►B

DIREKTIVA (EU) 2022/2555 EVROPSKEGA PARLAMENTA IN SVETA

z dne 14. decembra 2022

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

(Besedilo velja za EGP)

(UL L 333, 27.12.2022, str. 80)

popravljena z:

►C1 Popravek, UL L 239, 28.9.2023, str. 48 (2022/2555)

►C2 Popravek, UL L 90349, 12.6.2024, str. 1 (2022/2555)

▼B

DIREKTIVA (EU) 2022/2555 EVROPSKEGA PARLAMENTA IN SVETA

z dne 14. decembra 2022

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

(Besedilo velja za EGP)

POGLAVJE I

SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja

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

2. V ta namen ta direktiva določa:

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

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

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

(d) obveznosti nadzora in izvrševanja za države članice.

Člen 2

Področje uporabe

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

▼B

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

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

(a) storitve opravljajo:

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

(ii) ponudniki storitev zaupanja;

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

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

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

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

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

(f) gre za subjekt javne uprave:

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

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

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

▼B

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

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

(a) subjekte javne uprave na lokalni ravni;

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

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

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

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

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

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

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

12. Ta direktiva se uporablja brez poseganja v Uredbo (EU) 2016/679, Direktivo 2002/58/ES, direktivi 2011/93/EU ([1]) in 2013/40/EU ([2]) Evropskega parlamenta in Sveta ter Direktivo (EU) 2022/2557.

([1]) 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).

([2]) 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).

▼B

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

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

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

Člen 3

Bistveni in pomembni subjekti

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

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

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

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

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

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

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

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

▼B

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

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

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

(a) ime subjekta;

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

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

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

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

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

Države članice lahko vzpostavijo nacionalne mehanizme za samoregistracijo subjektov.

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

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

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

▼B

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

Člen 4

Sektorski pravni akti Unije

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

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

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

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

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

Člen 5

Minimalna harmonizacija

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

Člen 6

Opredelitev pojmov

V tej direktivi se uporabljajo naslednje opredelitve pojmov:

▼B

(1) „omrežni in informacijski sistem“ pomeni:

(a) elektronsko komunikacijsko omrežje, kot je opredeljeno v členu 2, točka 1, Direktive (EU) 2018/1972;

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

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

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

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

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

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

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

▼C1

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

▼B

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

▼B

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

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

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

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

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

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

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

(16) „standard“ pomeni standard, kot je opredeljen v členu 2, točka 1, Uredbe (EU) št. 1025/2012 Evropskega parlamenta in Sveta ([3]);

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

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

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

([3]) 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).

▼B

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

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

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

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

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

(23) „digitalna storitev“ pomeni storitev, kot je opredeljena v členu 1 (1), točka (b), Direktive (EU) 2015/1535 Evropskega parlamenta in Sveta ([4]);

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

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

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

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

(28) „spletna tržnica“ pomeni spletno tržnico, kot je opredeljena v členu 2, točka (n), Direktive 2005/29/ES Evropskega parlamenta in Sveta ([5]);

(29) „spletni iskalnik“ pomeni spletni iskalnik, kot je opredeljen v členu 2, točka 5, Uredbe (EU) 2019/1150 Evropskega parlamenta in Sveta ([6]);

([4]) 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).

([5]) 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).

([6]) 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).

▼B

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

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

POGLAVJE II

USKLAJENI OKVIRI ZA KIBERNETSKO VARNOST

Člen 7

Nacionalna strategija za kibernetsko varnost

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

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

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

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

▼B

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

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

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

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

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

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

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

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

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

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

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

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

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

▼B

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

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

(j) spodbujanja aktivne kibernetske zaščite.

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

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

Člen 8

Pristojni organi in enotne kontaktne točke

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

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

3. Vsaka država članica določi ali vzpostavi enotno kontaktno točko. Kadar država članica na podlagi odstavka 1 imenuje ali ustanovi le en pristojni organ, je ta organ tudi enotna kontaktna točka te države članice.

4. Vsaka enotna kontaktna točka ima povezovalno vlogo in tako zagotavlja čezmejno sodelovanje organov države članice z ustreznimi organi drugih držav članic in, kadar je to ustrezno, Komisijo in ENISA ter medsektorsko sodelovanje z drugimi pristojnimi nacionalnimi organi v svoji državi članici.

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

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

▼B

Člen 9

Nacionalni okviri za obvladovanje kibernetskih kriz

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

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

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

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

(a) cilji nacionalnih ukrepov in dejavnosti za pripravljenost;

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

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

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

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

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

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

▼B

Člen 10

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

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

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

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

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

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

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

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

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

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

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

▼B

Člen 11

Zahteve, tehnične zmogljivosti in naloge skupin CSIRT

1. Skupine CSIRT izpolnjujejo naslednje zahteve:

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

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

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

(d) skupine CSIRT zagotovijo zaupnost in zanesljivost svojih dejavnosti;

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

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

Skupine CSIRT lahko sodelujejo v mrežah za mednarodno sodelovanje.

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

3. Skupine CSIRT imajo naslednje naloge:

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

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

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

▼B

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

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

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

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

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

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

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

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

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

(a) postopki obvladovanja incidentov;

(b) obvladovanjem kriz ter

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

Člen 12

Usklajeno razkrivanje ranljivosti in evropska podatkovna zbirka ranljivosti

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

▼B

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

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

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

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

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

(a) informacije, ki opisujejo ranljivost;

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

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

Člen 13

Sodelovanje na nacionalni ravni

1. Kadar so pristojni organi, enotna kontaktna točka in skupine CSIRT iste države članice ločeni subjekti, med seboj sodelujejo pri izpolnjevanju obveznosti, ki jih določa ta direktiva.

▼B

2. Države članice zagotovijo, da njihove skupine CSIRT ali po potrebi njihovi pristojni organi prejmejo priglasitve pomembnih incidentov v skladu s členom 23 in incidentov, kibernetskih groženj in skorajšnjih incidentov v skladu s členom 30.

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

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

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

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

POGLAVJE III

SODELOVANJE NA RAVNI UNIJE IN MEDNARODNI RAVNI

Člen 14

Skupina za sodelovanje

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

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

▼B

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

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

Komisija zagotovi sekretariat.

4. Skupina za sodelovanje ima naslednje naloge:

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

Člen 15

Mreža skupin CSIRT

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

2. Mrežo skupin CSIRT sestavljajo predstavniki skupin CSIRT, ki so imenovani ali določeni na podlagi člena 10, in skupina za odzivanje na računalniške grožnje za evropske institucije, organe in agencije Unije (CERT-EU). Komisija sodeluje v mreži skupin CSIRT kot opazovalka. ENISA zagotovi sekretariat in dejavno podpira sodelovanje med skupinami CSIRT.

3. Mreža skupin CSIRT ima naslednje naloge:

(a) izmenjava informacij o zmogljivostih skupin CSIRT;

(b) omogočanje souporabe, prenosa in izmenjave tehnologije ter ustreznih ukrepov, politik, orodij, postopkov, primerov dobre prakse in okvirov med skupinami CSIRT;

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

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

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

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

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

▼B

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

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

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

(i) kategorij kibernetskih groženj in incidentov;

(ii) zgodnjega opozarjanja;

(iii) medsebojne pomoči;

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

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

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

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

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

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

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

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

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

5. Mreža skupin CSIRT sprejme svoj poslovnik.

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

▼B

Člen 16

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

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

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

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

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

3. Mreža EU-CyCLONe ima naslednje naloge:

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

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

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

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

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

4. Mreža EU-CyCLONe sprejme svoj poslovnik.

5. Mreža EU-CyCLONe redno poroča skupini za sodelovanje o obvladovanju kibernetskih incidentov velikih razsežnosti in kriz, pa tudi o trendih, pri čemer se osredotoča zlasti na njihov vpliv na bistvene in pomembne subjekte.

▼B

6. Mreža EU-CyCLONe sodeluje z mrežo skupin CSIRT na podlagi dogovorjenih postopkovnih ureditev iz člena 15(6).

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

Člen 17

Mednarodno sodelovanje

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

Člen 18

Poročilo o stanju kibernetske varnosti v Uniji

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

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

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

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

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

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

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

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

▼B

Člen 19

Medsebojni strokovni pregledi

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

Medsebojni strokovni pregledi vključujejo vsaj eno od naslednjega:

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

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

(c) operativne zmogljivosti skupin CSIRT;

(d) raven izvajanja medsebojne pomoči iz člena 37;

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

(f) posebni čezmejni ali medsektorski vidiki.

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

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

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

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

▼B

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

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

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

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

POGLAVJE IV

OBVEZNOSTI GLEDE UKREPOV ZA OBVLADOVANJE TVEGANJ ZA KIBERNETSKO VARNOST IN POROČANJA

Člen 20

Upravljanje

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

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

▼B

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

Člen 21

Ukrepi za obvladovanje tveganj za kibernetsko varnost

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

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

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

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

(b) obvladovanje incidentov;

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

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

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

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

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

▼B

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

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

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

3. Države članice zagotovijo, da subjekti pri preučevanju ustreznih ukrepov iz odstavka 2, točka (d), tega člena, upoštevajo ranljivosti, ki so specifične za posameznega neposrednega dobavitelja in ponudnika storitev ter splošno kakovost proizvodov ter praks svojih dobaviteljev in ponudnikov storitev na področju kibernetske varnosti, vključno z njihovimi varnimi razvojnimi postopki. Države članice zagotovijo tudi, da morajo subjekti pri ugotavljanju, kateri ukrepi iz navedene točke so ustrezni, upoštevati rezultate usklajenih ocen tveganja za kritične dobavne verige, izvedenih v skladu s členom 22(1).

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

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

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

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

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

Člen 22

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

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

▼B

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

Člen 23

Obveznosti poročanja

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

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

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

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

3. Incident se šteje za pomemben, če:

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

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

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

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

▼B

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

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

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

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

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

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

(iv) po potrebi čezmejni vpliv incidenta;

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

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

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

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

▼B

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

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

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

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

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

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

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

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

▼B

Člen 24

Uporaba evropskih certifikacijskih shem za kibernetsko varnost

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

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

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

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

Člen 25

Standardizacija

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

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

POGLAVJE V

PRISTOJNOST IN REGISTRACIJA

Člen 26

Pristojnost in teritorialnost

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

▼B

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

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

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

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

3. Če subjekt iz odstavka 1, točka (b), nima sedeža v Uniji, vendar v njej opravlja storitve, določi predstavnika v Uniji. Predstavnik ima sedež v eni od držav članic, v katerih se opravljajo storitve. Za tak subjekt se šteje, da je pod pristojnostjo države članice, v kateri ima predstavnik sedež. Če ni imenovanega predstavnika v Uniji v skladu s tem odstavkom, lahko katera koli država članica, v kateri subjekt opravlja storitve, uvede sodne postopke proti subjektu zaradi kršitve te direktive.

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

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

Člen 27

Register subjektov

1. ENISA vzpostavi in vzdržuje register ponudnikov storitev DNS, registrov TLD imen, subjektov, ki opravljajo storitve registracije domenskih imen, ponudnikov storitev računalništva v oblaku, ponudnikov storitev podatkovnih centrov, ponudnikov omrežij za dostavo vsebine, ponudnikov upravljanih storitev, ponudnikov upravljanih varnostnih storitev, kot tudi ponudnikov spletnih tržnic, spletnih brskalnikov in

▼B

platform za storitve družbenega mreženja na podlagi informacij, prejetih od enotnih kontaktnih točk v skladu z odstavkom 4. ENISA na zahtevo ustreznim pristojnim organom omogoči dostop do navedenega registra, pri čemer zagotovi, da je zaupnosti informacij zaščitena kadar je potrebno.

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

(a) ime subjekta;

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

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

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

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

(f) bloke naslovov IP subjekta.

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

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

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

Člen 28

Podatkovna zbirka o registraciji *domenskih imen*

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

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

▼B

(a) domensko ime;

(b) datum registracije;

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

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

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

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

5. Države članice zahtevajo, da registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen, omogočajo dostop do podatkov o registraciji posameznih domenskih imen na podlagi zakonitih in ustrezno utemeljenih zahtevkov oseb, ki imajo upravičen razlog za dostop, v skladu s pravom Unije o varstvu podatkov. Države članice zahtevajo, da registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen, odgovorijo brez nepotrebnega odlašanja, v vsakem primeru pa v 72 urah od prejema kakršnih koli zahtevkov za dostop. Države članice zahtevajo, da so politike in postopki v zvezi z razkritjem teh podatkov javno dostopni.

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

POGLAVJE VI

IZMENJAVA INFORMACIJ

Člen 29

Dogovori o izmenjavi informacij o kibernetski varnosti

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

▼B

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

(b) zvišuje raven kibernetske varnosti, zlasti z ozaveščanjem v zvezi s kibernetskimi grožnjami, omejevanjem ali oviranjem zmožnosti širjenja takih groženj, podpiranjem vrste obrambnih zmogljivosti, odpravljanjem in razkrivanjem ranljivosti, tehnikami odkrivanja, omejevanja in preprečevanja groženj, strategijami za zmanjšanje tveganja ali fazami odzivanja in okrevanja ali spodbujanjem sodelovanja med javnimi in zasebnimi subjekti pri raziskovanju kibernetskih groženj.

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

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

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

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

Člen 30

Prostovoljna priglasitev ustreznih informacij

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

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

▼B

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

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

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

POGLAVJE VII

NADZOR IN IZVRŠEVANJE

Člen 31

Splošni vidiki, povezani z nadzorom in izvrševanjem

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

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

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

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

▼B

Člen 32

Nadzorni in izvršilni ukrepi v zvezi z bistvenimi subjekti

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

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

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

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

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

   (i) ponavljajoče se kršitve;

   (ii) nepriglasitev ali neodprava pomembnih incidentov;

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

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

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

(b) trajanje kršitve;

(c) vse relevantne predhodne kršitve zadevnega subjekta;

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

▼B

(e) morebitno naklepnost ali malomarnost storilca kršitve;

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

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

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

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

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

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

Člen 33

Nadzorni in izvršilni ukrepi v zvezi s pomembnimi subjekti

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

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

▼B

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

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

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

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

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

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

Člen 34

Splošni pogoji za naložitev upravnih glob bistvenim in pomembnim subjektom

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

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

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

▼C2

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

▼C2

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

▼B

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

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

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

Člen 35

Kršitve, ki pomenijo kršitev varstva osebnih podatkov

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

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

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

▼B

Člen 36

Sankcije

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

Člen 37

Medsebojna pomoč

1. Kadar subjekt storitve opravlja v več kot eni državi članici ali storitve opravlja v eni ali več državah članicah, omrežni in informacijski sistemi pa so v eni ali več drugih državah članicah, pristojni organi zadevnih držav članic po potrebi sodelujejo in si pomagajo. Takšno sodelovanje vključuje vsaj naslednje:

(a) pristojni organi, ki uporabljajo nadzorne ali izvršilne ukrepe v državi članici, prek enotne kontaktne točke obvestijo pristojne organe v drugih zadevnih državah članicah o sprejetih nadzornih in izvršilnih ukrepih;

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

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

Medsebojna pomoč iz prvega pododstavka, točka (c), lahko zajema zahtevke za informacije in nadzorne ukrepe, vključno z zahtevki za izvajanje inšpekcijskih pregledov na kraju samem ali nadzora na daljavo ali ciljno usmerjenih varnostnih presoj. Pristojni organ, na katerega je naslovljen zahtevek za pomoč, zahtevka ne zavrne, razen če se ugotovi, da organ ni pristojen za zagotavljanje zahtevane pomoči, da zahtevana pomoč ni sorazmerna z nadzornimi nalogami pristojnega organa ali da zahtevek zadeva informacije ali dejavnosti, ki bi bile, če bi bile razkrite ali izvedene, v nasprotju z bistvenimi interesi nacionalne varnosti, javno varnostjo ali obrambo te države članice. Preden pristojni organ zavrne takšen zahtevek, se posvetuje z drugimi zadevnimi pristojnimi organi, na zahtevo katere od zadevnih držav članic pa tudi s Komisijo in ENISA.

▼B

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

POGLAVJE VIII

DELEGIRANI IN IZVEDBENI AKTI

Člen 38

Izvajanje prenosa pooblastila

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

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

3. Prenos pooblastila iz člena 24(2) lahko kadar koli prekliče Evropski parlament ali Svet. S sklepom o preklicu preneha veljati prenos pooblastila iz navedenega sklepa. Sklep začne učinkovati dan po njegovi objavi v *Uradnem listu Evropske unije* ali na poznejši dan, ki je določen v navedenem sklepu. Sklep ne vpliva na veljavnost že veljavnih delegiranih aktov.

4. Komisija se pred sprejetjem delegiranega akta posvetuje s strokovnjaki, ki jih imenujejo države članice, v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje.

5. Komisija takoj po sprejetju delegiranega akta o njem sočasno uradno obvesti Evropski parlament in Svet.

6. Delegirani akt, sprejet na podlagi člena 24(2), začne veljati le, če mu niti Evropski parlament niti Svet ne nasprotuje v roku dveh mesecev od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu ali če pred iztekom tega roka tako Evropski parlament kot Svet obvestita Komisijo, da mu ne bosta nasprotovala. Ta rok se na pobudo Evropskega parlamenta ali Sveta podaljša za dva meseca.

Člen 39

Postopek v odboru

1. Komisiji pomaga odbor. Ta odbor je odbor v smislu Uredbe (EU) št. 182/2011.

▼B

2. Pri sklicevanju na ta odstavek se uporablja člen 5 Uredbe (EU) št. 182/2011.

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

POGLAVJE IX

KONČNE DOLOČBE

Člen 40

Pregled

Komisija do 17. oktobra 2027 in nato vsakih 36 mesecev pregleda delovanje te direktive ter o tem poroča Evropskemu parlamentu in Svetu. V poročilu oceni zlasti pomen velikosti zadevnih subjektov ter sektorjev, podsektorjev in vrst subjektov iz prilog I in II za delovanje gospodarstva in družbe v zvezi s kibernetsko varnostjo. V ta namen in zaradi nadaljnje krepitve strateškega in operativnega sodelovanja Komisija upošteva poročila skupine za sodelovanje in mreže skupin CSIRT o izkušnjah, pridobljenih na strateški in operativni ravni. Poročilu po potrebi priloži zakonodajni predlog.

Člen 41

Prenos

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

Države članice te predpise uporabljajo od 18. oktobra 2024.

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

Člen 42

Sprememba Uredbe (EU) št. 910/2014

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

Člen 43

Sprememba Direktive (EU) 2018/1972

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

▼B

Člen 44

Razveljavitev

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

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

Člen 45

Začetek veljavnosti

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

Člen 46

Naslovniki

Ta direktiva je naslovljena na države članice.

▼B

PRILOGA I

VISOKO KRITIČNI SEKTORJI

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

▼B

Sektor	Podsektor	Vrsta subjekta
		— operaterji sistema za UZP, kot so opredeljeni v členu 2, točka 12, Direktive 2009/73/ES
		— podjetja plinskega gospodarstva, kot so opredeljeni v členu 2, točka 1, Direktive 2009/73/ES
		— upravljavci obratov za rafiniranje in predelavo zemeljskega plina
	(e) vodik	— upravljavci proizvodnje, shranjevanja in prenosa vodika
2. Promet	(a) zračni	— letalski prevozniki, kot so opredeljeni členu 3, točka 4, Uredbe (ES) št. 300/2008, ki se uporabljajo v komercialne namene
		— upravni organi letališča, kot so opredeljeni v členu 2, točka 2, Direktive 2009/12/ES Evropskega parlamenta in Sveta ([6]), letališča, kot so opredeljena v členu 2, točka 1, navedene direktive, vključno z jedrnimi letališči iz oddelka 2 Priloge II k Uredbi (EU) št. 1315/2013 Evropskega parlamenta in Sveta ([7]), ter subjekti, ki upravljajo pomožne objekte, naprave in sredstva na letališčih
		— kontrolorji upravljanja prometa, ki zagotavljajo kontrolo zračnega prometa (ATC), kot je opredeljena v členu 2, točka 1, Uredbe (ES) št. 549/2004 Evropskega parlamenta in Sveta ([8])
	(b) železniški	— upravljavci infrastrukture, kot so opredeljeni v členu 3, točka 2, Direktive 2012/34/EU Evropskega parlamenta in Sveta ([9])
		— prevozniki v železniškem prometu, kot so opredeljeni v členu 3, točka 1, Direktive 2012/34/EU, vključno z upravljavci objektov za izvajanje železniških storitev, kot so opredeljeni v členu 3, točka 12, navedene direktive
	(c) vodni	— prevozna podjetja za potniški in tovorni promet po kopenskih vodah, morju in obalnih vodah, kot so za področje vodnega prometa opredeljena v Prilogi I k Uredbi (ES) št. 725/2004 Evropskega parlamenta in Sveta ([10]), brez posameznih plovil, ki jih upravljajo ta podjetja

▼B

Sektor	Podsektor	Vrsta subjekta
		— upravni organi pristanišč, kot so opredeljena v členu 3, točka 1, Direktive 2005/65/ES Evropskega parlamenta in Sveta ([11]), vključno z njihovimi pristanišči, kot so opredeljena v členu 2, točka 11, Uredbe (ES) št. 725/2004, ter subjekti, ki izvajajo dela in upravljajo opremo v pristaniščih
		— upravljavci sistemov za nadzor plovbe (VTS), kot so opredeljeni v členu 3, točka (o), Direktive 2002/59/ES Evropskega parlamenta in Sveta ([12])
	(d) cestni	— cestni organi, kot so opredeljeni v členu 2, točka 12, Delegirane uredbe Komisije (EU) 2015/962 ([13]), odgovorni za nadzor upravljanja prometa, razen javnih subjektov, za katere je upravljanje prometa ali upravljanje inteligentnih prometnih sistemov le nebistven del splošne dejavnosti
		— upravljavci inteligentnih prometnih sistemov, kot so opredeljeni v členu 4, točka 1, Direktive 2010/40/EU Evropskega parlamenta in Sveta ([14])
3. Bančništvo		kreditne institucije, kot so opredeljene v členu 4, točka 1, Uredbe (EU) št. 575/2013 Evropskega parlamenta in Sveta ([15])
4. Infrastruktura finančnega trga		— upravljavci mest trgovanja, kot so opredeljena v členu 4, točka 24, Direktive 2014/65/EU Evropskega parlamenta in Sveta ([16])
		— centralne nasprotne stranke (CNS), kot so opredeljene v členu 2, točka 1, Uredbe (EU) št. 648/2012 Evropskega parlamenta in Sveta ([17])
5. Zdravje		— izvajalci zdravstvenega varstva, kot so opredeljeni v členu 3, točka (g), Direktive 2011/24/EU Evropskega parlamenta in Sveta ([18])
		— referenčni laboratoriji EU iz člena 15 Uredbe (EU) 2022/2371 Evropskega parlamenta in Sveta ([19])
		— subjekti, ki izvajajo raziskovalne in razvojne dejavnosti na področju zdravil, kot so opredeljena v členu 1, točka 2, Direktive 2001/83/ES Evropskega parlamenta in Sveta ([20]) — subjekti, ki proizvajajo farmacevtske surovine in preparate s področja C oddelka 21 NACE Rev. 2 — subjekti, ki proizvajajo medicinske pripomočke, ki se štejejo za kritične v času izrednih razmer v javnem zdravju (seznam kritičnih pripomočkov v izrednih razmerah v javnem zdravju) v smislu člena 22 Uredbe (EU) 2022/123 Evropskega parlamenta in Sveta ([21])

▼B

Sektor	Podsektor	Vrsta subjekta
6. Pitna voda		dobavitelji in distributerji vode, namenjene za prehrano ljudi, kot je opredeljena v členu 2, točka 1(a), Direktive (EU) 2020/2184 Evropskega parlamenta in Sveta ([22]), razen distributerjev, za katere je distribucija vode za prehrano ljudi le nebistven del splošne dejavnosti distribucije drugih dobrin in blaga
7. Odpadna voda		podjetja, ki zbirajo, odvajajo ali čistijo komunalno odpadno vodo, odpadno vodo iz gospodinjstev ali tehnološko odpadno vodo, kot je opredeljena v členu 2, točke 1, 2 in 3, Direktive Sveta 91/271/EGS ([23]), razen podjetij, za katera je zbiranje, odvajanje ali čiščenje komunalne odpadne vode, odpadne vode iz gospodinjstev ali tehnološke odpadne vode nebistven del splošne dejavnosti
8. Digitalna infrastruktura		— ponudniki stičišča omrežij
		— ponudniki storitev DNS, razen upravljavcev korenskih imenskih strežnikov
		— registri TLD imen
		— ponudniki storitev računalništva v oblaku
		— ponudniki storitev podatkovnih centrov
		— ponudniki omrežij za dostavo vsebin
		— ponudniki storitev zaupanja
		— ponudniki javnih elektronskih komunikacijskih omrežij
		— ponudniki javno dostopnih elektronskih komunikacijskih storitev
9. Upravljanje storitev IKT (med podjetji)		— ponudniki upravljanih storitev — ponudniki upravljanih varnostnih storitev
10. Javna uprava		— subjekti javne uprave enot centralne ravni držav, kot jih opredeli država članica v skladu z nacionalnim pravom
		— subjekti javne uprave enot na regionalni ravni, kot jih opredeli država članica v skladu z nacionalnim pravom

▼B

Sektor	Podsektor	Vrsta subjekta
11. Vesolje		upravljavci talne infrastrukture, ki jo imajo v lasti, vodijo in upravljajo države članice ali zasebne stranke, ki podpirajo opravljanje vesoljskih storitev, brez ponudnikov javnih elektronskih komunikacijskih omrežij

([1]) Direktiva (EU) 2019/944 Evropskega parlamenta in Sveta z dne 5. junija 2019 o skupnih pravilih notranjega trga električne energije in spremembi Direktive 2012/27/EU (UL L 158, 14.6.2019, str. 125).
([2]) Uredba (EU) 2019/943 Evropskega parlamenta in Sveta z dne 5. junija 2019 o notranjem trgu električne energije (UL L 158, 14.6.2019, str. 54).
([3]) Direktiva (EU) 2018/2001 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o spodbujanju uporabe energije iz obnovljivih virov (UL L 328, 21.12.2018, str. 82).
([4]) Direktiva Sveta 2009/119/ES z dne 14. septembra 2009 o obveznosti držav članic glede vzdrževanja minimalnih zalog surove nafte in/ali naftnih derivatov (UL L 265, 9.10.2009, str. 9).
([5]) Direktiva 2009/73/ES Evropskega parlamenta in Sveta z dne 13. julija 2009 o skupnih pravilih notranjega trga z zemeljskim plinom in o razveljavitvi Direktive 2003/55/ES (UL L 211, 14.8.2009, str. 94).
([6]) Direktiva 2009/12/ES Evropskega parlamenta in Sveta z dne 11. marca 2009 o letaliških pristojbinah (UL L 70, 14.3.2009, str. 11).
([7]) Uredba (EU) št. 1315/2013 Evropskega parlamenta in Sveta z dne 11. decembra 2013 o smernicah Unije za razvoj vseevropskega prometnega omrežja in razveljavitvi Sklepa št. 661/2010/EU (UL L 348, 20.12.2013, str. 1).
([8]) Uredba (ES) št. 549/2004 Evropskega parlamenta in Sveta z dne 10. marca 2004 o določitvi okvira za oblikovanje enotnega evropskega neba (okvirna uredba) (UL L 96, 31.3.2004, str. 1).
([9]) Direktiva 2012/34/EU Evropskega parlamenta in Sveta z dne 21. novembra 2012 o vzpostavitvi enotnega evropskega železniškega območja (UL L 343, 14.12.2012, str. 32).
([10]) Uredba (ES) št. 725/2004 Evropskega parlamenta in Sveta z dne 31. marca 2004 o povečanju zaščite na ladjah in v pristaniščih (UL L 129, 29.4.2004, str. 6).
([11]) Direktiva Evropskega parlamenta in Sveta 2005/65/ES z dne 26. oktobra 2005 o krepitvi varnosti v pristaniščih (UL L 310, 25.11.2005, str. 28).
([12]) Direktiva 2002/59/ES Evropskega parlamenta in Sveta z dne 27. junija 2002 o vzpostavitvi sistema spremljanja in obveščanja za ladijski promet ter o razveljavitvi Direktive Sveta 93/75/EGS (UL L 208, 5.8.2002, str. 10).
([13]) Delegirana uredba Komisije (EU) 2015/962 z dne 18. decembra 2014 o dopolnitvi Direktive 2010/40/EU Evropskega parlamenta in Sveta v zvezi z opravljanjem storitev zagotavljanja prometnih informacij v realnem času po vsej EU (UL L 157, 23.6.2015, str. 21).
([14]) Direktiva 2010/40/EU Evropskega parlamenta in Sveta z dne 7. julija 2010 o okviru za uvajanje inteligentnih prometnih sistemov v cestnem prometu in za vmesnike do drugih vrst prevoza (UL L 207, 6.8.2010, str. 1).
([15]) Uredba (EU) št. 575/2013 Evropskega parlamenta in Sveta z dne 26. junija 2013 o bonitetnih zahtevah za kreditne institucije in o spremembi Uredbe (EU) št. 648/2012 (UL L 176, 27.6.2013, str. 1).
([16]) Direktiva 2014/65/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o trgih finančnih instrumentov ter spremembi Direktive 2002/92/ES in Direktive 2011/61/EU (UL L 173, 12.6.2014, str. 349).
([17]) Uredba (EU) št. 648/2012 Evropskega parlamenta in Sveta z dne 4. julija 2012 o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov (UL L 201, 27.7.2012, str. 1).
([18]) Direktiva 2011/24/EU Evropskega parlamenta in Sveta z dne 9. marca 2011 o uveljavljanju pravic pacientov pri čezmejnem zdravstvenem varstvu (UL L 88, 4.4.2011, str. 45).
([19]) Uredba (EU) 2022/2371 Evropskega parlamenta in Sveta z dne 23. novembra 2022 o resnih čezmejnih grožnjah za zdravje in o razveljavitvi Sklepa št. 1082/2013/EU (UL L 314, 6.12.2022, str. 26).
([20]) Direktiva 2001/83/ES Evropskega parlamenta in Sveta z dne 6. novembra 2001 o zakoniku Skupnosti o zdravilih za uporabo v humani medicini (UL L 311, 28.11.2001, str. 67).
([21]) Uredba (EU) 2022/123 Evropskega parlamenta in Sveta z dne 25. januarja 2022 o okrepljeni vlogi Evropske agencije za zdravila pri pripravljenosti na krize in kriznem upravljanju na področju zdravil in medicinskih pripomočkov (UL L 20, 31.1.2022, str. 1).
([22]) Direktiva (EU) 2020/2184 Evropskega parlamenta in Sveta z dne 16. decembra 2020 o kakovosti vode, namenjene za prehrano ljudi (UL L 435, 23.12.2020, str. 1).
([23]) Direktiva Sveta 91/271/EGS z dne 21. maja 1991 o čiščenju komunalne odpadne vode (UL L 135, 30.5.1991, str. 40).

▼B

PRILOGA II

DRUGI KRITIČNI SEKTORJI

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

▼B

Sektor	Podsektor	Vrsta subjekta
	(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 platform za storitve družbenega mreženja
7. Raziskave		raziskovalne organizacije

([1]) Direktiva 2008/98/ES Evropskega parlamenta in Sveta z dne 19. novembra 2008 o odpadkih in razveljavitvi nekaterih direktiv (UL L 312, 22.11.2008, str. 3).
([2]) Uredba (ES) št. 1907/2006 Evropskega parlamenta in Sveta z dne 18. decembra 2006 o registraciji, evalvaciji, avtorizaciji in omejevanju kemikalij (REACH) ter o ustanovitvi Evropske agencije za kemikalije in o spremembi Direktive 1999/45/ES ter o razveljavitvi Uredbe Sveta (EGS) št. 793/93 in Uredbe Komisije (ES) št. 1488/94 ter Direktive Sveta 76/769/EGS in direktiv Komisije 91/155/EGS, 93/67/EGS, 93/105/ES in 2000/21/ES (UL L 396, 30.12.2006, str. 1).
([3]) Uredba (ES) št. 178/2002 Evropskega parlamenta in Sveta z dne 28. januarja 2002 o določitvi splošnih načel in zahtevah živilske zakonodaje, ustanovitvi Evropske agencije za varnost hrane in postopkih, ki zadevajo varnost hrane (UL L 31, 1.2.2002, str. 1).
([4]) Uredba (EU) 2017/745 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o medicinskih pripomočkih, spremembi Direktive 2001/83/ES, Uredbe (ES) št. 178/2002 in Uredbe (ES) št. 1223/2009 ter razveljavitvi direktiv Sveta 90/385/EGS in 93/42/EGS (UL L 117, 5.5.2017, str. 1).
([5]) Uredba (EU) 2017/746 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o *in vitro* diagnostičnih medicinskih pripomočkih ter razveljavitvi Direktive 98/79/ES in Sklepa Komisije 2010/227/EU (UL L 117, 5.5.2017, str. 176).

▼B

PRILOGA III

KORELACIJSKA TABELA

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

▼B

Direktiva (EU) 2016/1148	Ta direktiva
člen 11(4)	člen 14(4), prvi pododstavek, točka (r), in drugi pododstavek
člen 11(5)	člen 14(8)
člen 12(1) do (5)	člen 15(1) do (5)
člen 13	člen 17
člen 14(1) in (2)	člen 21(1) do (4)
člen 14(3)	člen 23(1)
člen 14(4)	člen 23(3)
člen 14(5)	člen 23(5), (6) in (8)
člen 14(6)	člen 23(7)
člen 14(7)	člen 23(11)
člen 15(1)	člen 31(1)
člen 15(2), prvi pododstavek, točka (a)	člen 32(2), točka (e)
člen 15(2), prvi pododstavek, točka (b)	člen 32(2), točka (g)
člen 15(2), drugi pododstavek	člen 32(3)
člen 15(3)	člen 32(4), točka (b)
člen 15(4)	člen 31(3)
člen 16(1) in (2)	člen 21(1) do (4)
člen 16(3)	člen 23(1)
člen 16(4)	člen 23(3)
člen 16(5)	-
člen 16(6)	člen 23(6)
člen 16(7)	člen 23(7)
člen 16(8) in (9)	člen 21(5) in člen 23(11)
člen 16(10)	-
člen 16(11)	člen 2(1), (2) in (3)
člen 17(1)	člen 33(1)
člen 17(2), točka (a)	člen 32(2), točka (e)
člen 17(2), točka (b)	člen 32(4), točka (b)

▼B

Direktiva (EU) 2016/1148	Ta direktiva
člen 17(3)	člen 37(1), točki (a) in (b)
člen 18(1)	člen 26(1), točka (b), in odstavek 2
člen 18(2)	člen 26(3)
člen 18(3)	člen 26(4)
člen 19	člen 25
člen 20	člen 30
člen 21	člen 36
člen 22	člen 39
člen 23	člen 40
člen 24	-
člen 25	člen 41
člen 26	člen 45
člen 27	člen 46
Priloga I, točka 1	člen 11(1)
Priloga I, točke 2(a)(i) do (iv)	člen 11(2), točke (a) do (d)
Priloga I, točka 2(a)(v)	člen 11(2), točka (f)
Priloga I, točka 2(b)	člen 11(4)
Priloga I, točki 2(c)(i) in (ii)	člen 11(5), točka (a)
Priloga II	Priloga I
Priloga III, točki 1 in 2	Priloga II, točka 6
Priloga III, točka 3	Priloga I, točka 8