a. [...] Za poenostavitev poročanja o incidentih lahko države članice vzpostavijo enotno vstopno točko za vse priglasitve, ki se zahtevajo v skladu s to direktivo in tudi v skladu z Uredbo (EU) 2016/679 in Direktivo 2002/58/ES. Države članice lahko uporabljajo enotno vstopno točko za priglasitve, ki se zahtevajo v skladu z drugimi sektorskimi pravnimi akti Unije. Ta enotna vstopna točka ne vpliva na uporabo določb Uredbe (EU) 2016/679 in Direktive 2002/58/ES, zlasti tistih, ki se nanašajo na neodvisne nadzorne organe.

POGLAVJE III

Sodelovanje EU

Člen 12

Skupina za sodelovanje

1. Za podpiranje in olajšanje strateškega sodelovanja ter izmenjave informacij med državami članicami [...], **pa tudi za krepitev zaupanja**, se ustanovi skupina za sodelovanje.
2. Skupina za sodelovanje opravlja svoje naloge na podlagi dvoletnih delovnih programov iz odstavka 6.
3. Skupino za sodelovanje sestavljajo predstavniki držav članic, Komisije in agencije ENISA. Evropska služba za zunanje delovanje sodeluje pri dejavnostih skupine za sodelovanje kot opazovalka. Evropski nadzorni organi **in pristojni organi, imenovani v skladu z Uredbo (EU) XXXX/XXXX [uredba o digitalni operativni odpornosti v finančnem sektorju]** [...], lahko **v skladu s členom 42(1) Uredbe (EU) XXXX/XXXX [uredba o digitalni operativni odpornosti v finančnem sektorju]** sodelujejo pri dejavnostih skupine za sodelovanje.

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

Komisija zagotovi sekretariat.

4. Skupina za sodelovanje ima naslednje naloge:
 - (a) zagotavljanje usmeritev pristojnim organom v zvezi s prenosom in izvajanjem te direktive;
 - (aa) **zagotavljanje usmeritev v zvezi z razvojem in izvajanjem politik za usklajeno razkrivanje šibkih točk iz člena 5(2)(c) in člena 6(1);**

- (b) izmenjava dobrih praks in informacij v zvezi z izvajanjem te direktive, tudi v zvezi s kibernetскими grožnjami, incidenti, šibkimi točkami, skorajšnjimi dogodki, pobudami za ozaveščanje, usposabljanji, vajami ter znanji in spretnostmi, krepitvijo zmogljivosti ter standardi in tehničnimi specifikacijami;
- (c) izmenjava nasvetov in sodelovanje s Komisijo pri nastajajočih pobudah za politiko o kibernetiski varnosti;
- (d) izmenjava nasvetov in sodelovanje s Komisijo pri pripravi osnutkov izvedbenih [...] aktov Komisije, sprejetih v skladu s to direktivo;
- (e) izmenjava dobrih praks in informacij z ustreznimi institucijami, organi, uradi in agencijami Unije;
- (ea) izmenjava mnenj o izvajanju sektorske zakonodaje, ki ureja vidike kibernetiske varnosti;**
- (f) obravnavanje poročil o [...] vzajemnem **učenju** iz člena 16(7);
- (g) obravnavanje [...] **izkušenj na podlagi** skupnih nadzornih dejavnosti v čezmejnih primerih iz člena 34;
- (h) zagotavljanje strateških usmeritev mreži skupin CSIRT **in mreži EU–CyCLONe** o posebnih porajajočih se vprašanjih;

(ha) izmenjava mnenj o nadaljnjem ukrepanju politike v zvezi z velikimi kibernetскими incidenti na podlagi izkušenj, pridobljenih v okviru mreže skupin CSIRT in mreže EU–CyCLONe;

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

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

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

(ka) vzpostavitev mehanizma vzajemnega učenja v skladu s členom 16 te direktive.

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

6. Skupina za sodelovanje do [24 mesecev po datumu začetka veljavnosti te direktive] in nato vsaki dve leti pripravi delovni program v zvezi z ukrepi, ki jih je treba sprejeti za izpolnitev njenih ciljev in nalog. Časovni okvir prvega programa, sprejetega v skladu s to direktivo, je usklajen s časovnim okvirom zadnjega programa, sprejetega v skladu z Direktivo (EU) 2016/1148.

7. Komisija lahko sprejme izvedbene akte, s katerimi določi postopkovne ureditve, potrebne za delovanje skupine za sodelovanje. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 37(2).
8. Skupina za sodelovanje se redno in vsaj enkrat letno sestane s skupino za odpornost kritičnih subjektov, ustanovljeno na podlagi Direktive (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov] z namenom spodbujanja strateškega sodelovanja in **olajševanja** izmenjave informacij.

Člen 13

Mreža skupin CSIRT

1. Za prispevanje h krepitvi zaupanja ter spodbujanje hitrega in učinkovitega operativnega sodelovanja med državami članicami se vzpostavi mreža nacionalnih skupin CSIRT.
2. Mrežo skupin CSIRT sestavljajo predstavniki tovrstnih skupin držav članic, **imenovanih v skladu s členom 9**, in CERT-EU. Komisija sodeluje v mreži skupin CSIRT kot opazovalka. Agencija ENISA zagotovi sekretariat in dejavno podpira sodelovanje med skupinami CSIRT.
3. Mreža skupin CSIRT ima naslednje naloge:
 - (a) izmenjava informacij o zmogljivostih skupin CSIRT;
 - (b) izmenjava ustreznih informacij o incidentih, skorajšnjih dogodkih, kibernetiskih grožnjah, tveganjih in šibkih točkah;

- (ba) **izmenjava informacij v zvezi s publikacijami in priporočili o kibernetiski varnosti;**
- (bb) **izmenjava tehničnih rešitev, ki olajšujejo tehnično obravnavo incidentov;**
- (bc) **izmenjava najboljših praks, orodij in postopkov v zvezi z nalogami skupin CSIRT;**
- (c) na prošnjo [...] **člana** mreže skupin CSIRT, na katero bi lahko vplival določen incident, izmenjava in obravnavanje informacij v zvezi z zadevnim incidentom ter z njim povezanimi kibernetiskimi grožnjami, tveganji in šibkimi točkami;
- (d) na prošnjo [...] **člana** mreže skupin CSIRT, obravnavanje in po možnosti izvajanje usklajenega odziva na incident, ki je bil ugotovljen na ozemlju v pristojnosti zadevne države članice;
- (e) zagotavljanje podpore državam članicam pri obravnavanju čezmejnih incidentov v skladu s to direktivo;
- (f) sodelovanje, **izmenjevanje najboljših praks** in zagotavljanje pomoči imenovanim skupinam CSIRT iz člena 6 v zvezi z upravljanjem usklajenega razkrivanja šibkih točk, ki vplivajo na več proizvajalcev ali ponudnikov proizvodov, storitev in postopkov IKT s sedežem v različnih državah članicah[...];
- (g) obravnavanje in določitev nadaljnjih oblik operativnega sodelovanja, tudi glede:
 - (i) kategorij kibernetiskih groženj in incidentov;
 - (ii) zgodnjega opozarjanja;
 - (iii) medsebojne pomoči;

- (iv) načel in načinov usklajevanja pri odzivanju na čezmejna tveganja in incidente;
- (v) prispevanja k nacionalnemu načrtu odzivanja na kibernetiske incidente in krize iz člena 7(3) **na zahtevo držav članic**;
- (h) obveščanje skupine za sodelovanje o svojih dejavnostih in nadaljnjih oblikah operativnega sodelovanja, obravnavanih v skladu s točko (g), ter po potrebi prošnja za usmeritve v zvezi s tem;
- (i) pregled vaj na področju kibernetiske varnosti, vključno s tistimi, ki jih organizira agencija ENISA;
- (j) na prošnjo posamezne skupine CSIRT obravnavanje njenih zmogljivosti in pripravljenosti;
- (k) sodelovanje in izmenjava informacij s centri za varnostne operacije na regionalni ravni in ravni Unije za izboljšanje skupnega situacijskega zavedanja na področju incidentov in groženj po vsej Uniji;
- (l) obravnavanje poročil o [...] **vzajemnem učenju** iz člena 16(7);
- (m) izdajanje smernic za olajšanje konvergence operativnih praks glede uporabe določb tega člena v zvezi z operativnim sodelovanjem.

4. Mreža skupin CSIRT za namene pregleda iz člena 35 do [24 mesecev po datumu začetka veljavnosti te direktive] in nato vsaki dve leti oceni napredek, dosežen na področju operativnega sodelovanja, in pripravi poročilo. V poročilu se zlasti oblikujejo sklepi o rezultatih [...] **vzajemnega učenja** iz člena 16, opravljenih v zvezi z nacionalnimi skupinami CSIRT, vključno s sklepi in priporočili v okviru navedenega člena. To poročilo se predloži tudi skupini za sodelovanje.
5. Mreža skupin CSIRT sprejme svoj poslovnik.
6. **Mreža skupin CSIRT sodeluje z mrežo EU-CyCLONe na podlagi sprejetih postopkovnih ureditev.**

Člen 14

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

1. Za podpiranje usklajenega upravljanja velikih kibernetiskih incidentov in kriz na operativni ravni in za zagotovitev redne izmenjave informacij med državami članicami ter institucijami, organi in agencijami Unije se ustanovi evropska organizacijska mreža za povezovanje v kibernetiski krizi (EU-CyCLONe).
2. Mreža EU-CyCLONe je sestavljena iz predstavnikov organov držav članic za upravljanje **kibernetiskih kriz**, imenovanih v skladu s členom 7[...]. **Komisija sodeluje pri dejavnostih mreže kot opazovalka.** Agencija ENISA zagotovi sekretariat mreže 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 k sodelovanju po potrebi povabi predstavnike ustreznih zainteresiranih strani.

3. Mreža EU-CyCLONe ima naslednje naloge:
- (a) zviševanje ravni pripravljenosti za upravljanje velikih **kibernetskih** incidentov in kriz;
 - (b) razvoj skupnega situacijskega zavedanja o [...] velikih **kibernetskih** incidentih in krizah;
 - (ba) ocenjevanje posledic in učinka zadevnih velikih kibernetskih incidentov ter predlaganje morebitnih blažilnih ukrepov;**
 - (c) usklajevanje upravljanja velikih **kibernetskih** incidentov in kriz ter podpiranje odločanja na politični ravni v zvezi s takimi incidenti in krizami;
 - (d) obravnavanje nacionalnih načrtov odzivanja na kibernetske incidente in krize iz člena 7(3[...]) **na zahtevo države članice**;[...]
4. Mreža EU-CyCLONe sprejme svoj poslovnik.
5. Mreža EU-CyCLONe redno poroča skupini za sodelovanje o **upravljanju velikih kibernetskih incidentov** in [...] kriznem upravljanju, pri čemer se osredotoča zlasti na njihov vpliv na bistvene in pomembne subjekte.
6. Mreža EU-CyCLONe sodeluje z mrežo skupin CSIRT na podlagi sprejetih postopkovnih ureditev.
7. **Mreža EU-CyCLONe Evropskemu parlamentu in Svetu do [24 mesecev po datumu začetka veljavnosti te direktive] predloži poročilo z oceno svojega dela.**

Člen 14a

Mednarodno sodelovanje

Unija lahko, kjer je ustrezno, v skladu s členom 218 PDEU sklene mednarodne sporazume s tretjimi državami ali mednarodnimi organizacijami, ki bi v skladu s pravom Unije o varstvu podatkov omogočali in urejali njihovo sodelovanje pri nekaterih dejavnostih skupine za sodelovanje, mreže skupin CSIRT in mreže EU-CyCLONe.

Člen 15

Poročilo o stanju kibernetске varnosti v Uniji

1. Agencija ENISA v sodelovanju s Komisijo **in skupino za sodelovanje** izda dvoletno poročilo o stanju kibernetске varnosti v Uniji. Poročilo [...] vključuje **zlasti** naslednje:
 - (aa) **oceno tveganja za kibernetско varnost na ravni Unije, pri čemer se upošteva okolje groženj;**
 - (a) [...] **oceno** razvoja zmogljivosti za kibernetско varnost v javnem in zasebnem sektorju po vsej Uniji;
 - (b) [...]
 - (c) **skupno oceno na podlagi [...] kvantitativnih in kvalitativnih kazalnikov** kibernetске varnosti, ki zagotavlja [...] **pregled** ravni zrelosti zmogljivosti za kibernetско varnost, **vključno z zmogljivostmi posameznih sektorjev.**

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

Člen 16

Vzajemno učenje

1. **Da bi se okrepilo medsebojno zaupanje, dosegla visoka skupna raven kibernetске varnosti ter okrepile zmogljivosti in politike držav članic na področju kibernetске varnosti, ki so potrebne za učinkovito izvajanje te direktive, skupina za sodelovanje ob podpori Komisije in po posvetovanju z [...] agencijo ENISA in po potrebi mrežo skupin CSIRT ter najpozneje v 24 [...] mesecih po začetku veljavnosti te direktive vzpostavi metodologijo [...] za objektivni, nediskriminatorni in pravičen sistem vzajemnega učenja [...] v zvezi z [...] izvajanjem te direktive v državah članicah. Sodelovanje pri vzajemnem učenju je prostovoljno. Sistem je sestavljen iz krogov ocenjevanja [...], ki jih izvajajo [...] strokovnjaki za kibernetско varnost iz držav članic [...], in zajema [...] enega ali več naslednjih vidikov:**
- (i) [...] izvajanje zahtev glede obvladovanja tveganj za kibernetско varnost ter obveznosti poročanja iz členov 18 in 20;
 - (ii) [...] zmogljivosti, vključno z razpoložljivimi [...] viri, in [...] opravljanje nalog nacionalnih pristojnih organov **iz člena 8 in skupin CSIRT iz člena 9;**

[...]

(iii[...]) [...] **izvajanje** medsebojne pomoči iz člena 34;

(iv) [...] **izvajanje** okvira za izmenjavo informacij iz člena 26 [...].

2. **Merila, na podlagi katerih države članice imenujejo strokovnjake, primerne za sodelovanje v krogih vzajemnega učenja, so [...]** objektivna, nediskriminatorna, pravična in pregledna [...] **ter vključena v metodologijo iz odstavka 1.** Agencija ENISA in Komisija **lahko** imenujeta strokovnjake, ki v **krogih vzajemnega učenja** sodelujejo kot opazovalci.
[...]

3. [...].

- 3a. **Pred začetkom krogov vzajemnega učenja lahko države članice opravijo samooceno vidikov, ki se obravnavajo v posameznem krogu vzajemnega učenja, to samooceno pa pošljejo imenovanim strokovnjakom iz odstavka 2.**
4. **Vzajemno učenje [...] lahko vključuje[...] fizične ali virtualne obiske na kraju samem in izmenjave na daljavo. Države članice [...], ki sodelujejo pri vzajemnem učenju, ob upoštevanju načela dobrega sodelovanja imenovanim strokovnjakom zagotovijo [...] informacije, potrebne za oceno [...], brez poseganja v nacionalno zakonodajo ali zakonodajo Unije o varstvu zaupnih ali tajnih podatkov ali zaščito temeljnih državnih funkcij, kot je nacionalna varnost. Vse informacije, pridobljene v okviru postopka [...] vzajemnega učenja, se uporabljajo izključno v ta namen. Strokovnjaki, ki sodelujejo pri [...] vzajemnem učenju, občutljivih ali zaupnih informacij, pridobljenih v tem okviru [...], ne razkrijejo tretjim osebam. Država članica, ki sodeluje pri vzajemnem učenju, lahko nasprotuje imenovanju določenih strokovnjakov na podlagi ustrezno utemeljenih razlogov, ki se sporočijo skupini za sodelovanje.**

5. Ko so vidiki **predmet kroga vzajemnega učenja** [...], so v [...] štirih letih po zaključku **zadevnega kroga vzajemnega učenja izključeni iz nadaljnjih krogov vzajemnega učenja** [...] **za sodelujočo državo članico, razen če zadevna država članica tega ne zahteva ali se strinja s predlogom skupine za sodelovanje** [...].
6. [...]
7. Strokovnjaki, ki sodelujejo v [...] **krogih vzajemnega učenja**, pripravijo poročila o ugotovitvah in sklepih [...] **iz ocen. Države članice lahko predložijo pripombe na osnutke poročil, priložene poročilu, ki jih zadevajo. Končna poročila se predložijo** [...] skupini za sodelovanje [...]. **Države članice se lahko odločijo, da poročila, ki jih zadevajo, javno objavijo.**

POGLAVJE IV

Obveznosti glede obvladovanja tveganj za kibernetško varnost in poročanja

ODDELEK I

Obvladovanje tveganj za kibernetško varnost in poročanje

Člen 17

Upravljanje

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

Uporaba tega odstavka ne posega v nacionalno zakonodajo držav članic v zvezi s pravili o odgovornosti v javnih institucijah, pa tudi ne v odgovornost javnih uslužbencev ter izvoljenih in imenovanih uradnikov.

2. Države članice zagotovijo, da se **morajo člani upravnega organa** redno udeleževati [...] usposabljanj, da pridobijo dovolj znanja in spretnosti za razumevanje in ocenjevanje tveganj za kibernetško varnost ter praks upravljanja in njihovega vpliva na dejavnosti subjekta.

Člen 18

Ukrepi za obvladovanje tveganj za kibernetisko varnost

- 1a. V tej direktivi je uporabljen pristop, ki vključuje vse nevarnosti, tj. zaščito omrežij in informacijskih sistemov ter njihovega fizičnega okolja pred kakršnimi koli dogodki, ki bi lahko ogrozili razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki jih ponujajo ali so dostopne prek omrežij in informacijskih sistemov.
1. Države članice zagotovijo, da bistveni in pomembni subjekti sprejmejo ustrezne in sorazmerne tehnične in organizacijske ukrepe za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih ti subjekti uporabljajo za opravljanje storitev. Ob upoštevanju stanja tehnike **in stroškov izvajanja** se s temi ukrepi zagotovi raven varnosti omrežij in informacijskih sistemov, primerna obstoječemu tveganju. **Pri ocenjevanju sorazmernosti teh ukrepov se ustrezno upoštevajo stopnja izpostavljenosti subjekta tveganjem, njegova velikost, verjetnost pojava incidentov in njihova resnost. Ob upoštevanju ravni in vrste tveganja za družbo v primeru incidentov, ki prizadenejo bistvene ali pomembne subjekte, so lahko ukrepi za obvladovanje tveganj za kibernetisko varnost, ki se naložijo pomembnim subjektom, manj strogi od ukrepov, ki se naložijo bistvenim subjektom.**

2. Ukrepi iz odstavka 1 vključujejo vsaj naslednje:
- (a) analizo tveganja in varnostna pravila za informacijske sisteme;
 - (b) obvladovanje incidentov (preprečevanje in odkrivanje incidentov ter odzivanje nanje **in okrevanje po njih**);
 - (c) upravljanje neprekinjenega poslovanja in krizno upravljanje;
 - (d) varnost dobavne verige, vključno z vidiki, povezanimi z varnostjo, ki se nanašajo na odnose med posameznim subjektom in njegovimi **neposrednimi** dobavitelji ali ponudniki storitev, kot so ponudniki storitev shranjevanja in obdelave podatkov ali upravljanih varnostnih storitev;
 - (e) varnost pri pridobivanju, razvoju in vzdrževanju omrežij in informacijskih sistemov, vključno z obravnavanjem in razkrivanjem šibkih točk;
 - (f) politike in postopke [...] za oceno učinkovitosti ukrepov za obvladovanje tveganj za kibernetško varnost;
 - (g) **politike o uporabi kriptografije in šifriranja;**
 - (ga) varnost človeških virov, politike nadzora dostopa in upravljanje sredstev.**
3. Države članice zagotovijo, da **morajo** subjekti pri preučevanju ustreznih ukrepov iz točke (d) odstavka 2 upoštevati šibke točke posameznega **neposrednega** dobavitelja in ponudnika storitev ter splošno kakovost proizvodov ter praks svojih dobaviteljev in ponudnikov storitev na področju kibernetške varnosti, vključno z njihovimi varnimi razvojnimi postopki. **Države članice zagotovijo tudi, da morajo subjekti pri obravnavi ustreznih ukrepov iz točke (d) odstavka 2 upoštevati rezultate usklajenih ocen tveganja, izvedenih v skladu s členom 19(1).**

4. Države članice zagotovijo, da subjekt, če ugotovi, da njegove storitve oziroma naloge ne izpolnjujejo zahtev iz odstavka 2, brez nepotrebnega odlašanja sprejme vse potrebne popravne ukrepe za zagotovitev, da zadevna storitev izpolnjuje zahteve.
5. Komisija lahko sprejme izvedbene akte, s katerimi določi tehnične in metodološke, **po potrebi pa tudi sektorske posebnosti** elementov iz odstavka 2 tega člena. **Komisija do [18 mesecev po začetku veljavnosti te direktive] sprejme izvedbene akte, s katerimi določi tehnične in metodološke specifikacije za subjekte iz člena 24(1) in ponudnike storitev zaupanja iz točke 8 Priloge I. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 37(2).** Komisija[...] pri pripravi [...] **takih izvedbenih aktov** [...] v največji možni meri **upoštevata** mednarodne in evropske standarde ter ustrezne tehnične specifikacije **in s skupino za sodelovanje in agencijo ENISA izmenja nasvete glede osnutka izvedbenega akta v skladu s členom 12(4)(d).**
6. [...]

Člen 19

Usklajene ocene tveganja v EU za kritične dobavne verige

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

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

Člen 20

Obveznosti poročanja

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

2. [...]

Po potrebi [...] **bistveni in pomembni** subjekti prejemnike svojih storitev, ki bi jih pomembna kibernetična grožnja lahko prizadela, brez nepotrebnega odlašanja obvestijo o vseh ukrepih ali sredstvih, ki jih lahko ti prejemniki sprejmejo v odziv na zadevno grožnjo. Kjer je ustrezno, subjekti zadevne prejemnike obvestijo tudi o sami grožnji. **Sama priglasitev priglasitelju ne sme naložiti dodatne odgovornosti.**

3. Incident se šteje za pomemben, če:
- (a) je zadevnemu subjektu povzročil ali bi mu lahko povzročil [...] **resne** operativne motnje **pri opravljanju storitve** ali finančne izgube;
 - (b) je vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnjih materialnih ali nematerialnih izgub.
4. Države članice zagotovijo, da zadevni subjekti za namen priglasitve iz odstavka 1 pristojnim organom in skupini CSIRT predložijo:
- (a) brez nepotrebnega odlašanja in v vsakem primeru v 24 urah po seznanitvi z incidentom začetno priglasitev **kot zgodnje opozorilo**, v kateri je, kjer je ustrezno, navedeno, ali je bil incident domnevno povzročen z nezakonitim ali zlonamernim dejanjem;
 - (b) na zahtevo pristojnega organa ali skupine CSIRT vmesno poročilo o ustreznih posodobitvah stanja;
 - (c) **končno** poročilo, najpozneje v enem mesecu po predložitvi začetne priglasitve iz točke (a), ki vključuje vsaj naslednje:
 - (i) podroben opis incidenta, njegove resnosti in vpliva;
 - (ii) vrsto grožnje ali temeljnega vzroka, ki je verjetno sprožil incident;
 - (iii) izvedene blažilne ukrepe in take ukrepe v teku.

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

Odstopanje od roka iz točke (c) je mogoče utemeljiti zlasti v primerih, ko incident še traja.

5. Pristojni nacionalni organi ali skupina CSIRT [...] **brez nepotrebnega odlašanja** po prejemu začetne priglasitve iz točke (a) odstavka 4 odgovorijo priglasitelju, vključno z začetnimi povratnimi informacijami o incidentu in, na zahtevo subjekta, usmeritvami glede izvajanja morebitnih blažilnih ukrepov. Če skupina CSIRT ni prejela priglasitve iz odstavka 1, usmeritve zagotovi pristojni organ v sodelovanju s skupino CSIRT. Skupina CSIRT na zahtevo zadevnega subjekta zagotovi dodatno tehnično podporo. Če se za incident sumi, da je kazenske narave, pristojni nacionalni organi ali skupina CSIRT zagotovijo tudi usmeritve o poročanju o incidentih organom kazenskega pregona.
6. Kadar je to ustrezno in zlasti če incident iz odstavka 1 zadeva dve ali več držav članic, pristojni organ, skupina CSIRT ali **enotna kontaktna točka** obvesti druge prizadete države članice in agencijo ENISA o incidentu. **Te informacije vključujejo vsaj elemente iz odstavka 4 tega člena.** Pristojni organi, skupine CSIRT in enotne kontaktne točke pri tem v skladu s pravom Unije ali nacionalno zakonodajo, ki je skladna s pravom Unije, zaščitijo varnost in poslovne interese subjekta ter zaupnost predloženih informacij.
7. Kadar je ozaveščenost javnosti potrebna za preprečitev incidenta ali obravnavo incidenta, ki je v teku, ali kadar je razkritje incidenta kako drugače v javnem interesu, lahko pristojni organ ali skupina CSIRT in po potrebi organi ali skupine CSIRT drugih zadevnih držav članic po posvetovanju z zadevnim subjektom obvestijo javnost o incidentu ali zahtevajo, da to stori subjekt.

8. Enotna kontaktna točka na zahtevo pristojnega organa ali skupine CSIRT priglasitve, prejete v skladu z odstavkom[...] 1 [...], posreduje enotnim kontaktnim točkam drugih prizadetih držav članic.
9. Enotna kontaktna točka agenciji ENISA vsakih šest mesecev predloži zbirno poročilo, vključno z anonimiziranimi in zbirnimi podatki o incidentih, pomembnih kibernetiskih grožnjah in skorajšnjih dogodkih, priglašeni v skladu z odstavkom[...] 1 [...] ter členom 27. Da bi prispevala k zagotavljanju primerljivih informacij, lahko agencija ENISA izda tehnične usmeritve o parametrih informacij, vključenih v zbirno poročilo. **Agencija ENISA vsakih šest mesecev obvešča skupino za sodelovanje in mrežo skupin CSIRT o svojih ugotovitvah v zvezi s prejetimi priglasitvami.**
10. Pristojni organi zagotovijo pristojnim organom, imenovanim v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov], informacije o incidentih in kibernetiskih grožnjah, ki so jih v skladu z odstavkoma 1 in 2 priglasili bistveni subjekti, opredeljeni kot kritični subjekti [ali kot subjekti, enakovredni kritičnim subjektom,] v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov].
11. Komisija lahko sprejme izvedbene akte, s katerimi se podrobneje določijo vrsta informacij, oblika in postopek priglasitve, predložene v skladu z odstavkoma 1 in 2. Komisija lahko sprejme izvedbene akte za podrobnejšo določitev primerov, v katerih se incident šteje za pomemben v skladu z odstavkom 3. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 37(2).

Člen 21

Uporaba evropskih certifikacijskih shem za kibernetko varnost

1. **Države članice lahko** za dokaz izpolnjevanja nekaterih zahtev iz člena 18 od [...] subjektov zahtevajo, naj **uporabljajo** [...] **določene** proizvode, storitve in postopke IKT, **ki so certificirani** na podlagi določenih evropskih certifikacijskih shem za kibernetko varnost, sprejetih v skladu s členom 49 Uredbe (EU) 2019/881. Proizvode, storitve in postopke **IKT**, ki so predmet certificiranja, lahko razvije bistveni ali pomembni subjekt ali jih dobavijo tretje osebe.
2. Komisija lahko [...] sprejme [...] **izvedbene** akte, s katerimi določi, od katerih kategorij bistvenih **ali pomembnih** subjektov se zahteva, **da uporabljajo določene certificirane izdelke, storitve in postopke IKT ali** pridobijo certifikat, na podlagi katerega [...] evropske certifikacijske sheme za kibernetko varnost, **sprejete v skladu s členom 49 Uredbe (EU) 2019/881.** [...] Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 37(2). Komisija pri pripravi takih izvedbenih aktov v skladu s členom 56 Uredbe (EU) 2019/881:
 - (i) **upošteva učinek ukrepov na proizvajalce ali ponudnike takšnih proizvodov, storitev ali postopkov IKT ter na uporabnike v smislu stroška teh ukrepov, pa tudi družbene ali gospodarske koristi zaradi pričakovane višje ravni varnosti ciljnih proizvodov, storitev ali postopkov IKT, pa tudi razpoložljivosti njihovih alternativ na trgu;**
 - (ii) **opravi odprto, pregledno in vključujoče posvetovanje z vsemi ustreznimi zainteresiranimi stranmi in državami članicami;**

- (i) **upošteva roke za izvajanje, prehodne ukrepe in obdobja, zlasti glede morebitnega učinka ukrepov na proizvajalce ali ponudnike proizvodov, storitev ali postopkov IKT ali njihove uporabnike, zlasti MSP;**
- (ii) **upošteva obstoj in izvajanje ustrezne zakonodaje držav članic.**

3. Komisija lahko od agencije ENISA zahteva, naj pripravi predlogo za shemo **ali pregleda obstoječo evropsko certifikacijsko shemo za kibernetško varnost** v skladu s členom 48(2) Uredbe (EU) 2019/881, če za namene odstavka 2 **tega člena** ni na voljo ustrezne evropske certifikacijske sheme za kibernetško varnost.

Člen 22

Standardizacija

1. Za zagotovitev usklajenega izvajanja člena 18(1) in (2) države članice spodbujajo uporabo evropskih ali mednarodno sprejetih standardov in specifikacij, pomembnih za varnost omrežij in informacijskih sistemov, ne da bi predpisale uporabo določene vrste tehnologije ali ji dajale prednost.
2. Agencija ENISA v sodelovanju z državami članicami pripravi nasvete in smernice za tehnična področja, ki se upoštevajo v zvezi z odstavkom 1, ter za že obstoječe standarde, vključno z nacionalnimi standardi držav članic, s katerimi bi lahko zajeli navedena področja.

Člen 23

Podatkovne zbirke domenskih imen in podatkov o registraciji

1. Da bi prispevale k varnosti, stabilnosti in odpornosti sistema domenskih imen, države članice zagotovijo, da registri vrhnjih domenskih imen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene, z ustrezno skrbnostjo zbirajo ter vzdržujejo točne in popolne podatke o registraciji domenskih imen v posebni podatkovni zbirki, [...] **v skladu z zakonodajo Unije o varstvu podatkov v zvezi s podatki, ki so osebni podatki.**
2. Države članice zagotovijo, da podatkovne zbirke podatkov o registraciji domenskih imen iz odstavka 1 vsebujejo ustrezne informacije za identifikacijo imetnikov domenskih imen in kontaktnih točk, ki upravljajo domenska imena v okviru vrhnjih domen, in navezavo stika z njimi, **vključno z vsaj naslednjimi podatki:**
 - (a) **domensko ime**
 - (b) **datum registracije**
 - (c) **podatki regulatorja, tudi:**
 - (i) **za posameznike – ime, priimek in elektronski naslov;**
 - (ii) **za pravne osebe – ime in elektronski naslov.**

3. Države članice zagotovijo, da imajo registri vrhnjih domenskih imen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene, vzpostavljene politike in postopke, ki zagotavljajo, da podatkovne zbirke vključujejo točne in popolne informacije. Države članice zagotovijo, da so take politike in postopki javno dostopni.
4. Države članice zagotovijo, da registri vrhnjih domenskih imen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene, po registraciji domenskega imena brez nepotrebnega odlašanja objavijo podatke o registraciji domene, ki niso osebni podatki.
5. Države članice zagotovijo, da registri vrhnjih domenskih imen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene, omogočajo dostop do podatkov o registraciji posameznih domenskih imen na podlagi zakonitih in ustrezno utemeljenih zahtevkov oseb, ki imajo upravičen razlog za dostop, v skladu z zakonodajo Unije o varstvu podatkov. Države članice zagotovijo, da registri vrhnjih domenskih imen in subjekti, ki opravljajo storitve registracije domenskih imen za vrhnje domene, brez nepotrebnega odlašanja, **v vsakem primeru pa v 72 urah**, odgovorijo na vse zahteve za dostop. Države članice zagotovijo, da so politike in postopki za razkrivanje takih podatkov javno dostopni.

Oddelek II

Sodna pristojnost in registracija

Člen 24

Sodna pristojnost in teritorialnost

- 1a. Za subjekte po tej direktivi se šteje, da so pod sodno pristojnostjo države članice, v kateri opravljajo svoje storitve. Za subjekte iz točk 1 do 7 in 10 Priloge I, ponudnike storitev zaupanja in ponudnike stičišča omrežij iz točke 8 Priloge I ter subjekte iz točk 1 do 5 Priloge II se šteje, da so pod sodno pristojnostjo države članice, na ozemlju katere imajo sedež.
1. Za ponudnike storitev sistema domenskih imen, registre vrhnjih domenskih imen, [...] in subjekte, ki opravljajo storitve registracije domenskih imen za vrhnje domene, ponudnike storitev računalništva v oblaku, ponudnike storitev podatkovnih centrov, [...] ponudnike omrežij za dostavo vsebine, **ponudnike upravljanih storitev in ponudnike upravljanih varnostnih storitev** iz točke 8 in točke 8a Priloge I ter ponudnike digitalnih storitev iz točke 6 Priloge II se šteje, da so pod sodno pristojnostjo države članice, v kateri imajo glavni sedež v Uniji.
2. Za namene te direktive se za subjekte iz odstavka 1 šteje, da imajo glavni sedež v Uniji v državi članici, v kateri se **večinoma** sprejemajo odločitve v zvezi z ukrepi za obvladovanje tveganj za kibernetско varnost. Če **kraja, kjer se takšne odločitve večinoma sprejemajo, ni mogoče določiti ali** se take odločitve ne sprejemajo na sedežu v Uniji, se šteje, da je glavni sedež v državi članici, v kateri je sedež subjekta z največjim številom zaposlenih v Uniji. **Kadar storitve opravljajo povezane družbe, se za glavni sedež šteje glavni sedež povezanih družb.**

3. Če subjekt iz odstavka 1 nima sedeža v Uniji, vendar v njej opravlja storitve, določi predstavnika v Uniji. Predstavnik ima sedež v eni od držav članic, v katerih se opravljajo storitve. Za tak subjekt se šteje, da je pod sodno pristojnostjo države članice, v kateri ima predstavnika sedež. Če ni imenovanega predstavnika v Uniji v skladu s tem členom, lahko katera koli država članica, v kateri subjekt opravlja storitve, uvede sodne postopke proti subjektu zaradi neizpolnjevanja obveznosti po tej direktivi.
4. Imenovanje predstavnika s strani subjekta iz odstavka 1 ne posega v sodne postopke, ki se lahko uvedejo proti samemu subjektu.
- 4a. **Države članice, ki so prejele zahtevek za medsebojno pomoč v zvezi s subjekti iz odstavka 1, lahko v mejah zahtevka sprejmejo ustrezne nadzorne in izvršilne ukrepe v zvezi z zadevnim subjektom, ki opravlja storitve ali ima omrežje in informacijski sistem na njihovem ozemlju.**

Člen 25

Register za nekatere subjekte za digitalno infrastrukturo in ponudnike digitalnih storitev

1. [...] **Države članice zagotovijo, da morajo** [...] subjekti iz člena 24(1), ki imajo na njihovem ozemlju glavni sedež, ali, če nimajo sedeža v Uniji, subjekti, katerih imenovani predstavnik v Uniji je bil ustanovljen na njihovem ozemlju, do [najpozneje 12 mesecev po začetku veljavnosti Direktive] [...] **pristojnim organom** [...] predložiti naslednje informacije:

(a) ime subjekta;

(aa) vrsto subjekta v skladu s prilogama I in II k tej direktivi;

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

(c) posodobljene kontaktne podatke, vključno z elektronskimi naslovi in telefonskimi številkami subjektov **in njihovih predstavnikov;**

(d) seznam držav članic, v katerih subjekt opravlja storitev.

Kjer je to ustrezno, se te informacije predložijo prek nacionalnih mehanizmov [...] za samopriglasitev iz člena 2a.

2. **Države članice zagotovijo, da s[...]**subjekti iz odstavka 1 brez odlašanja, v vsakem primeru pa v treh mesecih od datuma začetka veljavnosti spremembe, **priglasijo tudi [...]** vse spremembe podatkov, ki so jih predložili v skladu z odstavkom 1.
3. [...] **Enotne kontaktne točke držav članic posredujejo informacije iz odstavkov 1 in 2 [...]**
[...] **agenciji ENISA.** [...]

3a. Agencija ENISA na podlagi informacij, prejetih v skladu z odstavkom 3 tega člena, vzpostavi in vodi register subjektov iz odstavka 1. Agencija ENISA na zahtevo držav članic ustreznim pristojnim organom omogoči dostop do registra, pri čemer zagotovi potrebna jamstva za varovanje zaupnosti informacij, kjer je to ustrezno.

4. [...]

POGLAVJE V

Izmenjava informacij

Člen 26

Dogovori o izmenjavi informacij o kibernetiski varnosti

1. Države članice [...] zagotovijo, da si bistveni in pomembni subjekti lahko **prostovoljno** izmenjujejo ustrezne informacije o kibernetiski varnosti, vključno z informacijami, ki se nanašajo na kibernetiske grožnje, **skorajšnje dogodke**, šibke točke, kazalnike ogroženosti, taktike, tehnike in postopke, opozorila glede kibernetiske varnosti in orodja za konfiguracijo, če taka izmenjava informacij:
 - (a) stremlji k preprečevanju in odkrivanju incidentov, odzivanju nanje ali njihovi ublažitvi;

- (b) zvišuje raven kibernetске varnosti, zlasti z ozaveščanjem v zvezi s kibernetскими grožnjami, omejevanjem ali oviranjem zmožnosti širjenja takih groženj, podpiranjem vrste obrambnih zmogljivosti, odpravljanjem in razkrivanjem šibkih točk, tehnikami odkrivanja groženj, strategijami za zmanjšanje tveganja ali fazami odzivanja in okrevanja.
2. Države članice zagotovijo, da izmenjava informacij poteka v [...] skupnostih bistvenih in pomembnih subjektov. Taka izmenjava se izvaja na podlagi dogovorov o izmenjavi informacij, ob upoštevanju morebitne občutljivosti informacij, ki se izmenjujejo [...].
 3. Države članice **lahko** določijo pravila o postopku, operativnih elementih (vključno z uporabo namenskih platform IKT), vsebini in pogojih dogovorov o izmenjavi informacij iz odstavka 2. Taka pravila **lahko** določajo tudi podrobnosti sodelovanja javnih organov pri takih dogovorih in operativne elemente, vključno z uporabo namenskih platform informacijske tehnologije. Države članice nudijo podporo za uporabo takih dogovorov v skladu s svojimi politikami iz člena 5(2)(g).
 4. Bistveni in pomembni subjekti obvestijo pristojne organe o svojem sodelovanju pri dogovorih o izmenjavi informacij iz odstavka 2 po sklenitvi takih dogovorov ali, kjer je to ustrezno, o odstopu od dogovora, ko odstop začne veljati.
 5. Agencija ENISA [...] podpira sklenitev dogovorov o izmenjavi informacij o kibernetски varnosti iz odstavka 2 z zagotavljanjem dobrih praks in usmeritev.

Člen 27

Prostovoljna priglasitev ustreznih informacij

1. **Brez poseganja v člen 20 države članice zagotovijo, da lahko bistveni in pomembni subjekti pristojnim organom ali skupinam CSIRT prostovoljno priglasijo vse relevantne incidente, kibernetike grožnje ali skorajšnje dogodke.**
2. Države članice zagotovijo, da lahko subjekti, ki ne spadajo na področje uporabe te direktive, brez poseganja v člen 3 prostovoljno predložijo priglasitve o pomembnih incidentih, kibernetičnih grožnjah ali skorajšnjih dogodkih. Države članice pri obdelavi priglasitev ravnajo v skladu s postopkom iz člena 20. Pred prostovoljnimi priglasitvami lahko prednostno obdelajo obvezne priglasitve. **Brez poseganja v preiskovanje, odkrivanje in pregon kaznivih dejanj p[...]** prostovoljno poročanje poročajočemu subjektu ne naloži nikakršnih dodatnih obveznosti, ki zanj ne bi veljale, če ne bi predložil priglasitve.
3. **Prostovoljne priglasitve se obdelajo le, kadar takšna obdelava zadevnim državam članicam ne pomeni nesorazmernega ali neupravičenega bremena.**

POGLAVJE VI

Nadzor in izvrševanje

Člen 28

Splošni vidiki, povezani z nadzorom in izvrševanjem

1. Države članice zagotovijo, da pristojni organi učinkovito spremljajo izpolnjevanje obveznosti iz te direktive, zlasti obveznosti iz členov 18, [...] 20 in 23, in sprejmejo ukrepe za zagotovitev takega izpolnjevanja. **Države članice lahko pristojnim organom dovolijo prednostno razvrščanje nadzora na podlagi pristopa, ki temelji na tveganju.**
2. Pristojni organi pri obravnavi kibernetičnih incidentov [...] tesno sodelujejo z organi za varstvo podatkov, **pristojnimi organi, imenovanimi v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov], nadzornimi organi, imenovanimi v skladu z Uredbo (EU) št. 910/2014, in drugimi pristojnimi organi, imenovanimi v skladu s sektorskimi pravnimi akti Unije.**
3. **Brez poseganja v nacionalne zakonodajne in institucionalne okvire države članice zagotovijo, da imajo pristojni organi pri nadzoru skladnosti subjektov javne uprave s to direktivo in pri izvrševanju morebitnih sankcij za neskladnost ustrezna pooblastila, da lahko takšne naloge izvajajo operativno neodvisno od nadzorovanih subjektov. Države članice se lahko odločijo za uvedbo ustreznih, sorazmernih in učinkovitih nadzornih in izvršilnih ukrepov v zvezi s temi subjekti v skladu z nacionalnimi okviri in pravnim redom.**

Nadzor in izvrševanje pri bistvenih subjektih

1. Države članice zagotovijo, da so ukrepi nadzora ali izvrševanja, naloženi bistvenim subjektom v zvezi z obveznostmi iz te direktive, učinkoviti, sorazmerni in odvračilni, ob upoštevanju okoliščin posameznega primera.
2. Države članice zagotovijo, da pristojni organi pri izvajanju svojih nadzornih nalog v zvezi z bistvenimi subjekti **uporabljajo pristop, ki temelji na tveganju, in da so pooblaščen**, da v zvezi s temi subjekti **sprejmejo vsaj naslednje ukrepe**:
 - (a) inšpekcijske preglede na kraju samem in nadzor na daljavo, vključno z naključnimi pregledi;
 - (b) redne [...] **varnostne presoje**;
 - (c) ciljno usmerjene varnostne presoje, ki temeljijo na ocenah tveganja ali razpoložljivih informacijah o tveganju;
 - (d) varnostne preglede, ki temeljijo na objektivnih, nediskriminatornih, poštenih in preglednih merilih za oceno tveganja, **v sodelovanju z zadevnim subjektom, kadar je to potrebno iz tehničnih razlogov**;
 - (e) zahtevajo informacije, potrebne za oceno ukrepov za kibernetško varnost, ki jih je sprejel subjekt, vključno z dokumentiranimi politikami na področju kibernetške varnosti[...];
 - (f) zahtevajo dostop do podatkov, dokumentov ali kakršnih koli informacij, potrebnih za opravljanje njihovih nadzornih nalog;
 - (g) zahtevajo dokaze o izvajanju politik na področju kibernetške varnosti, kot so rezultati varnostnih presoj, ki jih izvede usposobljen presojevalec, in ustrezni temeljni dokazi.

- 2a. **Pristojni organi lahko za opravljanje svojih nadzornih nalog iz odstavka 2 tega člena izdelajo metodologijo za nadzor, ki omogoča prednostno razvrščanje takšnih nalog na podlagi pristopa, ki temelji na tveganju.**
3. Pristojni organi pri izvajanju svojih pooblastil iz točk (e) do (g) odstavka 2 navedejo namen zahteve in opredelijo zahtevane informacije.
4. Države članice zagotovijo, da so pristojni organi pri izvajanju svojih izvršilnih pooblastil v zvezi z bistvenimi subjekti pooblaščen **vsaj**, da:
- (a) izdajo opozorila o subjektovem neizpolnjevanju obveznosti, določenih v tej direktivi;
 - (b) izdajo zavezujoča navodila ali odredbo, s katero od takih subjektov zahtevajo, da odpravijo ugotovljene pomanjkljivosti ali kršitve obveznosti, določene v tej direktivi;
 - (c) takim subjektom odredijo, naj prenehajo z ravnanjem, ki ni skladno z obveznostmi, določenimi v tej direktivi, in naj tega ravnanja ne ponovijo več;
 - (d) takim subjektom odredijo, naj na določen način in v določenem roku uskladijo svoje ukrepe za obvladovanje tveganj in/ali obveznosti poročanja z obveznostmi iz členov 18 in 20;
 - (e) takim subjektom odredijo, naj obvestijo fizične ali pravne osebe, za katere opravljajo storitve ali dejavnosti, na katere bi lahko vplivala pomembna kibernetična grožnja, o **naravi grožnje, pa tudi o** vseh mogočih zaščitnih ali popravnih ukrepih, ki jih lahko take fizične ali pravne osebe sprejmejo v odziv na zadevno grožnjo;
 - (f) takim subjektom odredijo, naj v razumnem roku izvedejo priporočila, dana na podlagi varnostne presoje;
 - (g) [...]

- (h) takim subjektom odredijo, naj na določen način objavijo vidike neizpolnjevanja obveznosti, določenih v tej direktivi, **če takšno javno razkritje nima za posledico škodljive izpostavljenosti zadevnega subjekta;**
 - (i) [...]
 - (j) naložijo ali zahtevajo, naj ustrezni organi ali sodišča v skladu z nacionalno zakonodajo naložijo upravno globo v skladu s členom 31, poleg ali namesto ukrepov iz točk (a) do (i) tega odstavka glede na okoliščine posameznega primera.
5. Če se izvršilni ukrepi, sprejeti v skladu s točkami (a) do (d) in (f) odstavka (4) izkažejo za neučinkovite, države članice zagotovijo, da so pristojni organi pooblaščen za določitev roka, v katerem mora bistveni subjekt sprejeti potrebne ukrepe za odpravo pomanjkljivosti ali izpolnitev zahtev teh organov. Če se zahtevani ukrepi ne sprejmejo v določenem roku, države članice zagotovijo, da so pristojni organi pooblaščen, da:
- (a) začasno prekličejo ali od certifikacijskega organa ali organa, pristojnega za izdajo dovoljenj, **ali sodišč v skladu z nacionalno zakonodajo** zahtevajo, naj začasno prekliče certifikat ali dovoljenje za del storitev ali dejavnosti ali vse storitve ali dejavnosti, ki jih opravlja bistveni subjekt;
 - (b) uvedejo ali zahtevajo, naj ustrezni organi ali sodišča v skladu z nacionalno zakonodajo uvedejo začasno prepoved opravljanja vodstvenih funkcij vseh oseb, ki za bistveni subjekt opravljajo poslovodne naloge na ravni glavnega izvršnega direktorja ali pravnega zastopnika, in vseh drugih fizičnih oseb, ki so odgovorne za kršitev.

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

Sankcije 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 predstavnik bistvenega subjekta na podlagi pooblastila za njegovo zastopanje, odločanje v njegovem imenu ali izvajanje nadzora nad njim, pooblastila za zagotavljanje, da bistveni subjekt izpolnjuje obveznosti, določene v tej direktivi. Države članice zagotovijo, da lahko te fizične osebe odgovarjajo za kršitev svojih dolžnosti, da bi zagotovile izpolnjevanje obveznosti, določenih v tej direktivi. **Kar zadeva subjekte javne uprave, ta določba ne posega v zakonodajo držav članic glede odgovornosti javnih uslužbencev ter izvoljenih in imenovanih uradnikov.**
7. Pristojni organi pri sprejemanju kakršnih koli izvršilnih ukrepov ali uporabi kakršnih koli sankcij v skladu z odstavkoma 4 in 5 spoštujejo pravice do obrambe in upoštevajo okoliščine vsakega posameznega primera ter ustrezno upoštevajo vsaj naslednje:
 - (a) resnost kršitve in pomembnost kršenih določb. Med kršitvami, ki bi se morale šteti za resne, so: ponavljajoče se kršitve, nepriglasitev ali neodprava incidentov z znatnim negativnim vplivom, neodprava pomanjkljivosti v skladu z zavezujočimi navodili pristojnih organov, oviranje presoje ali dejavnosti spremljanja, ki jih je odredil pristojni organ po ugotovitvi kršitve, predložitev napačnih in zelo netočnih informacij v zvezi z zahtevami glede obvladovanja tveganj ali obveznostmi poročanja iz členov 18 in 20;

- (b) trajanje kršitve, vključno z elementom ponavljajočih se kršitev;
 - (c) dejansko povzročeno škodo ali nastale izgube ali morebitno škodo ali izgube, ki bi lahko nastale, če jih je mogoče določiti. Pri ocenjevanju tega vidika se med drugim upoštevajo dejanske ali morebitne finančne ali gospodarske izgube, učinki na druge storitve, število prizadetih ali potencialno prizadetih uporabnikov;
 - (d) ali je kršitev naklepna ali posledica malomarnosti;
 - (e) ukrepe, ki jih je subjekt sprejel za preprečevanje ali ublažitev škode in/ali izgub;
 - (f) upoštevanje odobrenih kodeksov ravnanja ali odobrenih mehanizmov certificiranja;
 - (g) raven sodelovanja fizičnih ali pravnih oseb, ki se štejejo za odgovorne, s pristojnimi organi.
8. Pristojni organi podrobno utemeljijo svoje odločitve o izvrševanju. Pred sprejetjem takih odločitev obvestijo zadevne subjekte o svojih predhodnih ugotovitvah in jim dajo na voljo dovolj časa za predložitev pripomb, **razen v primeru neposredne nevarnosti**.

9. Države članice zagotovijo, da njihovi organi, **pristojni na podlagi te direktive**, obvestijo ustrezne pristojne organe **v tej isti** [...] državi članici [...], imenovane v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov], kadar izvajajo nadzorna in izvršilna pooblastila, namenjena zagotavljanju, da bistveni subjekt, ki je v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov] določen kot kritičen [ali kot subjekt, enakovreden kritičnemu subjektu], izpolnjuje obveznosti v skladu s to direktivo. [...] Pristojni organi iz Direktive (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov] **lahko** od organov, **pristojnih na podlagi te direktive, po potrebi zahtevajo**, da izvajajo nadzorna in izvršilna pooblastila **v zvezi z** bistvenim subjektom, ki je prav tako določen kot kritičen [ali kot subjekt enakovreden kritičnemu subjektu] **v skladu z Direktivo (EU) XXXX/XXXX [direktiva o odpornosti kritičnih subjektov]**.
10. Države članice zagotovijo, da njihovi organi, pristojni na podlagi te direktive, obvestijo nadzorniški forum v skladu s členom 29(1) Uredbe (EU) XXXX/XXXX [uredba o digitalni operativni odpornosti v finančnem sektorju], kadar izvajajo svoja nadzorna in izvršilna pooblastila, katerih cilj je zagotoviti, da bistveni subjekt, ki je v skladu s členom 28 Uredbe (EU) XXXX/XXXX [uredba o digitalni operativni odpornosti v finančnem sektorju] imenovan za ključnega tretjega ponudnika storitev IKT, izpolnjuje obveznosti iz te direktive.
- 10a. Države članice zagotovijo, da njihovi organi, pristojni na podlagi te direktive, obvestijo ustrezne pristojne organe, imenovane v skladu z Uredbo (EU) št. 910/2014, kadar izvajajo svoja nadzorna in izvršilna pooblastila, katerih cilj je zagotoviti, da subjekt, imenovan za ponudnika storitev zaupanja v skladu z Uredbo (EU) št. 910/2014, izpolnjuje obveznosti iz te direktive.

Nadzor in izvrševanje pri pomembnih subjektih

1. Če obstajajo dokazi ali znaki **ali informacije**, da **naj** pomembni subjekt ne bi izpolnjeval obveznosti, določenih v tej direktivi, zlasti v členih 18 in 20, države članice zagotovijo, da pristojni organi ukrepajo, po potrebi z naknadnimi nadzornimi ukrepi.
2. Države članice zagotovijo, da pristojni organi pri izvajanju svojih nadzornih nalog v zvezi s pomembnimi subjekti **uporabljajo pristop, ki temelji na tveganju, in da so** pooblaščen, da v zvezi s temi subjekti **sprejmejo vsaj naslednje ukrepe**:
 - (a) inšpekcijske preglede na kraju samem in naknadni nadzor na daljavo;
 - (b) ciljno usmerjene varnostne presoje, ki temeljijo na ocenah tveganja ali razpoložljivih informacijah o tveganju;
 - (c) varnostne preglede, ki temeljijo na objektivnih, **nediskriminatornih**, poštenih in preglednih merilih za oceno tveganja, **v sodelovanju z zadevnim subjektom, kadar je to potrebno iz tehničnih razlogov**;
 - (d) zahtevajo kakršne koli informacije, potrebne za naknadno oceno ukrepov za kibernetско varnost [...];
 - (e) zahtevajo dostop do podatkov, dokumentov in/ali informacij, potrebnih za opravljanje nadzornih nalog;
 - (ea) **zahtevajo dokaze o izvajanju politik na področju kibernetске varnosti, kot so rezultati varnostnih presoj, ki jih izvede usposobljen presojevalec, in ustrezni temeljni dokazi.**

- 2a. **Pristojni organi lahko za opravljanje svojih nadzornih nalog iz odstavka 2 tega člena izdelajo metodologijo za nadzor, ki omogoča prednostno razvrščanje takšnih nalog na podlagi pristopa, ki temelji na tveganju.**
3. Pristojni organi pri izvajanju svojih pooblastil iz točk (d) **do (ea)** odstavka 2 navedejo namen zahteve in opredelijo zahtevane informacije.
4. Države članice zagotovijo, da so pristojni organi pri izvajanju svojih izvršilnih pooblastil v zvezi s pomembnimi subjekti pooblaščen **vsaj**, da:
- (a) izdajo opozorila o subjektovem neizpolnjevanju obveznosti, določenih v tej direktivi;
 - (b) izdajo zavezujoča navodila ali odredbo, s katero od takih subjektov zahtevajo, da odpravijo ugotovljene pomanjkljivosti ali kršitev obveznosti, določenih v tej direktivi;
 - (c) takim subjektom odredijo, naj prenehajo z ravnanjem, ki ni skladno z obveznostmi, določenimi v tej direktivi, in naj tega ravnanja ne ponovijo več;
 - (d) takim subjektom odredijo, naj na določen način in v določenem roku uskladijo svoje ukrepe za obvladovanje tveganj ali obveznosti poročanja z obveznostmi iz členov 18 in 20;
 - (e) takim subjektom odredijo, naj obvestijo fizične ali pravne osebe, za katere opravljajo storitve ali dejavnosti, na katere bi lahko vplivala pomembna kibernetična grožnja, o **naravi grožnje, pa tudi o** vseh mogočih zaščitnih ali popravnih ukrepih, ki jih lahko take fizične ali pravne osebe sprejmejo v odziv na zadevno grožnjo;
 - (f) takim subjektom odredijo, naj v razumnem roku izvedejo priporočila, dana na podlagi varnostne presoje;

(g) takim subjektom odredijo, naj na določen način objavijo vidike neizpolnjevanja obveznosti, določenih v tej direktivi, **če takšno javno razkritje nima za posledico škodljive izpostavljenosti zadevnega subjekta;**

(h) [...]

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

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

Člen 31

Splošni pogoji za naložitev upravnih glob bistvenim in pomembnim subjektom

1. Države članice zagotovijo, da je naložitev upravnih glob bistvenim in pomembnim subjektom v skladu s tem členom v zvezi s kršitvami obveznosti, določenih v tej direktivi, v vsakem posameznem primeru učinkovita, sorazmerna in odvračilna.
2. Glede na okoliščine posameznega primera se upravne globe naložijo poleg ali namesto ukrepov iz točk (a) do (i) člena 29(4), člena 29(5) in točk (a) do (h) člena 30(4).
3. Pri odločanju o naložitvi upravne globe in njeni višini se v vsakem posameznem primeru upoštevajo vsaj elementi, določeni v členu 29(7).

4. Države članice zagotovijo, da se za kršitve obveznosti iz člena 18 ali člena 20 **s strani bistvenih subjektov** v skladu z odstavkoma 2 in 3 tega člena naložijo ustrezno visoke upravne globe v višini najmanj 4[...] 000 000 EUR ali, **v primeru pravne osebe**, 2 % skupnega svetovnega letnega prometa podjetja, ki mu pripada bistveni [...] subjekt, v preteklem proračunskem letu, kateri koli znesek je višji.
- 4a. Države članice zagotovijo, da se za kršitve obveznosti iz člena 18 ali člena 20 **s strani pomembnih subjektov** v skladu z odstavkoma 2 in 3 tega člena naložijo ustrezno visoke upravne globe v višini najmanj 2 000 000 EUR ali, **v primeru pravne osebe**, 1 % skupnega svetovnega letnega prometa podjetja, ki mu pripada pomembni subjekt, v preteklem proračunskem letu, kateri koli znesek je višji.
5. Države članice lahko določijo pooblastila za naložitev periodičnih denarnih kazni, s katerimi se bistveni ali pomembni subjekt prisili, da preneha s kršitvijo v skladu s predhodno odločitvijo pristojnega organa.
6. Brez poseganja v pooblastila pristojnih organov na podlagi členov 29 in 30 lahko vsaka država članica določi pravila o tem, ali in v kolikšni meri se lahko subjektom javne uprave iz člena 4(23) naložijo upravne globe, v skladu z obveznostmi, določenimi v tej direktivi.

- 6a. Kadar pravni sistem države članice ne določa upravnih glob, države članice zagotovijo, da se lahko ta člen uporablja tako, da pristojni organ sproži postopek za naložitev globe, pristojna nacionalna sodišča pa jo izrečejo, pri čemer mora biti zagotovljeno, da so ta pravna sredstva učinkovita in imajo enak učinek, kot ga imajo upravne globe, ki jih naložijo nadzorni organi. V vsakem primeru pa so globe učinkovite, sorazmerne in odvračilne. Te države članice Komisijo uradno obvestijo o določbah svojih predpisov, ki jih sprejmejo na podlagi tega odstavka do [...], brez odlašanja pa tudi o vseh nadaljnjih spremembah teh predpisov ali spremembah, ki vplivajo nanje.

Člen 32

Kršitve, ki pomenijo kršitev varstva osebnih podatkov

1. Če so pristojni organi **med nadzorom ali izvrševanjem izvedeli** [...], da bi **lahko** kršitev obveznosti iz členov 18 in 20 **te direktive** s strani bistvenega ali pomembnega subjekta **pomenila** kršitev varstva osebnih podatkov, kot je opredeljena v členu 4(12) Uredbe (EU) 2016/679 in ki se uradno sporoči v skladu s členom 33 navedene uredbe, o tem **brez nepotrebne odlašanja** [...] obvestijo nadzorne organe, ki so pristojni v skladu s členoma 55 in 56 navedene uredbe.
2. Če se nadzorni organi, pristojni v skladu s členoma 55 in 56 Uredbe (EU) 2016/679, odločijo, da bodo izvajali svoja pooblastila v skladu s členom 58(2)(i) navedene uredbe, in naložijo upravno globo, pristojni organi **iz člena 8 te direktive** ne naložijo upravne globe za [...] kršitev, **ki jo predstavlja isto ravnanje**, po členu 31 te direktive. Vendar lahko pristojni organi uporabijo izvršilne ukrepe ali izvajajo pooblastila za naložitev sankcij iz točk (a) do (i) člena 29(4), člena 29(5) in točk (a) do (h) člena 30(4) te direktive.

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

Člen 33

Kazni

1. Države članice določijo pravila o kaznih, ki se uporabljajo za kršitve nacionalnih določb, sprejetih v skladu s to direktivo, in sprejmejo vse potrebne ukrepe za zagotovitev njihovega izvajanja. Te kazni so učinkovite, sorazmerne in odvračilne.
2. Države članice do [dve leti po začetku veljavnosti te direktive] Komisijo uradno obvestijo o navedenih pravilih in ukrepih ter ji brez nepotrebnega odlašanja uradno sporočijo vse poznejše spremembe, ki vplivajo nanje.

Člen 34

Medsebojna pomoč

1. Če bistveni ali pomembni subjekt opravlja storitve v več kot eni državi članici ali [...] **opravlja storitve v eni ali več državah članicah**, omrežja 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 pomoč **ki je sorazmerna z viri, ki jih ima na voljo**, da se lahko nadzorni ali izvršilni ukrepi [...] izvajajo učinkovito, uspešno in dosledno. Taka medsebojna pomoč lahko zajema zahtevke za informacije in nadzorne ukrepe, vključno z zahtevki za izvajanje inšpekcijskih pregledov na kraju samem ali nadzora na daljavo ali ciljno usmerjenih varnostnih presoj. Pristojni organ, na katerega je naslovljen zahtevke za pomoč, takega zahtevka ne sme zavrnil, razen če se po izmenjavi informacij z drugimi zadevnimi organi[...] ugotovi, da [...] organ ni pristojen za zagotavljanje zahtevane pomoči, **nima potrebnih virov** ali zahtevana pomoč ni sorazmerna z nadzornimi nalogami pristojnega organa, ki se izvajajo [...], **ali zahtevke zadeva informacije ali vključuje dejavnosti, ki so v nasprotju z nacionalno varnostjo, javno varnostjo ali obrambo te države članice.**

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

POGLAVJE VII

Prehodne in končne določbe

Člen 35

Pregled

Komisija redno pregleduje delovanje te direktive ter poroča Evropskemu parlamentu in Svetu. V poročilu oceni zlasti pomen sektorjev, podsektorjev, velikosti in vrste subjektov iz prilog I in II za delovanje gospodarstva in družbe v zvezi s kibernetско varnostjo. Za namene **pregleda** [...] Komisija upošteva poročila [...] mreže skupin CSIRT o izkušnjah, pridobljenih na [...] operativni ravni. Prvo poročilo se predloži do ... [54 mesecev po datumu začetka veljavnosti te direktive].

Člen 36

[...]

[...]

[...]

Člen 37

Postopek v odboru

1. Komisiji pomaga odbor. Ta odbor je odbor v smislu Uredbe (EU) št. 182/2011.
2. Pri sklicevanju na ta odstavek se uporablja člen 5 Uredbe (EU) št. 182/2011.
3. Kadar je treba pridobiti mnenje odbora na podlagi pisnega postopka, se ta postopek zaključi brez izida, ko v roku za izdajo mnenja tako odloči predsednik odbora ali to zahteva član odbora.

Člen 38

Prenos

1. Države članice [...] do ... [**24** mesecev od datuma začetka veljavnosti te direktive] sprejmejo in objavijo zakone in druge predpise, potrebne za uskladitev s to direktivo[...]. O tem nemudoma obvestijo Komisijo. Države članice začnejo te predpise uporabljati ... [dan po datumu iz prvega pododstavka].
2. Države članice se v sprejetih predpisih sklicujejo na to direktivo ali pa sklic nanjo navedejo ob njihovi uradni objavi. Način sklicevanja določijo države članice.

Člen 39

Sprememba Uredbe (EU) št. 910/2014

V Uredbi (EU) št. 910/2014 se člen 19 črta z učinkom od ... [datum roka za prenos te direktive].

Člen 40

Sprememba Direktive (EU) 2018/1972

V Direktivi (EU) 2018/1972 se člena 40 in 41 črtata z učinkom od ... [datum roka za prenos te direktive].

Člen 41

Razveljavitev

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

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

Člen 42

Začetek veljavnosti

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

Člen 43

Naslovniki

Ta direktiva je naslovljena na države članice.

V Bruslju,

Za Evropski parlament

Predsednik

Za Svet

Predsednik

PRILOGA I

SEKTORJI, PODSEKTORJI IN VRSTE SUBJEKTOV

Sektor	Podsektor	Vrsta subjekta
1. Energija	(a) elektrika	— elektroenergetska podjetja iz točke 57 člena 2 Direktive (EU) 2019/944, ki opravljajo dejavnost „dobave“ iz točke 12 člena 2 navedene direktive ⁽³⁹⁾
		— operaterji distribucijskega sistema iz točke 29 člena 2 Direktive (EU) 2019/944
		— operaterji prenosnega sistema iz točke 35 člena 2 Direktive (EU) 2019/944
		— proizvajalci iz točke 38 člena 2 Direktive (EU) 2019/944
		— imenovani operaterji trga električne energije iz točke 8 člena 2 Uredbe (EU) 2019/943 ⁽⁴⁰⁾
		— udeleženci na trgu električne energije iz točke 25 člena 2 Uredbe (EU) 2019/943, ki opravljajo storitve agregiranja, prilagajanja odjema ali shranjevanja energije iz točk 18, 20 in 59 člena 2 Direktive (EU) 2019/944
	(b) daljinsko ogrevanje in	— daljinsko ogrevanje ali daljinsko

³⁹ 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).

⁴⁰ Uredba (EU) 2019/943 Evropskega parlamenta in Sveta o notranjem trgu električne energije (UL L 158, 14.6.2019, str. 54).

	hlajenje	hlajenje iz točke 19 člena 2 Direktive (EU) 2018/2001 ⁽⁴¹⁾ o spodbujanju uporabe energije iz obnovljivih virov
	(c) nafta	— upravljavci naftovodov
		— upravljavci obratov za proizvodnjo, rafiniranje in predelavo nafte ter upravljavci skladišč in transporta nafte
		— osrednji organi za vzdrževanje zalog nafte iz točke (f) člena 2 Direktive Sveta 2009/119/ES ⁽⁴²⁾
	(d) plin	— dobavitelji iz točke 8 člena 2 Direktive 2009/73/ES ⁽⁴³⁾
		— operaterji distribucijskega sistema iz točke 6 člena 2 Direktive 2009/73/ES
		— operaterji prenosnega sistema iz točke 4 člena 2 Direktive 2009/73/ES
		— operaterji skladiščnega sistema iz točke 10 člena 2 Direktive 2009/73/ES
		— operaterji sistema za UZP iz točke 12 člena 2 Direktive 2009/73/ES

⁴¹ 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).

⁴² 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).

⁴³ 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).

		— podjetja plinskega gospodarstva, kot so opredeljena v točki 1 člena 2 Direktive 2009/73/ES
		— upravljavci obratov za rafiniranje in predelavo zemeljskega plina
	(e) vodik	upravljavci proizvodnje, shranjevanja in prenosa vodika
2. Promet	(a) zračni	— letalski prevozniki iz točke 4 člena 3 Uredbe (ES) št. 300/2008 ⁽⁴⁴⁾ , ki se uporabljajo v komercialne namene
		— upravni organi letališča iz točke 2 člena 2 Direktive 2009/12/ES ⁽⁴⁵⁾ , letališča iz točke 1 člena 2 navedene direktive, vključno z jedrnimi letališči, navedenimi v oddelku 2 Priloge II k Uredbi (EU) št. 1315/2013 ⁽⁴⁶⁾ , ter subjekti, ki upravljajo pomožne objekte, naprave in sredstva na letališčih
		— kontrolorji upravljanja prometa, ki zagotavljajo službe za kontrolo zračnega prometa (ATC) iz točke 1 člena 2 Uredbe (ES) št. 549/2004 ⁽⁴⁷⁾

⁴⁴ 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).

⁴⁵ Direktiva 2009/12/ES Evropskega parlamenta in Sveta z dne 11. marca 2009 o letaliških pristojbinah (UL L 70, 14.3.2009, str. 11).

⁴⁶ 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).

⁴⁷ 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).

	(b) železniški	— upravljavci infrastrukture iz točke 2 člena 3 Direktive 2012/34/EU ⁽⁴⁸⁾
		— prevozniki v železniškem prometu iz točke 1 člena 3 Direktive 2012/34/EU, vključno z upravljavci objektov za izvajanje železniških storitev iz točke 12 člena 3 Direktive 2012/34/EU
	(c) vodni	— prevozna podjetja za potniški in tovorni promet po kopenskih vodah, morju in obalnih vodah, navedena za področje pomorskega prometa v Prilogi I k Uredbi (ES) št. 725/2004 ⁽⁴⁹⁾ , brez posameznih plovil, ki jih upravljajo ta podjetja
		— upravni organi pristanišč iz točke 1 člena 3 Direktive 2005/65/ES ⁽⁵⁰⁾ , vključno z njihovimi pristaniškimi zmogljivostmi iz točke 11 člena 2 Uredbe (ES) št. 725/2004, ter subjekti, ki izvajajo dela in upravljajo opremo v pristaniščih
		— upravljavci sistemov za nadzor plovbe iz točke (o) člena 3 Direktive 2002/59/ES ⁽⁵¹⁾
	(d) cestni	— cestni organi iz točke 12 člena 2 Delegirane uredbe Komisije (EU) 2015/962 ⁽⁵²⁾ , odgovorni za nadzor

⁴⁸ 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).

⁴⁹ 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).

⁵⁰ 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).

⁵¹ 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).

⁵² 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

		upravljanja prometa, razen javnih subjektov, za katere je upravljanje prometa ali upravljanje inteligentnih prometnih sistemov le nebistven del splošne dejavnosti
		— upravljavci inteligentnih prometnih sistemov iz točke 1 člena 4 Direktive 2010/40/EU ⁽⁵³⁾
3. Bančništvo		— kreditne institucije iz točke 1 člena 4 Uredbe (EU) št. 575/2013 ⁽⁵⁴⁾ , [razen tistih iz točke 8 člena 2(5) Direktive 2013/36/EU, ki so izvzete v skladu s členom 2(4) Uredbe XX [uredba o digitalni operativni odpornosti v finančnem sektorju]]

zagotavljanja prometnih informacij v realnem času po vsej EU (UL L 157, 23.6.2015, str. 21).

⁵³ 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).

⁵⁴ Uredba (EU) št. 575/2013 Evropskega parlamenta in Sveta z dne 26. junija 2013 o bonitetnih zahtevah za kreditne institucije in investicijska podjetja ter o spremembi Uredbe (EU) št. 648/2012 (UL L 176, 27.6.2013, str. 1).

4. Infrastruktura finančnega trga		— upravljavci mest trgovanja iz točke 24 člena 4 Direktive 2014/65/EU ⁽⁵⁵⁾
		— centralne nasprotne stranke (CNS) iz točke 1 člena 2 Uredbe (EU) št. 648/2012 ⁽⁵⁶⁾
5. Zdravje		— izvajalci zdravstvenega varstva iz točke (g) člena 3 Direktive 2011/24/EU ⁽⁵⁷⁾
		— referenčni laboratoriji EU iz člena 15 Uredbe XXXX/XXXX o resnih čezmejnih grožnjah za zdravje ⁽⁵⁸⁾
		— subjekti, ki izvajajo raziskovalne in razvojne dejavnosti na področju zdravil iz točke 2 člena 1 Direktive 2001/83/ES ⁽⁵⁹⁾ — 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

⁵⁵ 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).

⁵⁶ 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).

⁵⁷ 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).

⁵⁸ [Uredba Evropskega parlamenta in Sveta o resnih čezmejnih grožnjah za zdravje in o razveljavitvi Sklepa št. 1082/2013/EU, sklic se posodobi po sprejetju predloga COM(2020) 727 final.]

⁵⁹ 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).

		javnem zdravju“) iz člena 20 Uredbe XXXX ⁽⁶⁰⁾
6. Pitna voda		dobavitelji in distributerji vode, namenjene za prehrano ljudi, iz točke 1(a) člena 2 Direktive Sveta 98/83/ES ⁽⁶¹⁾ , vendar brez 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 in tehnološko odpadno vodo iz točk 1 do 3 člena 2 Direktive Sveta 91/271/EGS ⁽⁶²⁾ , vendar brez podjetij, za katere je zbiranje, odvajanje ali čiščenje komunalne odpadne vode, odpadne vode iz gospodinjstev in tehnološke odpadne vode le nebistven del splošne dejavnosti [...]
8. Digitalna infrastruktura		— ponudniki stičišča omrežij
		— ponudniki storitev domenskih imen, razen upravljavcev korenskih imenskih strežnikov
		— registri vrhnjih domenskih imen
		— ponudniki storitev računalništva v oblaku

⁶⁰ [Uredba Evropskega parlamenta in Sveta o okrepljeni vlogi Evropske agencije za zdravila pri pripravljenosti na krize in kriznem upravljanju na področju zdravil in medicinskih pripomočkov, sklic se posodobi po sprejetju predloga COM(2020) 725 final.]

⁶¹ Direktiva Sveta 98/83/ES z dne 3. novembra 1998 o kakovosti vode, namenjene za prehrano ljudi (UL L 330, 5.12.1998, str. 32).

⁶² Direktiva Sveta 91/271/EGS z dne 21. maja 1991 o čiščenju komunalne odpadne vode (UL L 135, 30.5.1991, str. 40).

		— ponudniki storitev podatkovnih centrov
		— ponudniki omrežij za dostavo vsebin
		— ponudniki storitev zaupanja iz točke 19 člena 3 Uredbe (EU) št. 910/2014 ⁽⁶³⁾
		— ponudniki javnih elektronskih komunikacijskih omrežij iz točke 8 člena 2 Direktive (EU) 2018/1972 ⁽⁶⁴⁾ ali ponudniki elektronskih komunikacijskih storitev iz točke 4 člena 2 Direktive (EU) 2018/1972, če so njihove storitve javno dostopne
8.a Upravljanje storitev IKT (med podjetji)		— ponudniki upravljanih storitev — ponudniki upravljanih varnostnih storitev

⁶³ 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).

⁶⁴ 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).

9. Subjekti javne uprave		— subjekti javne uprave enot centralne ravni države, kot jih opredeli država članica v skladu z nacionalnim pravom — [...] ⁶⁵[...] — [...]
10. Vesolje		— upravljavci talne infrastrukture, ki jo imajo v lastijo, vodijo in upravljajo države članice ali zasebne stranke, ki podpirajo opravljanje vesoljskih storitev, brez ponudnikov javnih elektronskih komunikacijskih omrežij iz točke 8 člena 2 Direktive (EU) 2018/1972

⁶⁵ [...]

PRILOGA II

SEKTORJI, PODSEKTORJI IN VRSTE SUBJEKTOV

Sektor	Podsektor	Vrsta subjekta
1. Poštne in kurirske storitve		izvajalci poštnih storitev iz točke 1 [...] člena 2 Direktive 97/67/ES ⁽⁶⁶⁾ , vključno z [...] izvajalci kurirskih storitev
2. Ravnanje z odpadki		podjetja, ki izvajajo postopke ravnanja z odpadki iz točke 9 člena 3 Direktive 2008/98/ES ⁽⁶⁷⁾ , vendar brez podjetij, pri katerih ravnanje z odpadki ni glavna gospodarska dejavnost

⁶⁶ 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), **kakor je bila spremenjena z Direktivo 2008/6/ES Evropskega parlamenta in Sveta z dne 20. februarja 2008 o spremembi Direktive 97/67/ES glede popolnega oblikovanja notranjega trga poštnih storitev v Skupnosti (UL L 52, 27.2.2008, str. 3).**

⁶⁷ 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).

3. Izdelava, proizvodnja in distribucija kemikalij		podjetja, ki izdelujejo [...] in distribuirajo snovi in [...] zmesi , iz točk [...] 9 in 14 člena 3 Uredbe (ES) št. 1907/2006 ⁽⁶⁸⁾ in podjetja, ki izdelujejo izdelke iz točke 3 člena 3 te uredbe iz snovi ali zmesi
4. Pridelava, predelava in distribucija živil		živilske dejavnosti iz točke 2 člena 3 Uredbe (ES) št. 178/2002 ⁽⁶⁹⁾ , ki se ukvarjajo z distribucijo na debelo ter industrijsko pridelavo in predelavo
5. Proizvodnja	(a) proizvodnja medicinskih pripomočkov ter in vitro diagnostičnih medicinskih pripomočkov	subjekti, ki proizvajajo medicinske pripomočke iz člena 2, točka 1, Uredbe (EU) 2017/745 ⁽⁷⁰⁾ , in subjekti, ki proizvajajo in vitro diagnostične medicinske pripomočke iz člena 2, točka 2, Uredbe (EU) 2017/746 ⁽⁷¹⁾ , razen subjektov, ki proizvajajo medicinske pripomočke iz Priloge I, točka 5.
	(b) proizvodnja	podjetja, ki opravljajo katero koli

⁶⁸ 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 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).

⁶⁹ 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).

⁷⁰ 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).

⁷¹ 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).

	računalnikov, elektronskih in optičnih izdelkov	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
6. Digitalni ponudniki		— ponudniki spletnih tržnic
		— ponudniki spletnih iskalnikov
		— ponudniki platforme za storitve družbenega mreženja
