Vijeće
Europske unije

Bruxelles, 26. studenoga 2021.
(OR. en)

14337/21

Međuinstitucijski predmet:
2020/0359(COD)

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

NAPOMENA

Od:	Glavno tajništvo Vijeća
Za:	Vijeće
Br. preth. dok.:	9583/2/21, 11724/21
Br. dok. Kom.:	14150/20
Predmet:	Prijedlog direktive Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148 *– općí pristup*

I. UVOD

1. Komisija je 16. prosinca 2020. donijela Prijedlog direktive o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije (revidirana Direktiva NIS ili „NIS 2”)[1] u cilju zamjene postojeće Direktive o sigurnosti mrežnih i informacijskih sustava („Direktiva NIS”)[2].

[1] Prijedlog direktive Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148.

[2] Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije.

Taj je prijedlog bio jedno od djelovanja predviđenih Strategijom EU-a za kibersigurnost za digitalno desetljeće[3] kako bi se osiguralo da se građani i poduzeća mogu koristiti pouzdanim digitalnim tehnologijama.

2. Prijedlog se temelji na članku 114. Ugovora o funkcioniranju Europske unije (UFEU) i njime se nastoji dodatno poboljšati otpornost i kapacitete javnih i privatnih subjekata, nadležnih tijela i Unije u cjelini za odgovor na incidente.

3. Odbor nadležan za prijedlog u Europskom parlamentu jest Odbor za industriju, istraživanje i energetiku (ITRE). Odbor ITRE usvojio je izvješće izvjestitelja 28. listopada 2021.

4. Europski gospodarski i socijalni odbor donio je mišljenje 28. travnja 2021.

5. Odbor stalnih predstavnika odlučio je 3. veljače2021. savjetovati se s Europskim odborom regija o tom prijedlogu[4]. Europski odbor regija dosad nije dao mišljenje.

6. Europski nadzornik za zaštitu podataka dao je svoje mišljenje 11. ožujka 2021.[5]

7. U svojim zaključcima[6] od 22. ožujka 2021. o strategiji EU-a za kibersigurnost za digitalno desetljeće Vijeće je primilo na znanje novi prijedlog koji se nadovezuje na Direktivu o sigurnosti mrežnih i informacijskih sustava i ponovno istaknulo svoju potporu jačanju i usklađivanju nacionalnih okvira za kibersigurnost i stalnoj suradnji među državama članicama.

8. U svojim zaključcima od 21. i 22. listopada 2021. Europsko vijeće pozvalo je na nastavak rada na prijedlogu revidirane Direktive NIS.

---

3 14133/20.
4 5573/21.
5 Mišljenje 5/2021 o Strategiji za kibersigurnost i Direktivi NIS 2.0.
6 6722/21.

II. RAD U PRIPREMNIM TIJELIMA VIJEĆA

9. U okviru Vijeća prijedlog je razmatrala Horizontalna radna skupina za kiberpitanja. Razmatranje prijedloga započelo je 19. siječnja tijekom portugalskog predsjedanja pažljivim čitanjem prijedloga, čime je državama članicama omogućeno da postave pitanja i istaknu svoje glavne bojazni te da od Komisije dobiju detaljna objašnjenja o izmjenama u revidiranoj direktivi.

10. Tijekom portugalskog predsjedanja Horizontalna radna skupina za kiberpitanja predstavljanju i čitanju prijedloga posvetila je 17 sastanaka. Izvješće o napretku u pogledu čitanja podneseno je Vijeću za promet, telekomunikacije i energetiku 4. lipnja 2021.

11. Rad se od tada nastavio i dodatno pojačao tijekom slovenskog predsjedanja u cilju postizanja općeg pristupa na sastanku Vijeća (promet, telekomunikacije i energetika) 3. prosinca 2021. Slovensko predsjedništvo reviziji prijedloga NIS 2 posvetilo je 15 sastanaka, kao i mnoge bilateralne rasprave na svim razinama.

12. Horizontalna radna skupina za kiberpitanja usmjerila je svoj rad na preoblikovanje teksta prijedloga, prvo u pogledu interakcije Direktive NIS 2 sa sektorskim zakonodavstvom i područjem primjene, posebice u pogledu javne uprave, DNS korijenskih poslužitelja i klauzule o isključenju, te zatim u pogledu, među ostalim temama, istorazinskog ocjenjivanja, nadležnosti i uzajamne pomoći, koordiniranog otkrivanja ranjivosti, baza podataka s nazivima domena i registracijskim podacima te međunarodne suradnje.

13. Prvi kompromisni prijedlog teksta predložene Direktive objavljen je 21. rujna 2021.[7], na temelju pisanih komentara i neslužbenih dokumenata primljenih od država članica, kao i na temelju prethodnih kompromisnih prijedloga o interakciji Direktive NIS 2 sa sektorskim zakonodavstvom i o području primjene Direktive NIS 2.

[7] 12019/21.

14. O najnovijoj reviziji[8] kompromisnog prijedloga predsjedništva raspravljalo se na razini radne skupine 22. studenoga 2021. Delegacije su općenito pozdravile kompromisni tekst, ali nekoliko je ipak uložilo analitičku rezervu ili dalo primjedbe na dijelove kompromisnog prijedloga. Predložene su neke tehničke izmjene određenih dijelova teksta.

III. SADRŽAJ

15. Na temelju rasprava na razini radne skupine kao glavna politička pitanja utvrđene su sljedeće točke:

a) Područje primjene (članak 2.)

Od početka rasprava o Prijedlogu direktive NIS 2 glavni razlog za zabrinutost koji su navele države članice odnosi se na znatno povećanje broja subjekata obuhvaćenih Direktivom i, posebice, uvođenje pravila o veličini kojim su svi srednji i veliki subjekti koji posluju u sektorima ili pružaju usluge na koje se odnosi Direktiva NIS 2 obuhvaćeni njezinim područjem primjene. Kompromisnim prijedlogom zadržava se to opće pravilo, ali on uključuje i dodatne odredbe kako bi se osigurali potrebna proporcionalnost, veća razina upravljanja rizikom i jasni kriteriji kritičnosti za utvrđivanje subjekata koji su obuhvaćeni područjem primjene Direktive. Nadalje, kompromisni prijedlog sadržava posebne odredbe o određivanju prioriteta pri primjeni mjera nadzora, primjenom pristupa utemeljenog na procjeni rizika.

[8] 12019/5/21 REV 5.

b) Javna uprava (članak 2. stavak 2.a)

Uključivanje javne uprave u područje primjene Direktive NIS 2 bila je tema o kojoj se opširno raspravljalo, s obzirom na to da se sektor javne uprave više razlikuje od drugih sektora na koje se odnosi Direktiva NIS 2. Predsjedništvo je nastojalo postići uravnotežen pristup kojim se uzimaju u obzir posebnosti nacionalnih okvira javne uprave i osigurava da države članice imaju određeni stupanj fleksibilnosti u određivanju subjekata javne uprave koji su obuhvaćeni područjem primjene Direktive NIS 2. Stoga se u kompromisnom tekstu Direktiva NIS 2 primjenjuje na tijela središnje državne uprave, dok države članice mogu utvrditi i da se Direktiva odnosi na tijela javne uprave na regionalnoj ili lokalnoj razini.

c) Klauzula o isključenju (članak 2. stavci 3.a i 3.aa)

Države članice željele su dodatno pojasniti klauzulu o isključenju u smislu da se Direktiva ne primjenjuje na subjekte koji aktivnosti obavljaju u prvom redu u području obrane, nacionalne sigurnosti, javne sigurnosti ili izvršavanja zakonodavstva i na aktivnosti koje se odnose na nacionalnu sigurnost ili obranu. Isključeni su i sudstvo, parlamenti te središnje banke.

d) Interakcija sa sektorskim zakonodavstvom

Države članice istaknule su potrebu da se Direktiva NIS 2 uskladi sa sektorskim zakonodavstvom, osobito Uredbom o digitalnoj operativnoj otpornosti za financijski sektor („DORA”) i Direktivom o otpornosti kritičnih subjekata (Direktiva „CER”). Direktiva NIS 2, koja bi trebala biti osnova za minimalno usklađivanje u području kibersigurnosti, sadržava poseban članak o sektorskim aktima Unije (članak 2.b). Kad je riječ o interakciji s Direktivom o otpornosti kritičnih subjekata, kompromisnim prijedlogom osigurava se veća jasnoća u pogledu pristupa kojim se uzimaju u obzir sve opasnosti. Drugi važni dodaci povezani su s dogovorima o suradnji među nadležnim tijelima na temelju odgovarajućih pravnih akata.

e) Uzajamno učenje (članak 16.)

Uz neke iznimke, države članice usprotivile su se tome da Komisija uvode obvezna istorazinska ocjenjivanja. Predloženim kompromisom osigurava se da se novi mehanizam uzajamnog učenja temelji na uzajamnom povjerenju i da bude dobrovoljan proces koji pokreću države članice.

f) Nadležnost i teritorijalnost (članak 24.) i uzajamna pomoć (članak 34.)

Države članice izrazile su zabrinutost u vezi s posljedicama različite nadležnosti za subjekte u sektoru IKT-a, kako je predložila Komisija. U kompromisnom tekstu pojašnjena je nadležnost na temelju vrste subjekta i ojačan je tekst koji se odnosi na uzajamnu pomoć.

g) Obveze izvješćivanja (članak 20.)

Nakon što su države članice izrazile zabrinutost da bi obvezno izvješćivanje o ozbiljnim kiberprijetnjama preopteretilo subjekte na koje se odnosi Direktiva NIS 2 i dovelo do prekomjernog izvješćivanja, ono je isključeno iz kompromisnog teksta.

IV. ZAKLJUČAK

16. Odbor stalnih predstavnika 24. studenoga 2021. postigao je dogovor o kompromisnom tekstu kako je naveden u Prilogu i odlučio ga podnijeti Vijeću (promet, telekomunikacije i energetika) rada donošenja općeg pristupa.

17. Stoga se Vijeće poziva da odobri kompromisni tekst iz Priloga koji je predstavilo predsjedništvo te da na sastanku 3. prosinca 2021. donese opći pristup.

PRILOG

Prijedlog

DIREKTIVE EUROPSKOG PARLAMENTA I VIJEĆA

o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148

(Tekst značajan za EGP)

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 114.,

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacrta zakonodavnog akta nacionalnim parlamentima,

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora[9],

uzimajući u obzir mišljenje Odbora regija[10],

u skladu s redovnim zakonodavnim postupkom,

[9] SL C , , str. .
[10] SL C , , str. .

budući da:

(1) Cilj Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća[11] bio je izgradnja kibersigurnosnih kapaciteta širom Unije, ublažavanje prijetnji mrežnim i informacijskim sustavima koji se upotrebljavaju za pružanje osnovnih usluga u ključnim sektorima i osiguravanje kontinuiteta takvih usluga u slučaju kiberincidenata, što doprinosi djelotvornom funkcioniranju gospodarstva i društva Unije.

(2) Od stupanja na snagu Direktive (EU) 2016/1148 ostvaren je znatan napredak u povećanju Unijine razine otpornosti u području kibersigurnosti. Preispitivanje te direktive pokazalo je da je bila katalizator za institucionalni i regulatorni pristup kibersigurnosti u Uniji i omogućila bitnu promjenu načina razmišljanja. Njome je osiguran dovršetak nacionalnih okvira utvrđivanjem nacionalnih strategija za [...] **sigurnost mrežnih i informacijskih sustava**, uspostavom nacionalnih kapaciteta i provedbom regulatornih mjera kojima su obuhvaćeni ključna infrastruktura i akteri koje je utvrdila svaka država članica. Doprinijela je i suradnji na razini Unije osnivanjem skupine za suradnju[12] i mreže nacionalnih timova za odgovor na računalne sigurnosne incidente („mreža CSIRT-ova”)[13]. Neovisno o tim postignućima, preispitivanjem Direktive (EU) 2016/1148 otkriveni su bitni nedostaci zbog kojih se njome ne mogu djelotvorno svladati aktualni i novi izazovi u području kibersigurnosti.

---

11 Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194/1, 19.7.2016., str. 1.).

12 Članak 11. Direktive (EU) 2016/1148.

13 Članak 12. Direktive (EU) 2016/1148.

(3) Mrežni i informacijski sustavi razvili su se u okosnicu svakodnevnog života uz brzu digitalnu transformaciju i međupovezanost društva, među ostalim u prekograničnim razmjenama. Taj je razvoj doveo do povećanja kibersigurnosnih prijetnji te time i novih izazova koji zahtijevaju prilagođene, koordinirane i inovativne odgovore u svim državama članicama. Kiberincidenti sve su brojniji, sofisticiraniji, učestaliji, većih razmjera i utjecaja te predstavljaju veliku prijetnju funkcioniranju mrežnih i informacijskih sustava. Zbog toga kiberincidenti mogu ugroziti obavljanje gospodarskih djelatnosti na unutarnjem tržištu, uzrokovati financijske gubitke, narušiti povjerenje korisnika i nanijeti veliku štetu gospodarstvu i društvu Unije. Pripravnost i djelotvornost u području kibersigurnosti sada su važnije nego ikad za pravilno funkcioniranje unutarnjeg tržišta.

(4) Pravna osnova Direktive (EU) 1148/2016 bio je članak 114. Ugovora o funkcioniranju Europske unije (UFEU), čiji je cilj uspostava i funkcioniranje unutarnjeg tržišta jačanjem mjera za usklađivanje nacionalnih pravila. Kibersigurnosni zahtjevi koje moraju ispunjavati subjekti koji pružaju usluge ili obavljaju gospodarski relevantne djelatnosti znatno se razlikuju među državama članicama s obzirom na vrstu, razinu detalja i metodu nadzora tih zahtjeva. Te razlike uzrokuju dodatne troškove i stvaraju poteškoće poduzećima koja prekogranično nude robu ili usluge. Zahtjevi koje je odredila jedna država članica i koji se razlikuju od onih koje je odredila druga država članica ili su čak u sukobu s njima mogu znatno utjecati na te prekogranične djelatnosti.

Nadalje, mogućnost neoptimalne izrade ili provedbe kibersigurnosnih [...] **mjera** u jednoj državi članici vjerojatno će utjecati na razinu kibersigurnosti drugih država članica, posebno s obzirom na intenzivne prekogranične razmjene. Preispitivanje Direktive (EU) 2016/1148 pokazalo je da postoje velike razlike u njezinoj provedbi u državama članicama, među ostalim u pogledu njezina područja primjene, čije je određivanje u velikoj mjeri prepušteno državama članicama. Direktivom (EU) 2016/1148 državama članicama dano je i vrlo široko diskrecijsko pravo u pogledu provedbe obveza sigurnosti i izvješćivanja o incidentima koje su u njoj utvrđene. Stoga postoje velike razlike u provedbi tih obveza na nacionalnoj razini. Slične su se razlike u provedbi pojavile i u odnosu na odredbe te direktive o nadzoru i provedbi.

(5) Sve te razlike dovode do rascjepkanosti unutarnjeg tržišta i mogu štetno utjecati na njegovo funkcioniranje, posebno na prekogranično pružanje usluga i razinu otpornosti u području kibersigurnosti zbog primjene različitih [...] **mjera**. Cilj je ove Direktive ukloniti te velike razlike među državama članicama, posebno određivanjem minimalnih pravila o funkcioniranju koordiniranog regulatornog okvira, utvrđivanjem mehanizama za djelotvornu suradnju nadležnih tijela u svakoj državi članici, ažuriranjem popisa sektora i djelatnosti koji podliježu kibersigurnosnim obvezama te osiguravanjem djelotvornih pravnih lijekova i sankcija ključnih za djelotvorno izvršavanje tih obveza. Stoga bi Direktivu (EU) 2016/1148 trebalo staviti izvan snage i zamijeniti ovom Direktivom.

(6) [...] Države članice **trebale bi moći** poduzimati potrebne mjere za osiguravanje zaštite osnovnih interesa svoje sigurnosti, zaštitu javnog poretka i javne sigurnosti te omogućivanje istrage, otkrivanja i progona kaznenih djela[...].[...]**Direktiva se ne bi trebala primjenjivati na određene javne ili privatne subjekte koji obavljaju svoje aktivnosti u tim područjima. Također se ne bi trebala primjenjivati na aktivnosti subjekta obavljene u tim područjima. Nadalje,** nijedna država članica nije obvezna davati informacije ako smatra da bi njihovo otkrivanje bilo suprotno osnovnim interesima njezine javne sigurnosti. [...]**R**elevantna su nacionalna pravila[...] **ili** pravila Unije za zaštitu klasificiranih podataka, sporazumi o povjerljivosti podataka i neformalni sporazumi o povjerljivosti podataka kao što je Protokol o semaforu[14].

(6a) Pravo Unije o zaštiti osobnih podataka i privatnosti primjenjuje se na svaku obradu osobnih podataka na temelju ove Direktive. Osobito, ovom Direktivom ne dovode se u pitanje Uredba (EU) 2016/679 i Direktiva 2002/58/EZ Europskog parlamenta i Vijeća te stoga ona posebice ne bi trebala utjecati na zadaće i ovlasti neovisnih nadzornih tijela nadležnih za praćenje usklađenosti s odgovarajućim pravom Unije o zaštiti podataka.

---

14 Protokol o semaforu instrument je kojim netko tko dijeli informacije obavješćuje primatelje o svim ograničenjima u daljnjem širenju tih informacija. Upotrebljavaju ga gotovo sve zajednice CSIRT-ova i neki centri za analizu i razmjenu informacija (ISAC).

(7) Stavljanjem izvan snage Direktive (EU) 2016/1148 područje primjene po sektorima trebalo bi proširiti na veći dio gospodarstva s obzirom na razmatranja iz uvodnih izjava od 4. do 6. Obuhvaćenost sektora Direktivom (EU) 2016/1148 trebalo bi stoga proširiti kako bi se osigurala sveobuhvatna pokrivenost sektora i usluga od velike važnosti za ključne društvene i gospodarske djelatnosti na unutarnjem tržištu. Pravila se ne bi trebala razlikovati prema tome jesu li subjekti operatori ključnih usluga ili pružatelji digitalnih usluga. To se razlikovanje pokazalo zastarjelim jer ne odražava stvarnu važnost sektora ili usluga za društvene i gospodarske djelatnosti na unutarnjem tržištu.

(8) U skladu s Direktivom (EU) 2016/1148, države članice bile su odgovorne za utvrđivanje subjekata koji ispunjavaju kriterije na temelju kojih ih se smatralo operatorima ključnih usluga („postupak utvrđivanja”). Kako bi se uklonile velike razlike među državama članicama u tom pogledu i osigurala pravna sigurnost za zahtjeve za upravljanje rizicima i obveze izvješćivanja za sve relevantne subjekte, trebalo bi uspostaviti jedinstveni kriterij za određivanje subjekata obuhvaćenih područjem primjene ove Direktive. Taj bi se kriterij trebao sastojati od primjene pravila o veličini, prema kojem su područjem primjene ove Direktive obuhvaćena sva srednja i velika poduzeća, kako su definirana Preporukom Komisije 2003/361/EZ[15], koja posluju u sektorima ili pružaju vrste usluga na koje se odnosi ova Direktiva. [...]

[15] Preporuka Komisije 2003/361/EZ od 6. svibnja 2003. o definiciji mikropoduzeća te malih i srednjih poduzeća (SL L 124, 20.5.2003., str. 36.).

(8a) Kako bi se osigurao jasan pregled subjekata obuhvaćenih područjem primjene ove Direktive, države članice trebale bi uspostaviti nacionalne mehanizme za samostalno obavješćivanje kojima se od subjekata koji podliježu ovoj Direktivi zahtijeva da nadležnim tijelima iz ove Direktive ili tijelima koja su u tu svrhu imenovale države članice dostave barem svoje ime, adresu i podatke za kontakte te sektor u kojem posluju ili vrstu usluge koju pružaju i, prema potrebi, popis država članica u kojima subjekt pruža svoje usluge. Ako registri postoje na nacionalnoj razini, države članice mogu odlučiti o primjerenim mehanizmima kojima se omogućuje utvrđivanje subjekata obuhvaćenih područjem primjene ove Direktive.

(9) [...]Ovom Direktivom trebali bi biti obuhvaćeni i **mikrosubjekti ili** mali subjekti [...] koji ispunjavaju određene kriterije koji upućuju na ključnu ulogu za gospodarstva ili društva država članica ili za određene sektore ili vrste usluga. Države članice trebale bi biti odgovorne za [...] podnošenje [...] Komisiji **barem relevantnih informacija o broju utvrđenih subjekata, sektoru kojem pripadaju ili vrsti usluge koju pružaju, te posebnih kriterija na temelju kojih su utvrđeni. Države članice mogu također odlučiti, ako je to u skladu s nacionalnim sigurnosnim pravilima, Komisiji dostaviti imena tih subjekata.**

(9a) Tijela javne uprave koja obavljaju aktivnosti u područjima nacionalne sigurnosti, obrane, javne sigurnosti i izvršavanja zakonodavstva te sudstva, parlamenti i središnje banke isključeni su iz područja primjene ove Direktive. Za potrebe ove Direktive ne smatra se da subjekti s regulatornom nadležnošću obavljaju aktivnosti u području izvršavanja zakonodavstva i stoga nisu isključeni iz područja primjene ove Direktive na temelju tih razloga. Nadalje, tijela središnje državne uprave koja su uspostavljena zajednički s trećom zemljom u skladu s međunarodnim sporazumom nisu obuhvaćena područjem primjene ove Direktive.

(9aa) Države članice trebale bi moći utvrditi da se subjekti utvrđeni prije stupanja na snagu ove Direktive kao operatori ključnih usluga u skladu s Direktivom (EU) 2016/1148 trebaju smatrati ključnim subjektima.

(9aaa) Ova se Direktiva ne primjenjuje na diplomatske i konzularne misije država članica u inozemstvu i na njihovu infrastrukturu IKT-a kojom se koriste te misije, ako se takva infrastruktura nalazi u inozemstvu ili se njome upravlja za korisnike u inozemstvu.

(10) Komisija u suradnji sa skupinom za suradnju može izdati smjernice o provedbi kriterija koji se primjenjuju na mikropoduzeća i mala poduzeća.

(11) [...] **Subjekti koji su obuhvaćeni područjem primjene ove Direktive trebali bi biti razvrstani u dvije kategorije, ključnu i važnu, kojima se u obzir uzima razina kritičnosti sektora ili vrsta usluge koju pružaju, kao i njihova veličina. U tom bi pogledu nadležna tijela, prema potrebi, u obzir trebala uzeti sve relevantne sektorske procjene rizika ili smjernice.** Na ključne i važne subjekte trebali bi se primjenjivati [...] zahtjevi za upravljanje rizicima i obveze izvješćivanja. Sustavi nadzora i sankcija trebali bi biti različiti za te dvije kategorije subjekata kako bi se osigurala pravedna ravnoteža između zahtjeva i obveza **utemeljenih na procjeni rizika** s jedne strane te administrativnog opterećenja koje proizlazi iz nadzora usklađenosti s druge strane.

(12) **Ovom Direktivom utvrđuje se osnova za mjere upravljanja kibersigurnosnim rizicima i obvezama izvješćivanja u svim sektorima koji su obuhvaćeni njezinim područjem primjene. Kako bi se izbjegla rascjepkanost odredaba o kibersigurnosti u pravnim aktima Unije, kada se dodatne sektorske odredbe koje se odnose na** mjere upravljanja kibersigurnosnim rizicima **i obveze izvješćivanja smatraju nužnima kako bi se osigurala visoka razina kibersigurnosti, Komisija bi trebala procijeniti mogu li se takve odredbe propisati u provedbenom aktu na temelju ovlasti predviđenih ovom Direktivom. Ako takvi akti ne bi bili prikladni za tu svrhu,** sektorsko zakonodavstvo **moglo bi** doprinijeti osiguravanju visoke razine kibersigurnosti, uzimajući pritom potpuno u obzir posebnosti i složenosti [...] **dotičnih** sektora. **Razlog zbog kojeg provedbeni akt na temelju ovlasti predviđenih ovom Direktivom nije bio primjeren potrebno je objasniti u sektorskom zakonodavstvu. Istodobno bi se takvim sektorskim odredbama pravnih akata Unije u obzir trebala uzeti potreba za sveobuhvatnim i usklađenim okvirom za kibersigurnost.** [...] Time se [...] ne dovode u pitanje postojeće provedbene ovlasti dodijeljene Komisiji u brojnim sektorima, uključujući promet i energetiku.

(12a) Ako sektorski pravni akt Unije **sadrži odredbe** [...] kojima se od ključnih ili važnih subjekata zahtijeva donošenje **mjera koje su po učinku barem istovjetne obvezama utvrđenima u ovoj Direktivi koje se odnose na** upravljanje kibersigurnosnim rizicima [...] **i obveze** o obavješćivanju o svakom **ozbiljnom** incidentu ili ozbiljnoj kiberprijetnji [...], te bi se sektorske odredbe**, među ostalim o nadzoru i provedbi,** trebale primjenjivati. **Pri utvrđivanju istovjetnog učinka obveza utvrđenih u sektorskim odredbama pravnog akta Unije u obzir bi trebalo uzeti sljedeće aspekte: i. mjere upravljanja kibersigurnosnim rizicima trebale bi se sastojati od odgovarajućih i razmjernih tehničkih i organizacijskih mjera za upravljanje rizicima za sigurnost mrežnih i informacijskih sustava koje relevantni subjekti upotrebljavaju za pružanje svojih usluga te bi one trebale uključivati barem sve elemente utvrđene u ovoj Direktivi; ii. obveza obavješćivanja o ozbiljnim incidentima i kiberprijetnjama trebala bi biti barem istovjetna obvezama utvrđenima u ovoj Direktivi u pogledu sadržaja, oblika i rokova obavijesti; iii. modaliteti izvješćivanja koje provode subjekti i relevantna tijela sektorskih zakonodavnih akata Unije trebali bi biti barem istovjetni zahtjevima utvrđenima u ovoj Direktivi u pogledu sadržaja, oblika i rokova i trebali bi u obzir uzimati ulogu CSIRT-ova; iv. zahtjevi u pogledu prekogranične suradnje za relevantna tijela trebali bi biti barem istovjetni onima utvrđenima u ovoj Direktivi. Ako sektorske odredbe pravnog akta Unije ne obuhvaćaju sve subjekte u određenom sektoru koji su obuhvaćeni područjem primjene ove Direktive, relevantne odredbe ove Direktive trebale bi se i dalje primjenjivati na subjekte koji nisu obuhvaćeni tim sektorskim odredbama.**

(12aa) Komisija **bi trebala periodički preispitati primjenu zahtjeva z pogledu istovjetnog učinka u odnosu na sektorske odredbe pravnih akata Unije** [...]. **Komisija se pri pripremi periodičkog preispitivanja treba savjetovati sa skupinom za suradnju**.

(12aaa) U budućim sektorskim pravnim aktima Unije trebalo bi uzeti u obzir definicije navedene u članku 4. ove Direktive te nadzorni i provedbeni okvir utvrđen u poglavlju VI. ove Direktive.

(12ab) Ako se sektorskim odredbama pravnih akata Unije od ključnih ili važnih subjekata zahtijeva donošenje mjera koje su po učinku barem istovjetne obvezama izvješćivanja utvrđenima u ovoj Direktivi, trebalo bi izbjegavati preklapanje obveza izvješćivanja i trebalo bi osigurati usklađenost i djelotvornost postupanja s obavijestima o kiberprijetnjama ili incidentima. U tu se svrhu tim sektorskim odredbama može omogućiti državama članicama da uspostave zajednički, automatski i izravni mehanizam izvješćivanja za slanje obavijesti o ozbiljnim incidentima i kiberprijetnjama i tijelima čije su zadaće utvrđene u odgovarajućim sektorskim odredbama i nadležnim tijelima, uključujući jedinstvenu kontaktnu točku i CSIRT-ove, prema potrebi, odgovornima za kibersigurnosne zadaće predviđene u ovoj Direktivi, ili mehanizam kojim se osigurava sustavna i neposredna razmjena informacija i suradnja među nadležnim tijelima i CSIRT-ovima u vezi s postupanjem s takvim obavijestima. Za potrebe pojednostavnjenja izvješćivanja i provedbe zajedničkog, automatskog i izravnog mehanizma izvješćivanja, države članice mogu, u skladu sa sektorskim zakonodavstvom, iskoristiti jedinstvenu ulaznu točku koju uspostave u sladu s člankom 11. stavkom 5.a ove Direktive. Kako bi se osigurala usklađenost, obveze izvješćivanja iz sektorskih pravnih akata Unije trebale bi biti usklađene s onima utvrđenima na temelju ove Direktive. Države članice mogu odrediti da su nadležna tijela iz ove Direktive ili nacionalni CSIRT-ovi adresati izvješćivanja, u skladu sa sektorskim zakonodavstvom.

(13) Uredbu XXXX/XXXX Europskog parlamenta i Vijeća trebalo bi smatrati sektorskim pravnim aktom Unije u odnosu na ovu Direktivu u pogledu subjekata financijskog sektora. Umjesto odredaba utvrđenih ovom Direktivom trebale bi se primjenjivati odredbe Uredbe XXXX/XXXX koje se odnose na mjere upravljanja rizicima informacijskih i komunikacijskih tehnologija (IKT), upravljanje IKT incidentima, a posebno izvješćivanje o incidentima, kao i na testiranje digitalne operativne otpornosti, mehanizme razmjene informacija i IKT rizik treće strane. Države članice stoga ne bi trebale primjenjivati odredbe ove Direktive o obvezama upravljanja kibersigurnosnim rizicima i [...] izvješćivanja te nadzoru i provedbi na [...] financijske subjekte obuhvaćene Uredbom XXXX/XXXX. Istodobno je važno održavati blizak odnos i razmjenu informacija s financijskim sektorom na temelju ove Direktive. U tu se svrhu Uredbom XXXX/XXXX [...] europskim nadzornim tijelima za financijski sektor i nacionalnim nadležnim tijelima iz Uredbe XXXX/XXXX[...] omogućuje sudjelovanje u [...] **radu** [...] skupine za suradnju te razmjena informacija i suradnja s jedinstvenim kontaktnim točkama imenovanima u skladu s ovom Direktivom**,** [...] **kao i** s nacionalnim CSIRT-ovima. Nadležna tijela iz Uredbe XXXX/XXXX trebala bi podatke o velikim IKT incidentima **i ozbiljnim kiberprijetnjama** slati i jedinstvenim kontaktnim točkama**, nadležnim tijelima ili nacionalnim CSIRT-ovima** imenovanima na temelju ove Direktive. **To se može ostvariti automatskim i izravnim prosljeđivanjem obavijesti o incidentima ili zajedničkom platformom za izvješćivanje.** Osim toga, države članice trebale bi nastaviti uključivati financijski sektor u svoje strategije za kibersigurnost, a nacionalni CSIRT-ovi [...] **mogu** ga obuhvatiti svojim aktivnostima.

(13a) Kako bi se izbjegle praznine u području kibersigurnosnih obveza koje su određene subjektima u zrakoplovnom sektoru iz točke 2. podtočke (a) Priloga I. i udvostručavanje tih obveza, nacionalna tijela imenovana na temelju uredaba (EZ) br. 300/2008[16] i (EU) 2018/1139[17] Europskog parlamenta i Vijeća i nadležna tijela na temelju ove Direktive trebala bi surađivati u vezi s provedbom mjera upravljanja kibersigurnosnim rizicima i nadzorom nad tim mjerama na nacionalnoj razini. Nacionalna tijela imenovana na temelju uredaba (EZ) br. 300/2008 i (EU) 2018/1139 mogla bi smatrati da je usklađenost subjekta s mjerama upravljanja kibersigurnosnim rizicima na temelju ove Direktive [...] u skladu sa zahtjevima utvrđenima u tim uredbama te relevantnim delegiranim i provedbenim aktima donesenima na temelju njih.

---

16 **Uredba (EZ) br. 300/2008 Europskog parlamenta i Vijeća od 11. ožujka 2008. o zajedničkim pravilima u području zaštite civilnog zračnog prometa i stavljanju izvan snage Uredbe (EZ) br. 2320/2002 (SL L 97, 9.4.2008., str. 72.).**

17 **Uredba (EU) 2018/1139 Europskog parlamenta i Vijeća od 4. srpnja 2018. o zajedničkim pravilima u području civilnog zrakoplovstva i osnivanju Agencije Europske unije za sigurnost zračnog prometa i izmjeni uredbi (EZ) br. 2111/2005, (EZ) br. 1008/2008, (EU) br. 996/2010, (EU) br. 376/2014 i direktiva 2014/30/EU i 2014/53/EU Europskog parlamenta i Vijeća te stavljanju izvan snage uredbi (EZ) br. 552/2004 i (EZ) br. 216/2008 Europskog parlamenta i Vijeća i Uredbe Vijeća (EEZ) br. 3922/91 (SL L 212, 22.8.2018., str. 1.).**

(14) S obzirom na međupovezanost kibersigurnosti i fizičke sigurnosti subjekata, trebalo bi osigurati usklađen pristup između Direktive (EU) XXX/XXX Europskog parlamenta i Vijeća i ove Direktive. Kako bi se to postiglo, države članice trebale bi osigurati da se kritični **[**i njima istovjetni subjekti**]** iz Direktive (EU) XXX/XXX smatraju ključnim subjektima na temelju ove Direktive. Države članice trebale bi osigurati i da se njihovim strategijama za kibersigurnost osigurava okvir politike za pojačanu koordinaciju između nadležnog tijela na temelju ove Direktive i nadležnog tijela na temelju Direktive (EU) XXX/XXX u kontekstu razmjene informacija o incidentima i kiberprijetnjama te izvršavanja nadzornih zadaća. **Nadležna** [...] **t**ijela na temelju obiju direktiva trebala bi surađivati i razmjenjivati informacije, posebno u pogledu utvrđivanja kritičnih subjekata, kiberprijetnji, kibersigurnosnih rizika, incidenata **te rizika, prijetnji i incidenata izvan kiberprostora** koji utječu na kritične subjekte ili **subjekte istovjetne kritičnim subjektima,** [...] **uključujući** kibersigurnosne **i fizičke** mjere koje kritični subjekti poduzimaju **i rezultate nadzornih aktivnosti provedenih u odnosu na te subjekte. Nadalje, kako bi se pojednostavnile nadzorne aktivnosti među nadležnim tijelima imenovanima na temelju obiju direktiva te kako bi se smanjilo administrativno opterećenje za dotične subjekte, nadležna tijela trebala bi nastojati uskladiti predloške za obavješćivanje o incidentima i nadzorne postupke.** [...] **Prema potrebi,** nadležna tijela na temelju Direktive (EU) XXX/XXX[...] **mogu zahtijevati** od nadležnih tijela na temelju ove Direktive [...] da izvršavaju svoje nadzorne i provedbene ovlasti [...] **u vezi s** ključnim subjektom koji je utvrđen kao kritičan. [...]

(14a) Subjekti koji pripadaju sektoru digitalne infrastrukture u suštini se temelje na mrežnim i informacijskim sustavima te bi se stoga obvezama koje su ovom Direktivom određene tim subjektima trebalo na sveobuhvatan način obuhvatiti fizičku sigurnost takvih sustava kao dio njihovih obveza upravljanja kibersigurnosnim rizicima i obveza izvješćivanja. S obzirom na to da su ta pitanja obuhvaćena ovom Direktivom, obveze utvrđene u poglavljima od III. do VI. Direktive (EU) XXX/XXX [Direktiva o otpornosti kritičnih subjekata] ne primjenjuju se na takve subjekte.

(15) Vođenje i održavanje pouzdanog, otpornog i sigurnog sustava naziva domena (DNS) ključni su za očuvanje cjelovitosti interneta te njegov kontinuiran i stabilan rad, o kojem ovise digitalno gospodarstvo i društvo. Stoga bi se ova Direktiva trebala primjenjivati na pružatelje DNS usluga u lancu DNS **rezerviranja i** prevođenja **koji su važni za internetsko tržište,** uključujući [...], [...] **registre** naziva vršnih domena, **subjekte koji pružaju usluge registracije naziva domena, operatore** mjerodavnih poslužitelja naziva za nazive domena i **operatore** rekurzivnih prevoditelja. **Pojam „pružatelj DNS usluge" ne bi se trebao primjenjivati na DNS usluge koje se pružaju za vlastite potrebe dotičnog subjekta i njegovih povezanih subjekata. Kibersigurnosne obveze koje proizlaze iz ove Direktive za ovu kategoriju pružatelja usluga strogo su ograničene na mjere upravljanja kibersigurnosnim rizicima i izvješćivanje te se stoga njima ne dovodi u pitanje upravljanje globalnim DNS-om od strane šire zajednice dionika.**

(16) Usluge računalstva u oblaku trebale bi obuhvaćati usluge koje omogućuju pristup na zahtjev i široki daljinski pristup nadogradivom i elastičnom skupu djeljivih i distribuiranih računalnih resursa. Ti računalni resursi uključuju mreže, poslužitelje ili drugu infrastrukturu, operacijske sustave, softver, pohranu, aplikacije i usluge. **Modeli usluga računalstva u oblaku obuhvaćaju, među ostalim, infrastrukturu kao uslugu (IaaS), platformu kao uslugu (PaaS), softver kao uslugu (SaaS) i mrežu kao uslugu (NaaS).** Modeli uvođenja računalstva u oblaku trebali bi uključivati privatne, zajedničke, javne i hibridne oblake. Navedeni modeli usluga i uvođenja imaju isto značenje kao modeli usluga i uvođenja definirani u normi ISO/IEC 17788:2014. Sposobnost korisnika računalstva u oblaku da jednostrano samostalno pruža računalne kapacitete, kao što je vrijeme poslužitelja ili mrežna pohrana, bez ljudske interakcije pružatelja usluga računalstva u oblaku, može se opisati kao administracija na zahtjev. Pojam „široki daljinski pristup" upotrebljava se kako bi se opisalo da se kapaciteti u oblaku osiguravaju preko mreže i da im se pristupa putem mehanizama kojima se promiče upotreba heterogenih tankih ili debelih klijentskih platformi (uključujući mobilne telefone, tablete, prijenosna računala i radne stanice).

Pojam „nadogradiv" odnosi se na računalne usluge koje pružatelj usluga u oblaku dodjeljuje fleksibilno, bez obzira na zemljopisni položaj resursa, kako bi se riješile fluktuacije u potražnji. Pojam „elastičan skup" upotrebljava se za opisivanje računalnih resursa koji se rezerviraju i isporučuju u skladu s potražnjom kako bi se raspoloživi resursi mogli brzo povećati i smanjiti ovisno o radnom opterećenju. Pojam „djeljiv" upotrebljava se za opisivanje računalnih resursa koji se pružaju većem broju korisnika sa zajedničkim pristupom usluzi, pri čemu se obrada provodi odvojeno za svakog korisnika, iako se usluga pruža putem iste elektroničke opreme. Pojam „distribuiran" upotrebljava se za opisivanje računalnih resursa koji se nalaze na različitim umreženim računalima ili uređajima te čija se međusobna komunikacija i koordinacija odvija slanjem poruka.

(17) S obzirom na razvoj inovativnih tehnologija i novih poslovnih modela, očekuje se da će se na tržištu pojaviti novi modeli uvođenja i usluga računalstva u oblaku kao odgovor na rastuće potrebe korisnika. U tom se kontekstu usluge računalstva u oblaku mogu pružati u vrlo distribuiranom obliku, još bliže mjestu na kojem se podaci generiraju ili prikupljaju, čime se prelazi s tradicionalnog modela na visoko distribuirani model („računalstvo na rubu”).

(18) Usluge koje nude pružatelji usluga podatkovnog centra ne mogu se uvijek pružati u obliku usluge računalstva u oblaku. Stoga podatkovni centri ne mogu uvijek biti dio infrastrukture računalstva u oblaku. Kako bi se upravljalo svim rizicima za sigurnost mrežnih i informacijskih sustava, ovom bi Direktivom trebalo obuhvatiti i pružatelje usluga podatkovnog centra koje nisu usluge računalstva u oblaku. Za potrebe ove Direktive, pojam „usluga podatkovnog centra” trebao bi obuhvaćati pružanje usluge koja uključuje strukture ili skupine struktura namijenjenih centraliziranom smještaju, međupovezivanju i radu opreme informacijske tehnologije i mreže za usluge pohrane, obrade i prijenosa podataka, uključujući sve objekte i infrastrukturu za distribuciju električne energije i kontrolu okoliša. Pojam „usluga podatkovnog centra” ne primjenjuje se na interne korporativne podatkovne centre kojima dotični subjekt u čijem su vlasništvu upravlja za vlastite potrebe.

(19) Pružatelji poštanskih usluga u smislu Direktive 97/67/EZ Europskog parlamenta i Vijeća[18], [...] **uključujući** [...] pružatelje usluga [...] kurirske dostave, trebali bi podlijegati ovoj Direktivi ako poduzimaju barem jedan od koraka u poštanskom lancu dostave, a posebno prijam, usmjeravanje ili distribuciju, uključujući i usluge preuzimanja. Usluge prijevoza koje se ne poduzimaju u kombinaciji s jednim od tih koraka ne bi trebale biti obuhvaćene opsegom poštanskih usluga.

---

18 Direktiva 97/67/EZ Europskog parlamenta i Vijeća od 15. prosinca 1997. o zajedničkim pravilima za razvoj unutarnjeg tržišta poštanskih usluga u Zajednici i poboljšanje kvalitete usluga (SL L 15, 21.1.1998., str. 14.).

(20) Te rastuće međuovisnosti rezultat su sve veće prekogranične i međuovisne mreže pružanja usluga koja upotrebljava ključnu infrastrukturu diljem Unije u sektorima energetike, prometa, digitalne infrastrukture, vode za piće i otpadne vode, zdravlja, određenih aspekata javne uprave, kao i u svemirskom sektoru u pogledu pružanja određenih usluga koje ovise o zemaljskoj infrastrukturi koja je u vlasništvu i kojom upravljaju države članice ili privatne strane te stoga ne obuhvaća infrastrukturu koja je u vlasništvu Unije, kojom Unija upravlja ili kojom se upravlja u ime Unije kao dijelom njezinih svemirskih programa. Te međuovisnosti znače da svaki poremećaj, čak i onaj koji je prvotno ograničen na jedan subjekt ili jedan sektor, može imati kaskadne učinke u širem smislu, što može dovesti do dalekosežnih i dugotrajnih negativnih učinaka na pružanje usluga na cijelom unutarnjem tržištu. Pandemija bolesti COVID-19 pokazala je ranjivost naših sve više međuovisnih društava suočenih s rizicima male vjerojatnosti.

(**20a**) **Za potrebe ostvarenja i održavanja visoke razine kibersigurnosti, nacionalne strategije za kibersigurnost koje se zahtijevaju ovom Direktivom trebale bi se sastojati od usklađenih okvira kojima se predviđa upravljanje u području kibersigurnosti. Te strategije mogu se sastojati od jednog dokumenta zakonodavne ili nezakonodavne prirode ili više njih.**

(21) S obzirom na razlike u nacionalnim upravljačkim strukturama i radi zaštite postojećih sektorskih rješenja ili nadzornih i regulatornih tijela Unije, države članice trebale bi moći imenovati više od jednog nadležnog nacionalnog tijela odgovornog za izvršavanje zadaća povezanih sa sigurnošću mrežnih i informacijskih sustava ključnih i važnih subjekata obuhvaćenih ovom Direktivom. Države članice trebale bi moći tu ulogu dodijeliti postojećem tijelu.

(22) Kako bi se olakšala prekogranična suradnja i komunikacija među tijelima i kako bi se omogućila djelotvorna provedba ove Direktive, nužno je da svaka država članica imenuje jedinstvenu nacionalnu kontaktnu točku odgovornu za koordinaciju pitanja sigurnosti mrežnih i informacijskih sustava te za prekograničnu suradnju na razini Unije.

(23) Nadležna tijela ili CSIRT-ovi trebali bi od subjekata primati obavijesti o incidentima na djelotvoran i učinkovit način**, među ostalim kako bi se olakšao, prema potrebi, pravodoban odgovor na incidente i odgovorilo subjektu koji šalje obavijest**. Zadaća jedinstvenih kontaktnih točaka trebala bi biti prosljeđivanje obavijesti o incidentima jedinstvenim kontaktnim točkama drugih pogođenih država članica. [...]

(23a) Sektorskim pravnim aktima Unije kojima se zahtijevaju mjere upravljanja kibersigurnosnim rizicima ili obveze izvješćivanja koje su po učinku barem istovjetne onima utvrđenima u ovoj Direktivi moglo bi se predvidjeti da njihova imenovana nadležna tijela izvršavaju svoje nadzorne i provedbene ovlasti u vezi s takvim mjerama ili obvezama uz pomoć nadležnih tijela imenovanih u skladu s ovom Direktivom. Dotična nadležna tijela mogla bi u tu svrhu uspostaviti dogovore o suradnji. Takvim dogovorima o suradnji mogli bi se, među ostalim, utvrditi postupci koji se odnose na koordinaciju nadzornih aktivnosti, uključujući postupke istraga i izravnog nadzora u skladu s nacionalnim pravom te mehanizam za razmjenu relevantnih informacija o nadzoru i provedbi među nadležnim tijelima, uključujući pristup informacijama povezanima s kibersigurnošću koje zahtijevaju nadležna tijela imenovana u skladu s ovom Direktivom.

(24) Države članice trebale bi biti dostatno opremljene, u smislu tehničkih i organizacijskih sposobnosti, za sprečavanje i otkrivanje incidenata i rizika u mrežnim i informacijskim sustavima, odgovaranje na njih i njihovo ublažavanje. Države članice stoga bi trebale osigurati da njihovi CSIRT-ovi, poznati i kao timovi za hitne računalne intervencije („CERT-ovi”), dobro funkcioniraju i da poštuju ključne zahtjeve kako bi se zajamčile djelotvorne i uskladive sposobnosti za rješavanje incidenata i rizika te kako bi se osigurala učinkovita suradnja na razini Unije. U cilju jačanja odnosa povjerenja između subjekata i CSIRT-ova, u slučajevima kada je CSIRT dio nadležnog tijela, države članice [...] **mogu** razmotriti funkcionalno odvajanje operativnih zadaća koje obavljaju CSIRT-ovi, posebno u vezi s razmjenom informacija i potporom subjektima, te nadzornih aktivnosti nadležnih tijela.

(25) Kad je riječ o osobnim podacima, CSIRT-ovi bi, u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća[19] o osobnim podacima, u ime subjekta iz ove Direktive i na njegov zahtjev, trebali moći osigurati proaktivno pregledavanje mrežnih i informacijskih sustava koji se upotrebljavaju za pružanje njihovih usluga. **Ako je to primjenjivo,** države članice trebale bi nastojati osigurati jednaku razinu tehničkih sposobnosti za sve sektorske CSIRT-ove. Države članice mogu zatražiti pomoć Agencije Europske unije za kibersigurnost (ENISA) u razvoju nacionalnih CSIRT-ova.

(26) S obzirom na važnost međunarodne suradnje u području kibersigurnosti, CSIRT-ovi bi trebali moći, uz mrežu CSIRT-ova uspostavljenu ovom Direktivom, sudjelovati u međunarodnim mrežama suradnje. **Stoga bi CSIRT-ovi i nadležna tijela mogli razmjenjivati informacije, uključujući osobne podatke, s CSIRT-ovima trećih zemalja ili njihovim tijelima u svrhu obavljanja svojih zadaća u skladu s Uredbom (EU) 2016/679. U slučajevima kada nema odluke o primjerenosti donesene u skladu s člankom 45. Uredbe (EU) 2016/679 ili odgovarajućih zaštitnih mjera na temelju članka 46. te uredbe, razmjena osobnih podataka koja se smatra potrebnom za ublažavanje ozbiljnih kiberprijetnji i odgovaranje na ozbiljan incident koji je u tijeku mogla bi se smatrati važnim razlogom od javnog interesa u smislu članka 49. stavka 1. točke (d) Uredbe (EU) 2016/679.**

[19] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

(27) U skladu s Prilogom Preporuci Komisije (EU) 2017/1548 o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera („plan”)[20], incident velikih razmjera trebao bi značiti incident sa znatnim učinkom na najmanje dvije države članice ili incident čiji učinci premašuju sposobnost države članice da na njega odgovori. Ovisno o svojem uzroku i učinku, incidenti velikih razmjera mogu se proširiti i pretvoriti u prave krize koje onemogućavaju pravilno funkcioniranje unutarnjeg tržišta. S obzirom na širok opseg i, u većini slučajeva, prekograničnu prirodu takvih incidenata, države članice i relevantne institucije, tijela i agencije Unije trebali bi surađivati na tehničkoj, operativnoj i političkoj razini kako bi pravilno koordinirali odgovor u cijeloj Uniji.

(28) Budući da iskorištavanje ranjivosti u mrežnim i informacijskim sustavima može uzrokovati znatne poremećaje i štetu, brzo prepoznavanje i otklanjanje tih ranjivosti važan je čimbenik u smanjenju kibersigurnosnog rizika. Subjekti koji razvijaju takve sustave **ili upravljaju njima** trebali bi stoga uspostaviti odgovarajuće postupke za otklanjanje ranjivosti kada ih se otkrije. Budući da ranjivosti često prepoznaju i prijavljuju (otkrivaju) treće strane (subjekti koji podliježu obvezi obavješćivanja), proizvođač ili pružatelj IKT proizvoda ili usluga trebao bi uspostaviti i postupke potrebne za primanje informacija o ranjivosti od trećih strana. U tom pogledu međunarodne norme ISO/IEC 30111 i ISO/IEC [...] **29147** pružaju smjernice o postupanju s ranjivostima i njihovu otkrivanju. Kad je riječ o otkrivanju ranjivosti, posebno je važna koordinacija između subjekata koji podliježu obvezi obavješćivanja i proizvođača ili pružatelja IKT proizvoda ili usluga. Koordinirano otkrivanje ranjivosti odvija se strukturiranim postupkom u okviru kojeg se ranjivosti prijavljuju organizacijama na način kojim se organizaciji omogućuje dijagnosticiranje i otklanjanje ranjivosti prije nego što se detaljne informacije o ranjivosti otkriju trećim stranama ili javnosti. Koordinirano otkrivanje ranjivosti trebalo bi obuhvaćati i koordinaciju između subjekta koji podliježe obvezi obavješćivanja i organizacije u pogledu vremena otklanjanja i objave ranjivosti.

---

[20] Preporuka Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera (SL L 239, 19.9.2017., str. 36.).

(29) Države članice trebale bi stoga poduzeti mjere za olakšavanje koordiniranog otkrivanja ranjivosti uspostavom relevantne nacionalne politike. **U okviru svoje nacionalne politike i u skladu sa svojim nacionalnim pravnim poretkom države članice trebale bi, u mjeri u kojoj je to moguće, nastojati rješavati izazove s kojima se suočavaju oni koji istražuju ranjivosti, uključujući njihovu moguću izloženost kaznenoj odgovornosti.** [...] Države članice trebale bi imenovati CSIRT koji će preuzeti ulogu „koordinatora" i, prema potrebi, djelovati kao posrednik između subjekata koji podliježu obvezi obavješćivanja i proizvođača ili pružatelja IKT proizvoda ili usluga. Zadaće koordinacijskog CSIRT-a trebale bi posebno uključivati utvrđivanje i kontaktiranje dotičnih subjekata, pružanje podrške subjektima koji podliježu obvezi obavješćivanja, pregovaranje o vremenskom okviru za otkrivanje i upravljanje ranjivostima koje utječu na više organizacija (**koordinirano** otkrivanje ranjivosti koje uključuje više strana). Ako **bi prijavljena** ranjivost **potencijalno mogla imati znatan učinak na subjekte** [...] u više država članica, imenovani CSIRT-ovi [...] trebali bi**, prema potrebi,** surađivati u okviru mreže CSIRT-ova.

(30) Pristup točnim i pravodobnim informacijama o ranjivostima koje utječu na IKT proizvode i usluge doprinosi boljem upravljanju kibersigurnosnim rizicima. U tom su pogledu izvori javno dostupnih informacija o ranjivostima važan alat za subjekte i njihove korisnike, ali i za nacionalna nadležna tijela i CSIRT-ove. Zbog toga bi ENISA trebala uspostaviti registar ranjivosti u kojem ključni i važni subjekti i njihovi dobavljači te subjekti koji nisu obuhvaćeni područjem primjene ove Direktive **ili imenovani CSIRT-ovi** mogu dobrovoljno otkriti ranjivosti i pružiti informacije o ranjivostima koje korisnicima omogućuju poduzimanje odgovarajućih mjera ublažavanja.

(31) Iako slični registri ili baze podataka o ranjivosti postoje, na poslužitelju ih smještaju i vode subjekti koji nemaju poslovni nastan u Uniji. Europski registar ranjivosti koji bi vodila ENISA omogućio bi veću transparentnost u pogledu postupka objavljivanja prije službenog otkrivanja ranjivosti i otpornost u slučajevima poremećaja ili prekida u pružanju sličnih usluga. Kako bi se izbjeglo udvostručavanje aktivnosti i postigla komplementarnost u mjeri u kojoj je to moguće, ENISA bi trebala istražiti mogućnost sklapanja sporazuma o strukturiranoj suradnji sa sličnim registrima u jurisdikcijama trećih zemalja. **ENISA bi posebno trebala istražiti mogućnost bliske suradnje s operatorima sustava zajedničkih ranjivosti i izloženosti (CVE), uključujući mogućnost da postane tijelo za korijensko numeriranje CVE-a.**

(32) **Skupina za suradnju trebala bi nastaviti podupirati i olakšavati stratešku suradnju i razmjenu informacija te jačati povjerenje i pouzdanje među državama članicama.** Skupina za suradnju trebala bi svake dvije godine uspostaviti program rada, uključujući djelovanja koja ta skupina treba poduzeti radi provedbe svojih ciljeva i zadaća. Vremenski okvir prvog programa donesenog na temelju ove Direktive trebalo bi uskladiti s vremenskim okvirom posljednjeg programa donesenog na temelju Direktive (EU) 2016/1148 kako bi se izbjegli mogući poremećaji u radu skupine.

(33) Pri izradi smjernica skupina za suradnju trebala bi dosljedno: mapirati nacionalna rješenja i iskustva, procjenjivati učinak rezultata skupine za suradnju na nacionalne pristupe, raspravljati o izazovima u provedbi i izrađivati posebne preporuke koje će se nastojati ispuniti boljom provedbom postojećih pravila.

(34) Skupina za suradnju trebala bi ostati fleksibilan forum i trebala bi moći odgovoriti na nove i promjenjive prioritete i izazove politike, uzimajući pritom u obzir raspoloživost resursa. Trebala bi organizirati redovite zajedničke sastanke s relevantnim privatnim dionicima iz cijele Unije na kojima bi se raspravljalo o aktivnostima skupine i prikupljale informacije o novim izazovima politike. Kako bi se poboljšala suradnja na razini Unije, skupina bi trebala razmotriti mogućnost pozivanja tijela i agencija Unije uključenih u politiku kibersigurnosti, kao što su Europski centar za kiberkriminalitet (EC3), Agencija Europske unije za sigurnost zračnog prometa (EASA) i Agencija Europske unije za svemirski program (EUSPA), da sudjeluju u njezinu radu.

(35) Nadležna tijela i CSIRT-ove trebalo bi poticati na sudjelovanje u programima razmjene za službenike iz drugih država članica u cilju poboljšanja suradnje. Nadležna tijela trebala bi poduzeti potrebne mjere kako bi službenicima iz drugih država članica omogućila da imaju djelotvornu ulogu u aktivnostima nadležnog tijela domaćina.

(35a) Mreža CSIRT-ova trebala bi nastaviti doprinositi jačanju povjerenja i pouzdanja te promicati brzu i djelotvornu operativnu suradnju među državama članicama. Kako bi se poboljšala operativna suradnja na razini Unije, mreža CSIRT-ova trebala bi razmotriti mogućnost pozivanja tijela i agencija Unije uključenih u politiku kibersigurnosti, kao što je Europol, da sudjeluju u njezinu radu.

(36) [...]

(36a) Kako bi se olakšala djelotvorna provedba odredaba ove Direktive, kao što su upravljanje ranjivostima, upravljanje kibersigurnosnim rizicima, mjere izvješćivanja i mehanizmi za razmjenu informacija, države članice mogu surađivati s trećim zemljama i poduzimati aktivnosti koje se u tu svrhu smatraju primjerenima, uključujući razmjenu informacija o prijetnjama, incidentima, ranjivostima, alatima i metodama, taktikama, tehnikama i postupcima, pripravnosti i vježbama za upravljanje kiberkrizom, osposobljavanju, izgradnji povjerenja i strukturiranim mehanizmima za razmjenu informacija. Takvi sporazumi o suradnji trebali bi biti u skladu s pravom Unije o zaštiti podataka.

(37) Države članice trebale bi doprinijeti uspostavi okvira EU-a za odgovor na kiberkrize utvrđenog u Preporuci (EU) 2017/1584 putem postojećih mreža suradnje, posebno Europske mreže organizacija za vezu za kiberkrize (EU-CyCLONe), mreže CSIRT-ova i skupine za suradnju. EU-CyCLONe i mreža CSIRT-ova trebali bi surađivati na temelju postupovnih aranžmana kojima se utvrđuju načini te suradnje **i izbjegavati udvostručavanje zadaća**. U poslovniku EU-CyCLONe-a trebalo bi dodatno utvrditi načine funkcioniranja mreže, uključujući, ali ne ograničavajući se na, uloge, oblike suradnje, interakcije s drugim relevantnim akterima i predloške za razmjenu informacija, kao i komunikacijska sredstva. Za upravljanje krizama na **političkoj** razini Unije relevantne strane trebale bi se oslanjati na aranžmane za integrirani politički odgovor na krizu (IPCR). Komisija bi u tu svrhu trebala primjenjivati međusektorski postupak koordiniranja krize na visokoj razini ARGUS. Ako kriza ima znatan utjecaj na vanjsku ili zajedničku sigurnosnu i obrambenu politiku (ZSOP), trebalo bi aktivirati mehanizam za odgovor na krizu (CRM) Europske službe za vanjsko djelovanje (ESVD).

(37a) EU-CyCLONe bi trebao djelovati kao posrednička mreža između tehničke i političke razine tijekom kiberincidenata i kiberkriza velikih razmjera. Nadovezivanjem na nalaze mreže CSIRT-ova i upotrebom vlastitih kapaciteta za izradu analize učinka incidenata i kriza velikih razmjera te podupiranjem donošenja odluka na političkoj razini trebao bi poboljšati suradnju na operativnoj razini. Institucije, tijela i agencije EU-a trebali bi članom EU-CyCLONe-a imenovati nadležno tijelo odgovorno za upravljanje incidentima i krizama velikih razmjera.

(38) [...]

(39) [...]

(39a) Ključni i važni subjekti u velikoj mjeri snose odgovornost za osiguravanje sigurnosti mrežnih i informacijskih sustava. Trebalo bi promicati i razvijati kulturu upravljanja rizicima, uključujući procjenu rizika i provedbu sigurnosnih mjera primjerenih rizicima s kojima se suočava.

(40) Mjerama za upravljanje rizicima **trebalo bi uzeti u obzir stupanj ovisnosti subjekta o mrežnim i informacijskim sustavima te** bi one trebale uključivati mjere za utvrđivanje rizika od incidenata, sprečavanje, otkrivanje i rješavanje incidenata te ublažavanje njihova učinka. Sigurnost mrežnih i informacijskih sustava trebala bi uključivati sigurnost podataka koji se pohranjuju, prenose i obrađuju.

(40a) Budući da prijetnje sigurnosti mrežnih i informacijskih sustava mogu biti različitog podrijetla, u ovoj se Direktivi primjenjuje pristup kojim se uzimaju u obzir sve opasnosti, a koji uključuje zaštitu mrežnih i informacijskih sustava i njihova fizičkog okruženja od bilo kojeg događaja poput krađe, požara, poplave, telekomunikacijskih problema ili prekida opskrbe električnom energijom ili od bilo kojeg neovlaštenog fizičkog pristupa te oštećenja i ometanja informacija i objekata za obradu podataka subjekta koji bi mogli ugroziti dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koji se nude i kojima se pristupa putem mrežnih i informacijskih sustava. Mjere za upravljanje rizicima trebale bi se stoga odnositi i na fizičku sigurnost i sigurnost okruženja uključivanjem mjera za zaštitu mrežnih i informacijskih sustava subjekta od kvarova u sustavu, ljudske pogreške, zlonamjernih radnji ili prirodnih pojava u skladu s europskim ili međunarodno priznatim normama, kao što su one iz serije ISO 27000. U tom pogledu subjekti bi se u okviru svojih mjera za upravljanje rizicima trebali baviti i sigurnošću ljudskih resursa te bi trebali uspostaviti odgovarajuće politike kontrole pristupa. Te bi mjere trebale biti usklađene s Direktivom XXXX [Direktiva o otpornosti kritičnih subjekata].

(40b) U nedostatku odgovarajućih europskih programa kibersigurnosne certifikacije donesenih u skladu s Uredbom (EU) 2019/881, za potrebe usklađivanja sa zahtjevima za upravljanje kibersigurnosnim rizicima iz ove Direktive države članice mogle bi zahtijevati od subjekata da upotrebljavaju certificirane IKT proizvode, usluge i procese ili da pribave certifikat u okviru dostupnih nacionalnih programa u području kibersigurnosti.

(41) Kako bi se izbjeglo nerazmjerno financijsko i administrativno opterećenje za ključne i važne subjekte, zahtjevi za upravljanje kibersigurnosnim rizicima trebali bi biti razmjerni riziku kojemu je izložen dotični mrežni ili informacijski sustav, uzimajući u obzir suvremenost takvih mjera **i trošak njihove provedbe**. **Trebalo bi uzeti u obzir i veličinu subjekta te vjerojatnost pojave incidenata i njihovu ozbiljnost.**

(41a) Kako bi se smanjilo regulatorno opterećenje, zahtjevi za provedbu mjera upravljanja kibersigurnosnim rizicima za srednje ili male subjekte te mikrosubjekte trebali bi u načelu biti blaži, osim ako bi se kriterijima kritičnosti ili nacionalnim procjenama rizika opravdali stroži zahtjevi, posebno u pogledu subjekata koji ispunjavaju kriterije povezane s kritičnošću utvrđene u ovoj Direktivi.

(42) Ključni i važni subjekti trebali bi jamčiti sigurnost mrežnih i informacijskih sustava koje upotrebljavaju u svojim aktivnostima. To su ponajprije privatni mrežni i informacijski sustavi kojima upravljaju njihovi vlastiti zaposlenici u IT-u ili vanjski zaposlenici koji se brinu o sigurnosti. Na temelju ove Direktive, zahtjevi za upravljanje kibersigurnosnim rizicima i zahtjevi izvješćivanja trebali bi se primijeniti na relevantne ključne i važne subjekte bez obzira na to održavaju li sami svoje mrežne i informacijske sustave ili to eksternaliziraju.

(42aa) Uzimajući u obzir njihovu prekograničnu prirodu, pružatelji DNS usluga, registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu, pružatelji usluga računalstva u oblaku, pružatelji usluga podatkovnog centra, pružatelji mreža za isporuku sadržaja, pružatelji upravljanih usluga i pružatelji upravljanih sigurnosnih usluga trebali bi podlijegati višem stupnju usklađenosti na razini Unije. Stoga bi provedbu kibersigurnosnih mjera trebalo olakšati putem provedbenog akta.

(43) Suzbijanje kibersigurnosnih rizika koji proizlaze iz lanca opskrbe subjekta i njegova odnosa s dobavljačima posebno je važno s obzirom na učestalost incidenata u kojima su subjekti postali žrtve kibernapada i u kojima su zlonamjerni akteri ugrozili sigurnost mrežnih i informacijskih sustava subjekta iskorištavanjem ranjivosti koje utječu na proizvode i usluge trećih strana. Subjekti bi stoga trebali procijeniti i uzeti u obzir ukupnu kvalitetu proizvoda i kibersigurnosnih praksi svojih dobavljača i pružatelja usluga, uključujući njihove sigurne razvojne postupke.

(44) U područjima kao što su odgovor na incidente, penetracijska testiranja, revizije sigurnosti i savjetovanje, pružatelji upravljanih sigurnosnih usluga (MSSP-ovi) imaju posebno važnu ulogu među pružateljima usluga u pomaganju subjektima u njihovim nastojanjima da otkriju incidente i odgovore na njih. Međutim, MSSP-ovi su i sami bili meta kibernapada te njihova bliska integracija u rad operatora predstavlja poseban kibersigurnosni rizik. Subjekti bi stoga trebali postupati s većom pažnjom pri odabiru MSSP-a.

(44a) U kontekstu svojih nadzornih zadaća i nacionalna nadležna tijela mogu imati koristi od kibersigurnosnih usluga kao što su revizije sigurnosti i penetracijska testiranja ili odgovor na incidente. Kako bi pomogla subjektima i nacionalnim nadležnim tijelima pri odabiru kvalificiranih i pouzdanih pružatelja kibersigurnosnih usluga, Komisija bi uz pomoć skupine za suradnju i ENISA-e trebala razmotriti mogućnost podnošenja zahtjeva za europske programe kibersigurnosne certifikacije u skladu s člankom 48. Uredbe (EU) 2019/881.

(45) Subjekti bi trebali raditi i na suzbijanju kibersigurnosnih rizika koji proizlaze iz njihove interakcije i odnosa s drugim dionicima unutar šireg ekosustava. Osobito, subjekti bi trebali poduzeti odgovarajuće mjere kako bi osigurali da se njihova suradnja s akademskim i istraživačkim institucijama odvija u skladu s njihovim kibersigurnosnim politikama i da slijedi dobre prakse u pogledu sigurnog pristupa informacijama i širenja informacija općenito, a posebno u pogledu zaštite intelektualnog vlasništva. Slično tome, s obzirom na važnost i vrijednost podataka za aktivnosti subjekata, pri oslanjanju na usluge transformacije i analize podataka koje pružaju treće strane subjekti bi trebali poduzeti sve odgovarajuće kibersigurnosne mjere.

(46) Kako bi se dodatno suzbili ključni rizici u lancu opskrbe i pomoglo subjektima koji djeluju u sektorima obuhvaćenima ovom Direktivom da na odgovarajući način upravljaju kibersigurnosnim rizicima u lancu opskrbe i kibersigurnosnim rizicima povezanima s dobavljačima, skupina za suradnju koja uključuje relevantna nacionalna tijela, u suradnji s Komisijom i ENISA-om, trebala bi provoditi koordinirane procjene rizika u lancu opskrbe pojedinog sektora, kao što je već učinjeno za 5G mreže u skladu s Preporukom (EU) 2019/534 o kibersigurnosti 5G mreža[21], u cilju utvrđivanja ključnih IKT usluga, sustava ili proizvoda, relevantnih prijetnji i ranjivosti za pojedini sektor.

[21] Preporuka Komisije (EU) 2019/534 od 26. ožujka 2019. Kibersigurnost 5G mreža (SL L 88, 29.3.2019., str. 42.).

(47) U procjenama rizika u lancu opskrbe, s obzirom na značajke dotičnog sektora, trebalo bi uzeti u obzir tehničke i, prema potrebi, netehničke čimbenike, uključujući one definirane u Preporuci (EU) 2019/534, u usklađenoj procjeni rizika sigurnosti 5G mreža na razini EU-a i u paketu instrumenata EU-a za kibersigurnost 5G tehnologije oko kojih se usuglasila skupina za suradnju. Pri utvrđivanju lanaca opskrbe koji bi trebali biti podložni koordiniranoj procjeni rizika, u obzir bi trebalo uzeti sljedeće kriterije: i. mjeru u kojoj se ključni i važni subjekti koriste određenim ključnim IKT uslugama, sustavima ili proizvodima i oslanjaju na njih; ii. važnost specifičnih ključnih IKT usluga, sustava ili proizvoda u obavljanju kritičnih ili osjetljivih funkcija, uključujući obradu osobnih podataka; iii. dostupnost alternativnih IKT usluga, sustava ili proizvoda; iv. otpornost cjelokupnog lanca opskrbe IKT uslugama, sustavima ili proizvodima na ometajuće događaje i v. potencijalnu buduću važnost novih IKT usluga, sustava ili proizvoda za aktivnosti subjekata.

(48) Kako bi se pojednostavnile pravne obveze određene pružateljima javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga i pružateljima usluga povjerenja povezane sa sigurnošću njihovih mrežnih i informacijskih sustava te kako bi se tim subjektima i njihovim nadležnim tijelima omogućilo ostvarivanje koristi od pravnog okvira uspostavljenog ovom Direktivom (uključujući imenovanje CSIRT-ova odgovornih za rješavanje rizika i incidenata, sudjelovanje nadležnih vlasti i tijela u radu skupine za suradnju i mreže CSIRT-ova), trebalo bi ih uključiti u područje primjene ove Direktive. Stoga bi trebalo staviti izvan snage odgovarajuće odredbe utvrđene Uredbom (EU) br. 910/2014 Europskog parlamenta i Vijeća[22] i Direktivom (EU) 2018/1972 Europskog parlamenta i Vijeća[23] koje se odnose na uvođenje zahtjeva sigurnosti i obavješćivanja za te vrste subjekata.

---

[22] Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (SL L 257, 28.8.2014., str. 73.).

[23] Direktiva (EU) 2018/1972 Europskog parlamenta i Vijeća od 11. prosinca 2018. o Europskom zakoniku elektroničkih komunikacija (SL L 321, 17.12.2018., str. 36.).

(48a) Sigurnosne obveze utvrđene u ovoj Direktivi trebale bi se smatrati dopunom zahtjeva uvedenih pružateljima usluga povjerenja na temelju Uredbe (EU) br. 910/2014 (Uredba eIDAS). Od pružatelja usluga povjerenja trebalo bi zatražiti da poduzmu sve odgovarajuće i razmjerne mjere za upravljanje rizicima kojima su izložene njihove usluge, među ostalim u odnosu na korisnike i ovisne treće strane, te da prijavljuju sigurnosne incidente iz ove Direktive. Takve obveze u pogledu sigurnosti i izvješćivanja trebale bi se odnositi i na fizičku zaštitu pružene usluge. I dalje se primjenjuje članak 24. Uredbe (EU) 910/2014.

(48aa) Države članice nadzornim tijelima eIDAS-a mogu dodijeliti ulogu nadležnih tijela za usluge povjerenja kako bi se osigurao nastavak postojećih praksi i nadogradilo znanje i iskustvo stečeni u primjeni Uredbe eIDAS. Ako je ta uloga dodijeljena drugom tijelu, nacionalna nadležna tijela iz ove Direktive trebala bi pravodobno blisko surađivati razmjenjujući relevantne informacije kako bi se osigurao djelotvoran nadzor i usklađenost pružatelja usluga povjerenja sa zahtjevima utvrđenima u ovoj Direktivi i Uredbi [XXXX/XXXX].

Ako je to primjenjivo, nacionalno nadležno tijelo iz ove Direktive trebalo bi odmah obavijestiti nadzorno tijelo eIDAS-a o svim prijavljenim ozbiljnim kiberprijetnjama ili incidentima s učinkom na usluge povjerenja te o svim neusklađenostima pružatelja usluga povjerenja sa zahtjevima iz ove Direktive. Za potrebe izvješćivanja države članice mogu se, ako je to primjenjivo, koristiti jedinstvenom kontaktnom točkom uspostavljenom kako bi se postiglo zajedničko i automatsko izvješćivanje nadzornog tijela eIDAS-a i nadležnog tijela iz ove Direktive o incidentima. Pravilima o obvezama izvješćivanja ne bi se trebale dovesti u pitanje Uredba (EU) 2016/679 i Direktiva 2002/58/EZ Europskog parlamenta i Vijeća[24].

[24] Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL L 201, 31.7.2002., str. 37.).

(49) Prema potrebi i kako bi se izbjegli nepotrebni poremećaji, **u okviru aranžmana za prenošenje koje provode države članice u odnosu na ovu Direktivu trebale bi se uzeti u obzir** postojeće nacionalne smjernice [...] donesene za prenošenje pravila povezanih sa sigurnosnim mjerama utvrđenima u član**cima** 40. [...] i 41. Direktive (EU) 2018/1972 [...]**, čime se nadograđuju znanje i vještine stečeni na temelju Direktive (EU) 2018/1972 koji se odnose na mjere upravljanja sigurnosnim rizicima i obavješćivanja o incidentima. ENISA ujedno može izraditi smjernice o sigurnosnim zahtjevima i zahtjevima izvješćivanja za pružatelje javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga kako bi se olakšalo usklađivanje i prijelaz, a poremećaji sveli na najmanju moguću mjeru. Države članice nacionalnim regulatornim tijelima mogu dodijeliti ulogu nadležnih tijela za elektroničke komunikacije kako bi se osigurao nastavak postojećih praksi i nadogradilo znanje i iskustvo stečeni u okviru Direktive (EU) 2018/1972.**

(50) S obzirom na sve veću važnost brojevno neovisnih interpersonalnih komunikacijskih usluga, potrebno je osigurati da se i na takve usluge primjenjuju odgovarajući sigurnosni zahtjevi u skladu s njihovim posebnostima i gospodarskom važnošću. Stoga bi pružatelji takvih usluga trebali osigurati i odgovarajuću razinu sigurnosti mrežnih i informacijskih sustava s obzirom na rizik kojem su izloženi. S obzirom na to da pružatelji brojevno neovisnih interpersonalnih komunikacijskih usluga obično nemaju stvarnu kontrolu nad prijenosom signala mrežama, stupanj rizika za takve usluge može se u nekim aspektima smatrati nižim od rizika za tradicionalne elektroničke komunikacijske usluge. Isto bi trebalo primijeniti na interpersonalne komunikacijske usluge koje se koriste brojevima, a koje nemaju stvarnu kontrolu nad prijenosom signala.

(51) Unutarnje tržište ovisi o funkcioniranju interneta više nego ikad prije. Usluge gotovo svih ključnih i važnih subjekata ovise o uslugama koje se pružaju putem interneta. Kako bi se osiguralo neometano pružanje usluga ključnih i važnih subjekata, važno je da javne elektroničke komunikacijske mreže, kao što su, primjerice, okosnice internetske mreže ili podmorski komunikacijski kabeli, uspostave odgovarajuće kibersigurnosne mjere i prijave incidente povezane s njima.

(52) [...] **Ako je to primjenjivo**, subjekti bi trebali obavijestiti svoje primatelje usluga o posebnim [...] mjerama koje mogu poduzeti kako bi ublažili rizik koji im je uzrokovala **ozbiljna kiberprijetnja**. **Subjekti bi trebali, prema potrebi, a posebno u slučajevima u kojima može nastati ozbiljna kiberprijetnja, o samoj prijetnji obavijestiti i svoje primatelje usluga istodobno s nadležnim tijelima ili CSIRT-ovima.** Zahtjev obavješćivanja primatelja usluga o takvim prijetnjama ne bi trebao podrazumijevati oslobađanje subjekata od obveze da o vlastitom trošku poduzmu odgovarajuće i hitne mjere kako bi se spriječile ili uklonile sve kiberprijetnje i ponovno uspostavila normalna sigurnosna razina usluge. Pružanje takvih informacija o [...] **kiber**prijetnjama trebalo bi biti besplatno za primatelje usluga.

(53) Osobito, pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga trebali bi obavijestiti primatelje usluga o posebnim i ozbiljnim kiberprijetnjama te o mjerama koje mogu poduzeti kako bi očuvali sigurnost svojih komunikacija, na primjer upotrebom posebnih vrsta softvera ili tehnologija šifriranja.

(54) Kako bi se zaštitila sigurnost elektroničkih komunikacijskih mreža i usluga, trebalo bi promicati upotrebu šifriranja, posebice šifriranja s kraja na kraj, koja bi, prema potrebi, trebala biti obvezna za pružatelje takvih usluga i mreža u skladu s načelima zadane i integrirane sigurnosti i privatnosti za potrebe članka 18. Upotrebu šifriranja s kraja na kraj trebalo bi uskladiti s ovlastima država članica da osiguraju zaštitu svojih ključnih sigurnosnih interesa i javne sigurnosti te da dopuste istragu, otkrivanje i progon kaznenih djela u skladu s pravom Unije. Rješenjima za zakonit pristup informacijama u komunikacijama šifriranima s kraja na kraj trebala bi se očuvati djelotvornost šifriranja u zaštiti privatnosti i sigurnosti komunikacija te bi se istodobno trebao osigurati djelotvoran odgovor na kriminal.

(55) Ovom se Direktivom utvrđuje pristup izvješćivanju o incidentima u dvije faze kako bi se uspostavila prava ravnoteža između, s jedne strane, brzog izvješćivanja koje pridonosi ublažavanju potencijalnog širenja incidenata i omogućuje subjektima da traže podršku te, s druge strane, detaljnog izvješćivanja kojim se iz pojedinačnih incidenata izvlače vrijedne pouke i s vremenom poboljšava otpornost na kiberprijetnje pojedinačnih poduzeća i cijelih sektora. Kada subjekti dobiju informaciju o incidentu, trebali bi biti dužni u roku od 24 sata dostaviti prvu obavijest, nakon čega u roku od mjesec dana moraju dostaviti završno izvješće. Prva obavijest trebala bi sadržavati samo informacije koje su nužne kako bi nadležna tijela bila upoznata s incidentom i kako bi se subjektu omogućilo traženje pomoći, ako je to potrebno. U takvoj bi obavijesti, ako je to moguće, trebalo navesti pretpostavlja li se da je incident uzrokovan nezakonitim ili zlonamjernim djelovanjem. Države članice trebale bi osigurati da se zahtjevom za podnošenje te prve obavijesti resursi subjekta koji podliježe obvezi obavješćivanja ne preusmjeravaju s aktivnosti povezanih s rješavanjem incidenata koje bi trebale biti prioritetne. Kako bi se dodatno spriječilo da se zbog obveza izvješćivanja o incidentima preusmjeravaju resursi za rješavanje incidenata ili na drugi način ugrožavaju aktivnosti subjekata u tom pogledu, države članice trebale bi također, u opravdanim slučajevima i u dogovoru s nadležnim tijelima ili CSIRT-om, dotičnom subjektu omogućiti odstupanje od roka od 24 sata za prvu obavijest i roka od mjesec dana za završno izvješće.

(55a) Proaktivan pristup kiberprijetnjama ključan je za upravljanje kibersigurnosnim rizicima te bi nadležnim tijelima trebao omogućiti da djelotvorno spriječe da se kiberprijetnje pretvore u stvarne incidente koji mogu uzrokovati znatne materijalne ili nematerijalne gubitke. U tu je svrhu od ključne važnosti obavješćivanje o ozbiljnim kiberprijetnjama.

(56) Ključni i važni subjekti često određeni incident, zbog njegovih značajki, moraju prijaviti različitim tijelima u skladu s obvezama obavješćivanja uključenima u razne pravne instrumente. Takvi slučajevi stvaraju dodatna opterećenja i mogu dovesti i do nesigurnosti u pogledu oblika obavijesti i postupanja s njima. S obzirom na to i u svrhu pojednostavnjenja izvješćivanja o sigurnosnim incidentima, države članice [...] **mogle** bi uspostaviti *jedinstvenu ulaznu točku* za sve obavijesti koje se zahtijevaju ovom Direktivom i drugim pravom Unije, kao što su Uredba (EU) 2016/679 i Direktiva 2002/58/EZ. ENISA bi sa skupinom za suradnju trebala izraditi zajedničke predloške za obavješćivanje s pomoću smjernica kojima bi se pojednostavnile i uskladile informacije o kojima se izvješćuje koje se zahtijevaju pravom Unije i smanjilo opterećenje za poduzeća.

(57) Ako se sumnja da je incident povezan s aktivnostima koje se prema pravu Unije ili nacionalnom pravu smatraju ozbiljnim kriminalnim aktivnostima, države članice trebale bi ključne i važne subjekte poticati da, na temelju primjenjivih pravila kaznenog postupka u skladu s pravom Unije, relevantnim tijelima za izvršavanje zakonodavstva prijave incidente za koje se sumnja da su ozbiljne kriminalne naravi. Prema potrebi i ne dovodeći u pitanje pravila o zaštiti osobnih podataka koja se primjenjuju na Europol, poželjno je da EC3 i ENISA olakšavaju koordinaciju između nadležnih tijela i tijela za izvršavanje zakonodavstva različitih država članica.

(58) U mnogim slučajevima osobni podaci ugroženi su zbog incidenata. U tom kontekstu nadležna tijela trebala bi surađivati i razmjenjivati informacije o svim relevantnim pitanjima s tijelima za zaštitu podataka i nadzornim tijelima na temelju Direktive 2002/58/EZ.

(59) Vođenje točnih i potpunih baza podataka s nazivima domena i registracijskim podacima (tzv. podaci WHOIS) te omogućivanje zakonitog pristupa takvim podacima ključni su za osiguravanje sigurnosti, stabilnosti i otpornosti DNS-a, što doprinosi visokoj zajedničkoj razini kibersigurnosti u Uniji. Obrada koja uključuje osobne podatke u skladu je s pravom Unije o zaštiti podataka.

(60) Dostupnost i pravodobna pristupačnost tih podataka javnim tijelima, uključujući nadležna tijela na temelju prava Unije ili nacionalnog prava za sprečavanje, istragu ili progon kaznenih djela, CERT-ovima, [...]CSIRT-ovima te, u pogledu podataka njihovih klijenata, pružateljima elektroničkih komunikacijskih mreža i usluga te pružateljima kibersigurnosnih tehnologija i usluga koji djeluju u ime tih klijenata, ključni su za sprečavanje i suzbijanje zlouporabe sustava naziva domena, posebno za sprečavanje, otkrivanje i odgovor na kiberincidente. Takav pristup trebao bi biti u skladu s pravom Unije o zaštiti podataka u mjeri u kojoj se odnosi na osobne podatke.

(61) Kako bi se osigurala dostupnost točnih i potpunih podataka o registraciji naziva domena, registri vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu (tzv. registrari) trebali bi prikupljati i jamčiti cjelovitost i dostupnost podataka o registraciji naziva domena. **Kad je riječ o registracijskim podacima, subjekti bi posebno trebali provjeriti ime i e-adresu korisnika domene.** [...] Registri vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu trebali bi uspostaviti politike i postupke za prikupljanje i održavanje točnih i potpunih registracijskih podataka te za sprečavanje i ispravljanje netočnih registracijskih podataka u skladu s pravilima Unije o zaštiti podataka.

(62) Registri vršnih domena i subjekti koji im pružaju usluge registracije naziva domena trebali bi objaviti podatke o registraciji naziva domena koji nisu obuhvaćeni područjem primjene pravila Unije o zaštiti podataka, kao što su podaci o pravnim osobama.[25] Registri vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu trebali bi usto zakonitim tražiteljima pristupa omogućiti legalan pristup podacima o registraciji određenih naziva domena koji se odnose na fizičke osobe, u skladu s pravom Unije o zaštiti podataka. Države članice trebale bi osigurati da registri vršnih domena i subjekti koji im pružaju usluge registracije naziva domena bez nepotrebne odgode odgovaraju na zahtjeve za otkrivanje podataka o registraciji naziva domena **koje upute zakoniti tražitelji pristupa, kao što su nadležna tijela na temelju prava Unije ili nacionalnog prava u području nacionalne sigurnosti ili kaznenog pravosuđa ili CSIRT-ovi**. Registri vršnih domena i subjekti koji im pružaju usluge registracije naziva domena trebali bi uspostaviti politike i postupke za objavljivanje i otkrivanje registracijskih podataka, uključujući sporazume o razini usluga za rješavanje zahtjeva za pristup zakonitih tražitelja pristupa. Postupak pristupa može uključivati i upotrebu sučelja, portala ili drugog tehničkog alata kako bi se osigurao učinkovit sustav za podnošenje zahtjeva i pristupanje registracijskim podacima. **Države članice trebale bi osigurati da sve vrste pristupa registracijskim podacima domena (osobnim i neosobnim podacima) budu besplatne.** U cilju promicanja usklađenih praksi na unutarnjem tržištu, Komisija može donijeti smjernice o takvim postupcima ne dovodeći u pitanje nadležnosti Europskog odbora za zaštitu podataka **u skladu s i kao dopuna međunarodnim normama koje je razvila šira zajednica dionika**.

---

25 **25** U uvodnoj izjavi 14. [...] Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća navodi se: „Ovom se Uredbom ne obuhvaća obrada osobnih podataka koji se tiču pravnih osoba, a osobito poduzetnika koji su ustanovljeni kao pravne osobe, uključujući ime i oblik pravne osobe i kontaktne podatke pravne osobe”.

(63) [...]**K**ljučni i važni subjekti obuhvaćeni ovom Direktivom trebali bi biti u nadležnosti države članice u kojoj pružaju usluge. **Subjekti iz točaka od 1. do 7. i 10. Priloga I., pružatelji usluga povjerenja i pružatelji središta za razmjenu internetskog prometa iz točke 8. Priloga I. i točaka od 1. do 5. Priloga II. ovoj Direktivi trebali bi biti u nadležnosti države članice u kojoj imaju poslovni nastan.** Ako subjekt pruža usluge **ili ima poslovni nastan** u više država članica, trebao bi biti u zasebnoj i istodobnoj nadležnosti svake od tih država članica. Nadležna tijela tih država članica trebala bi surađivati, međusobno si pomagati i, prema potrebi, provoditi zajedničke nadzorne aktivnosti. **Ako države članice odluče izvršavati nadležnost, trebale bi izbjegavati da se isto postupanje sankcionira više puta za povredu obveza utvrđenih u ovoj Direktivi.**

(64) Kako bi se u obzir uzela prekogranična priroda usluga i aktivnosti pružatelja DNS usluga, registara naziva vršnih domena, **subjekata koji pružaju usluge registracije naziva domena za vršnu domenu,** pružatelja mreža za isporuku sadržaja, pružatelja usluga računalstva u oblaku, pružatelja usluga podatkovnog centra i pružatelja digitalnih usluga, samo bi jedna država članica trebala imati nadležnost nad tim subjektima. Nadležnost bi se trebala dodijeliti državi članici u kojoj predmetni subjekt ima glavni poslovni nastan u Uniji. Kriterij poslovnog nastana za potrebe ove Direktive podrazumijeva djelotvorno obavljanje djelatnosti putem stabilnih aranžmana. Pravni oblik takvih aranžmana, bilo kroz podružnicu ili društvo kćer s pravnom osobnošću, nije odlučujući čimbenik u tom pogledu.

Ispunjenje tog kriterija ne bi trebalo ovisiti o tome jesu li mrežni i informacijski sustavi fizički smješteni na određenom mjestu; postojanje i upotreba takvih sustava sami po sebi ne čine takav glavni poslovni nastan i stoga nisu odlučujući kriteriji za određivanje glavnog poslovnog nastana. Glavni poslovni nastan trebao bi biti mjesto na kojem se u Uniji **pretežno** donose odluke o mjerama upravljanja kibersigurnosnim rizicima. To će obično odgovarati mjestu u Uniji na kojem se nalazi središnja uprava poduzeća. Ako **se mjesto na kojem se takve odluke pretežno donose ne može odrediti ili** se takve odluke ne donose u Uniji, trebalo bi smatrati da se glavni poslovni nastan nalazi u državama članicama u kojima subjekt ima poslovnu jedinicu s najvećim brojem zaposlenika u Uniji. Ako usluge pruža grupa poduzeća, glavni poslovni nastan vladajućeg poduzeća trebao bi se smatrati glavnim nastanom grupe poduzeća.

(64a) Ako rekurzivnu DNS uslugu pruža pružatelj javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga samo kao dio usluge pristupa internetu, trebalo bi smatrati da je subjekt u nadležnosti svih država članica u kojima se pružaju njegove usluge.

(64aa) Kako bi se osigurao jasan pregled pružatelja DNS usluga, registara naziva vršnih domena, subjekata koji pružaju usluge registracije naziva domena za vršnu domenu, pružatelja mreže za isporuku sadržaja, pružatelja usluga računalstva u oblaku, pružatelja usluga podatkovnog centra i pružatelja digitalnih usluga diljem Unije u okviru područja primjene ove Direktive, ENISA bi trebala uspostaviti i održavati registar za takve subjekte na temelju obavijesti koje su primile države članice, prema potrebi putem nacionalnih mehanizama za samostalno obavješćivanje. Kako bi se osigurala točnost i potpunost informacija koje bi trebale biti uključene u taj registar, države članice trebale bi dostaviti ENISA-i informacije o tim subjektima koje su dostupne u njihovim nacionalnim registrima. ENISA i države članice trebale bi poduzeti mjere za olakšavanje interoperabilnosti takvih registara, osiguravajući pritom zaštitu povjerljivih ili klasificiranih podataka.

(65) U slučajevima u kojima pružatelj DNS usluga, registar naziva vršnih domena, pružatelj mreža za isporuku sadržaja, pružatelj usluga računalstva u oblaku, pružatelj usluga podatkovnog centra i pružatelj digitalnih usluga koji nemaju poslovni nastan u Uniji nude usluge unutar Unije, trebali bi imenovati predstavnika. Kako bi se utvrdilo nudi li takav subjekt usluge u Uniji, trebalo bi provjeriti može li se zaključiti da subjekt planira ponuditi usluge osobama u jednoj državi članici ili više njih. Sama dostupnost u Uniji internetskih stranica subjekta ili posrednog pružatelja takvih usluga ili e-adrese i drugih podataka za kontakt ili korištenje jezikom koji je općenito u uporabi u trećoj zemlji u kojoj subjekt ima poslovni nastan nedovoljna je za utvrđivanje takve namjere. Međutim, čimbenici kao što su korištenje jezikom ili valutom koji su općenito u uporabi u jednoj državi članici ili više njih, s mogućnošću naručivanja usluga na tom drugom jeziku ili spominjanje kupaca ili korisnika koji se nalaze u Uniji, mogu jasno pokazati da subjekt planira ponuditi usluge u Uniji. Predstavnik bi trebao djelovati u ime subjekta te bi nadležna tijela ili CSIRT-ovi trebali moći stupiti u kontakt s predstavnikom. Subjekt bi trebao pisanim ovlaštenjem izričito imenovati predstavnika da djeluje u njegovo ime s obzirom na obveze tog subjekta prema ovoj Direktivi, što uključuje izvješćivanja o incidentima.

(66) Ako se informacije koje se smatraju klasificiranima u skladu s nacionalnim pravom ili pravom Unije razmjenjuju, dostavljaju ili na drugi način dijele na temelju odredaba ove Direktive, trebalo bi primjenjivati odgovarajuća posebna pravila o postupanju s klasificiranim podacima.

(67) S obzirom na to da kiberprijetnje postaju sve složenije i sofisticiranije, dobre mjere otkrivanja i sprečavanja uvelike ovise o redovitoj razmjeni informacija o prijetnjama i ranjivostima među subjektima. Razmjena informacija doprinosi boljoj informiranosti o kiberprijetnjama, što poboljšava kapacitet subjekata da spriječe da se prijetnje pretvore u stvarne incidente te omogućuje subjektima da bolje ograniče učinke incidenata i učinkovitije se oporave od njih. U nedostatku smjernica na razini Unije čini se da nekoliko čimbenika sprečava takvu razmjenu informacija, osobito nesigurnost u pogledu usklađenosti s pravilima o tržišnom natjecanju i odgovornosti.

(68) Subjekte bi stoga trebalo potaknuti da zajednički iskoriste znanje i praktično iskustvo svakog od njih na strateškoj, taktičkoj i operativnoj razini kako bi poboljšali svoje kapacitete za odgovarajuću procjenu, praćenje, obranu i odgovor na kiberprijetnje. Stoga je potrebno omogućiti razvijanje mehanizama dobrovoljne razmjene informacija na razini Unije. U tu bi svrhu države članice trebale aktivno podupirati i poticati i relevantne subjekte koji nisu obuhvaćeni područjem primjene ove Direktive na sudjelovanje u takvim mehanizmima razmjene informacija. Ti bi se mehanizmi trebali u cijelosti provoditi u skladu s pravilima Unije o tržišnom natjecanju te pravilima prava Unije o zaštiti podataka.

(69) [...]**U** mjeri u kojoj je to izričito nužno i razmjerno za potrebe osiguravanja mrežne i informacijske sigurnosti, **obrada osobnih podataka** koju provode **ključni i važni** subjekti [...] i pružatelji sigurnosnih tehnologija i usluga **mogla bi se smatrati nužnom za usklađenost s pravnom obvezom ili** [...] predstavljati legitimni interes dotičnog voditelja obrade podataka**[...]** kako je navedeno u Uredbi (EU) 2016/679. To bi **moglo** [...] uključivati mjere za sprečavanje, otkrivanje, analizu i odgovor na incidente, mjere za informiranje o određenim kiberprijetnjama, razmjenu informacija u kontekstu uklanjanja i koordiniranog otkrivanja ranjivosti, kao i dobrovoljnu razmjenu informacija o tim incidentima, kiberprijetnjama i ranjivostima, pokazatelje ugroženosti, taktike, tehnike i postupke, kibersigurnosna upozorenja i konfiguracijske alate. Takve mjere mogu zahtijevati obradu [...] **različitih** vrsta osobnih podataka**, kao što su**: IP adrese, jedinstveni lokatori resursa (URL-ovi), nazivi domena i e-adrese. **Obrada osobnih podataka koju provode nadležna tijela, jedinstvene kontaktne točke i CSIRT-ovi trebala bi se utvrditi u nacionalnom pravu i smatrati potrebnom za usklađenost s pravnom obvezom ili izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade podataka kako je navedeno u članku 6. stavku 1. točkama (c) ili (e) Uredbe (EU) 2016/679.**

(69a) Zakonima država članica mogu se utvrditi pravila kojima se nadležnim tijelima, jedinstvenim kontaktnim točkama i CSIRT-ovima, u mjeri u kojoj je to izričito nužno i razmjerno za potrebe osiguravanja sigurnosti mrežnih i informacijskih sustava ključnih i važnih subjekata, omogućuje obrada posebnih kategorija osobnih podataka u skladu s člankom 9. [...] Uredbe (EU) 2016/679, posebno predviđanjem odgovarajućih i posebnih mjera za zaštitu temeljnih prava i interesa fizičkih osoba, uključujući tehnička ograničenja ponovne upotrebe takvih podataka i upotrebe vrhunskih sigurnosnih mjera i mjera za zaštitu privatnosti, kao što je pseudonimizacija ili šifriranje ako anonimizacija može znatno utjecati na svrhu koja se želi ostvariti.

(70) Kako bi se ojačale nadzorne ovlasti i aktivnosti koje pomažu u osiguravanju djelotvorne usklađenosti, ovom bi se Direktivom trebao predvidjeti popis minimalnih nadzornih aktivnosti i sredstava putem kojih nadležna tijela mogu nadzirati ključne i važne subjekte. Usto, ovom Direktivom trebalo bi se utvrditi razlikovanje sustava nadzora između ključnih i važnih subjekata kako bi se osigurala pravedna ravnoteža obveza subjekata i nadležnih tijela. Stoga bi se na ključne subjekte trebao primjenjivati sveobuhvatni sustav nadzora (*ex ante* i *ex post*), dok bi se na važne subjekte trebao primjenjivati blagi sustav nadzora, i to samo *ex post*. U potonjem slučaju to znači da se od važnih subjekata ne bi trebalo **zahtijevati da** [...] sustavno **dokumentiraju** usklađenost sa zahtjevima za upravljanje kibersigurnosnim rizicima, dok bi nadležna tijela trebala primjenjivati reaktivni *ex post* pristup nadzoru te stoga ne bi trebala imati opću obvezu nadzora nad tim subjektima. **Za važne subjekte, *ex post* nadzor može se pokrenuti na temelju dokaza ili bilo kakvih naznaka ili informacija o kojima su nadležna tijela obaviještena i za koje ta tijela smatraju da upućuju na moguću neusklađenost s obvezama utvrđenima u ovoj Direktivi. Na primjer, takvi dokazi, naznake ili informacije mogli bi biti oni koje nadležnim tijelima dostavljaju druga tijela, subjekti, građani, mediji ili drugi izvori, javno dostupne informacije ili bi mogli proizlaziti iz drugih aktivnosti koje provode nadležna tijela pri obavljanju svojih zadaća.**

(70a) Pri provedbi *ex ante* nadzora nadležna tijela trebala bi moći na razmjeran način odlučiti o određivanju prioriteta u pogledu upotrebe nadzornih aktivnosti i sredstava koji su im na raspolaganju. To podrazumijeva da nadležna tijela mogu odlučiti o takvom određivanju prioriteta na temelju nadzornih metodologija koje bi trebale slijediti pristup utemeljen na procjeni riziku. Konkretnije, te metodologije mogle bi uključivati kriterije ili referentna mjerila za razvrstavanje ključnih subjekata u kategorije rizika i odgovarajuće nadzorne aktivnosti i preporučena sredstva po kategoriji rizika, kao što su upotreba, učestalost ili vrsta izravnog nadzora ili ciljanih sigurnosnih revizija ili sigurnosnih pregleda, vrsta informacija koje se trebaju tražiti i razina detalja tih informacija. Takve nadzorne metodologije mogu biti popraćene i programima rada i može ih se redovito ocjenjivati i preispitivati, među ostalim u pogledu aspekata kao što su dodjela resursa i potrebe u vezi s resursima.

(70aa) U odnosu na subjekte javne uprave, nadzorne ovlasti trebalo bi izvršavati u skladu s nacionalnim okvirima i pravnim poretkom. Države članice trebale bi moći odlučiti o uvođenju odgovarajućih, razmjernih i djelotvornih mjera nadzora i provedbe u odnosu na te subjekte.

(70aaa) Kako bi se dokazala usklađenost s određenim mjerama upravljanja kibersigurnosnim rizicima, države članice mogle bi zahtijevati da se ključni i važni subjekti koriste kvalificiranim uslugama povjerenja ili prijavljenim sustavima elektroničke identifikacije na temelju Uredbe (EU) br. 910/2014.

(71) Kako bi provedba bila djelotvorna, potrebno je utvrditi popis minimalnih administrativnih sankcija za kršenje obveza upravljanja kibersigurnosnim rizicima i izvješćivanja predviđenih ovom Direktivom, čime bi se uspostavio jasan i usklađen okvir za takve sankcije širom Unije. Posebna bi se pozornost trebala posvetiti prirodi, ozbiljnosti i trajanju povrede, stvarno prouzročenoj šteti ili nastalim gubicima ili potencijalnoj šteti ili gubicima, namjernom ili nehotičnom obilježju povrede, djelovanjima poduzetima radi sprečavanja ili ublažavanja pretrpljene štete i/ili gubitaka, stupnju odgovornosti ili svim relevantnim prethodnim povredama, stupnju suradnje s nadležnim tijelom kao i bilo kojem drugom otegotnom ili olakotnom čimbeniku. Izricanje sankcija, uključujući upravne novčane kazne, trebalo bi podlijegati odgovarajućim postupovnim zaštitnim mjerama u skladu s općim načelima prava Unije i Poveljom Europske unije o temeljnim pravima, uključujući djelotvornu sudsku zaštitu i zakonito postupanje.

(71a) Odredbama koje se odnose na odgovornost fizičkih osoba koje imaju određene odgovornosti u tom subjektu za kršenje svoje dužnosti osiguravanja usklađenosti s obvezama utvrđenima u ovoj Direktivi ne zahtijeva se od država članica da osiguraju kazneni progon ili građansku odgovornost za štetu prouzročenu takvim kršenjem prema trećim stranama.

(72) Kako bi se osiguralo djelotvorno izvršavanje obveza utvrđenih u ovoj Direktivi, svako bi nadležno tijelo trebalo imati ovlast izricati ili zahtijevati izricanje upravnih novčanih kazni.

(73) Kada se upravne novčane kazne izriču poduzetniku, poduzetnikom bi se u te svrhe trebao smatrati poduzetnik u skladu s člancima 101. i 102. UFEU-a. Ako su upravne novčane kazne izrečene osobama koje nisu poduzeće, pri razmatranju odgovarajućeg iznosa novčane kazne nadzorno tijelo trebalo bi uzeti u obzir opću razinu dohotka u državi članici te ekonomsko stanje osobe. Države članice trebale bi utvrditi i trebaju li i do koje mjere primjenjivati upravne novčane kazne za javna tijela. Izricanje upravne novčane kazne ne utječe na primjenu drugih ovlasti nadležnih tijela ili drugih sankcija utvrđenih u nacionalnim pravilima kojima se prenosi ova Direktiva.

(74) Države članice [...] **mogu** propisati pravila o kaznenim sankcijama za povrede nacionalnih pravila kojima se prenosi ova Direktiva. Međutim, izricanje kaznenih sankcija za povrede takvih nacionalnih pravila i povezanih administrativnih sankcija ne bi smjelo dovesti do kršenja načela *ne bis in idem*, kako ga tumači Sud.

(75) Ako ovom Direktivom nisu usklađene administrativne sankcije ili ako je to potrebno u drugim slučajevima, primjerice u slučajevima teških povreda obveza utvrđenih u ovoj Direktivi, države članice trebale bi uvesti sustav kojim se predviđaju učinkovite, razmjerne i odvraćajuće sankcije. Prirodu tih kaznenih ili administrativnih sankcija trebalo bi odrediti pravom države članice.

(76) Kako bi se dodatno ojačali učinkovitost i odvraćajući učinak sankcija koje se primjenjuju na povrede obveza utvrđenih na temelju ove Direktive, nadležna tijela trebala bi biti ovlaštena za primjenu sankcija koje se sastoje od suspenzije certifikata ili ovlaštenja za dio usluga ili sve usluge koje pruža ključni subjekt i izricanja privremene zabrane fizičkoj osobi da obavlja rukovoditeljske dužnosti. S obzirom na njihovu ozbiljnost i učinak na aktivnosti subjekata te naposljetku na njihove potrošače, takve bi se sankcije trebale primjenjivati samo razmjerno ozbiljnosti povrede i uzimajući u obzir posebne okolnosti svakog slučaja, uključujući namjerna ili nehotična obilježja povrede, kao i djelovanja poduzeta radi sprečavanja ili ublažavanja pretrpljene štete i/ili gubitaka. Takve bi se sankcije trebale primjenjivati samo kao *ultima ratio*, što znači tek nakon što se iscrpe druga odgovarajuća provedbena djelovanja utvrđena ovom Direktivom i samo dok subjekti na koje se primjenjuju ne poduzmu potrebna djelovanja za otklanjanje nedostataka ili dok ne ispune zahtjeve nadležnog tijela na koje se odnose te sankcije. Izricanje takvih sankcija podliježe odgovarajućim postupovnim zaštitnim mjerama u skladu s općim načelima prava Unije i Poveljom Europske unije o temeljnim pravima, uključujući djelotvornu sudsku zaštitu, zakonito postupanje, pretpostavku nedužnosti i pravo na obranu.

(76a) Kako bi se osigurali djelotvoran nadzor i provedba, posebno u slučajevima s prekograničnom dimenzijom, države članice koje su primile zahtjev za uzajamnu pomoć trebale bi, u okvirima zahtjeva, poduzeti odgovarajuće nadzorne i provedbene mjere u odnosu na dotični subjekt koji pruža usluge ili koji ima mrežni i informacijski sustav na njihovu državnom području.

(77) Ovom bi se Direktivom trebala utvrditi pravila suradnje između nadležnih tijela i nadzornih tijela u skladu s Uredbom (EU) 2016/679 radi postupanja u slučaju povreda povezanih s osobnim podacima.

(78) Cilj ove Direktive trebao bi biti osiguravanje visoke razine odgovornosti za mjere upravljanja kibersigurnosnim rizicima i obveze izvješćivanja na razini organizacija. Zbog toga bi upravljačka tijela subjekata koji su obuhvaćeni područjem primjene ove Direktive trebala odobriti mjere u pogledu kibersigurnosnih rizika i nadzirati njihovu provedbu.

(79) Trebalo bi uvesti [...] **sustav uzajamnog** [...] **učenja za doprinos jačanju uzajamnog** povjerenja **i učenju iz dobre prakse i iskustva**, kojim bi se stručnjacima koje su imenovale države članice omogućile [...] **razmjene** o provedbi kibersigurnosnih politika [...]. **Pri provedbi sustava uzajamnog učenja posebnu bi pozornost trebalo posvetiti osiguravanju toga da se njime ne stvara nepotrebno ili nerazmjerno opterećenje za relevantna tijela država članica. Komisija bi trebala istražiti sve mogućnosti za potencijalno jamčenje dovoljnog iznosa financijskih sredstava za pokrivanje troškova koji mogu proizaći iz organizacije misija uzajamnog učenja. Nadalje, u sustavu uzajamnog učenja trebalo bi uzeti u obzir rezultate sličnih mehanizama, kao što je sustav istorazinskog ocjenjivanja mreže CSIRT-ova, dodati vrijednost i izbjeći udvostručavanje. Provedbom sustava uzajamnog učenje ne bi se trebalo dovoditi u pitanje nacionalno pravo ili pravo Unije o zaštiti povjerljivih i klasificiranih informacija. Prije početka krugova uzajamnog učenja, države članice mogu provesti samoprocjenu relevantnih aspekata. Na zahtjev skupine za suradnju ENISA može, prema potrebi, pružiti smjernice o samoprocjeni i relevantne predloške. Države članice mogle bi odlučiti javno objaviti svoja izvješća.**

(80) [...]

(81) Kako bi se osigurali jedinstveni uvjeti za provedbu relevantnih odredaba ove Direktive koje se odnose na postupovne aranžmane potrebne za funkcioniranje skupine za suradnju, tehničke elemente povezane s mjerama upravljanja rizicima ili vrstu informacija, oblik i postupak obavješćivanja o incidentima**, kategorije subjekata od kojih treba zahtijevati da upotrebljavaju određene certificirane IKT proizvode, usluge i postupke**, provedbene ovlasti trebalo bi dodijeliti Komisiji. Te bi ovlasti trebalo izvršavati u skladu s Uredbom (EU) br. 182/2011 Europskog parlamenta i Vijeća[26].

(82) Komisija bi periodično trebala preispitivati ovu Direktivu, uz savjetovanje sa zainteresiranim stranama, posebno u cilju utvrđivanja potrebe za njezinom izmjenom u svjetlu promjene društvenih, političkih, tehnoloških i tržišnih uvjeta.

[26] Uredba (EU) br. 182/2011 Europskog parlamenta i Vijeća od 16. veljače 2011. o utvrđivanju pravila i općih načela u vezi s mehanizmima nadzora država članica nad izvršavanjem provedbenih ovlasti Komisije (SL L 55, 28.2.2011., str. 13.).

(83) S obzirom na to da cilj ove Direktive, to jest postizanje visoke zajedničke razine kibersigurnosti u Uniji, ne mogu dostatno ostvariti države članice, nego se zbog učinka djelovanja on na bolji način može ostvariti na razini Unije, Unija može donijeti mjere u skladu s načelom supsidijarnosti utvrđenim u članku 5. Ugovora o Europskoj uniji. U skladu s načelom proporcionalnosti utvrđenim u tom članku, ova Direktiva ne prelazi ono što je potrebno za ostvarivanje tog cilja.

(84) Ovom Direktivom poštuju se temeljna prava i načela priznata Poveljom Europske unije o temeljnim pravima, posebno pravo na poštovanje privatnog života i komuniciranja, zaštitu osobnih podataka, slobodu poduzetništva, pravo na vlasništvo, pravo na djelotvoran pravni lijek pred sudom i pravo na saslušanje. Ova Direktiva trebala bi se provoditi u skladu s tim pravima i načelima,

DONIJELI SU OVU DIREKTIVU:

POGLAVLJE I.

Opće odredbe

Članak 1.

Predmet

1. Ovom se Direktivom utvrđuju mjere kojima se osigurava visoka zajednička razina kibersigurnosti unutar Unije **kako bi se poboljšalo funkcioniranje unutarnjeg tržišta**.

2. U tu svrhu, ovom se Direktivom:

   (a) utvrđuju obveze država članica da donesu nacionalne strategije za kibersigurnost, imenuju nadležna nacionalna tijela, jedinstvene kontaktne točke i timove za odgovor na računalne sigurnosne incidente (CSIRT-ovi);

   (b) utvrđuju obveze upravljanja kibersigurnosnim rizicima i izvješćivanja o njima za vrste subjekata [...] iz priloga **I. i II.** [...];

   (c) utvrđuju **pravila i** obveze u pogledu razmjene informacija o kibersigurnosti.

Članak 2.

Područje primjene

1. Ova Direktiva primjenjuje se na vrste javnih i privatnih subjekata **navedenih** [...] u [...] prilozi**ma I. i II.** [...] **koji ispunjavaju ili premašuju gornje granice za srednja poduzeća** [...] u smislu Preporuke Komisije 2003/361/EZ[27]. **Članak 3. stavak 4. i članak 6. stavak 2. drugi i treći podstavak Priloga toj preporuci ne primjenjuje se za potrebe ove Direktive.**

2. [...]**N**eovisno o [...] veličini **subjekata iz stavka 1.**, ova Direktiva primjenjuje se i: [...]

   (a) ako usluge pruža jedan od sljedećih subjekata:

      (i) **pružatelji** javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga iz točke 8. Priloga I.;

      (ii) **kvalificirani pružatelji usluga povjerenja iz točke XX. Priloga I.;**

      (iii) **iii. nekvalificirani pružatelji usluga povjerenja iz točke XX. Priloga I.;**

      (iv) iv. registri naziva vršnih domena [...] iz točke 8. Priloga I.;

   (b) [...]

---

27 Preporuka Komisije 2003/361/EZ od 6. svibnja 2003. o definiciji mikropoduzeća te malih i srednjih poduzeća (SL L 124, 20.5.2003., str. 36.).

(c) ako je subjekt jedini pružatelj **u državi članici** usluge [...] **koja je ključna za održavanje kritičnih društvenih ili gospodarskih djelatnosti**;

(d) ako bi mogući prekid usluge koju pruža subjekt mogao [...] **znatno** utjecati na javnu sigurnost, javnu zaštitu ili javno zdravlje;

(e) ako bi mogući prekid usluge koju pruža subjekt mogao prouzročiti [...] **znatne** sistemske rizike, posebno u sektorima u kojima bi takav prekid mogao imati prekogranični učinak;

(f) [...];

(g) ako se utvrdi da je subjekt kritični subjekt na temelju Direktive (EU) XXXX/XXXX Europskog parlamenta i Vijeća[28] [Direktiva o otpornosti kritičnih subjekata] **[**ili subjekt istovjetan kritičnom subjektu na temelju članka 7. te direktive**]**.

2.a Neovisno o njihovoj veličini, ova Direktiva primjenjuje se i na tijela središnje državne uprave koja su kao takva priznata u državi članici u skladu s nacionalnim pravom i navedena u točki 9. Priloga I. Države članice mogu utvrditi da se ova Direktiva primjenjuje i na tijela javne uprave na regionalnoj i lokalnoj razini.

28 [Upisati puni naslov i upućivanje na objavu u SL-u kada budu poznati.]

3. [...]

Ovom Direktivom ne dovode se u pitanje odgovornosti država članica za zaštitu nacionalne sigurnosti ili njihove ovlasti za zaštitu drugih ključnih državnih funkcija, uključujući osiguravanje teritorijalne cjelovitosti države i održavanje javnog poretka.

3.a (1) Ova se Direktiva ne primjenjuje na:

(a) subjekte koji nisu obuhvaćeni područjem primjene prava Unije i u svakom slučaju na sve subjekte koji uglavnom obavljaju aktivnosti u području obrane, nacionalne sigurnosti, javne sigurnosti ili izvršavanja zakonodavstva bez obzira na to koji subjekt obavlja te aktivnosti i je li riječ o javnom ili privatnom subjektu, ne dovodeći u pitanje točku (2);

(b) subjekte **koji obavljaju aktivnosti u područjima sudstva, parlamente i središnje banke.** [...]

(2) Ako tijela javne uprave obavljaju aktivnosti u tim područjima samo kao dio svojih ukupnih aktivnosti, ona se u cijelosti isključuju iz područja primjene ove Direktive.

3.aa Ova se Direktiva ne primjenjuje na:

(i) aktivnosti subjekata koji nisu obuhvaćeni područjem primjene prava Unije i u svakom slučaju sve aktivnosti koje se odnose na nacionalnu sigurnost ili obranu, bez obzira na to koji subjekt obavlja te aktivnosti i je li riječ o javnom ili privatnom subjektu;

(ii) aktivnosti subjekata u sudstvu, parlamentima, središnjim bankama i u području javne sigurnosti, uključujući subjekte javne uprave koji obavljaju aktivnosti izvršavanja zakonodavstva u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenopravnih sankcija.

3.aaa Obveze utvrđene u ovoj Direktivi ne podrazumijevaju dostavu informacija čije je otkrivanje u suprotnosti s bitnim interesima država članica u pogledu nacionalne sigurnosti, javne sigurnosti ili obrane.

3.aaaa Ovom Direktivom ne dovodi se u pitanje pravo Unije o zaštiti osobnih podataka, osobito Uredba (EU) 2016/679 i Direktiva 2002/58/EZ.

3.b Ova Direktiva ne primjenjuje se na subjekte koji su izuzeti iz Uredbe (EU) XXXX/XXXX Europskog parlamenta i Vijeća [Uredba DORA] u skladu s člankom 2. stavkom 4. Uredbe DORA.

4. Ova Direktiva primjenjuje se ne dovodeći u pitanje [...][29] [...] direktive 2011/93/EU[30] i 2013/40/EU[31] Europskog parlamenta i Vijeća.

5. Ne dovodeći u pitanje članak 346. UFEU-a, informacije koje se smatraju povjerljivima na temelju pravila Unije i nacionalnih pravila, kao što su pravila o poslovnoj tajni, razmjenjuju se s Komisijom i drugim relevantnim tijelima **u skladu s ovom Direktivom** samo u slučaju kad je takva razmjena nužna za primjenu ove Direktive. Razmijenjene informacije ograničuju se na ono što je relevantno i razmjerno svrsi te razmjene. Pri razmjeni informacija čuva se njihova povjerljivost te se štite sigurnost i komercijalni interesi ključnih ili važnih subjekata.

---

29 [...]

30 Direktiva 2011/93/EU Europskog parlamenta i Vijeća od 13. prosinca 2011. o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i dječje pornografije, te o zamjeni Okvirne odluke Vijeća 2004/68/PUP (SL L 335, 17.12.2011., str. 1.).

31 Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP (SL L 218, 14.8.2013., str. 8.).

Članak 2.a

Ključni i važni subjekti

1. Među subjektima na koje se ova Direktiva primjenjuje, sljedeći se smatraju ključnima:

(i) vrsta subjekata predviđenih u točkama od 1. do 8.a Priloga I. ovoj Direktivi koji premašuju gornje granice za srednja poduzeća kako je definirano u Preporuci Komisije 2003/361/EZ;

(ii) srednja poduzeća iz članka 2. stavka 2. točke (a) podtočke i.;

(iii) subjekti iz članka 2. stavka 2. točke (a) podtočaka ii. i iv. ove Direktive, bez obzira na njihovu veličinu;

(iv) subjekti iz članka 2. stavka 2. točke (g) ove Direktive, bez obzira na njihovu veličinu;

(v) ako su ih osnovale države članice, subjekti koje su države članice prije stupanja na snagu ove Direktive utvrdile kao operatore ključnih usluga u skladu s Direktivom (EU) 2016/1148 ili nacionalnim pravom;

(vi) subjekti koji premašuju gornju granicu za srednja poduzeća kako je definirano u Preporuci Komisije2003/361/EZ koji su vrsta predviđena u Prilogu II. i za koje države članice odrede da su ključni na temelju kriterija iz članka 2. stavka 2. točaka od (c) do (e);

(vii) srednji subjekti u smislu Preporuke Komisije 2003/361/EZ za koje države članice odrede da su ključni na temelju kriterija iz članka 2. stavka 2. točaka od (c) do (e);

(viii) mikrosubjekti ili mali subjekti u smislu Preporuke Komisije 2003/361/EZ predviđeni u stavku 2. točki (a) podtočki i. ili utvrđeni na temelju stavka 2. točaka od (c) do (e) ovog članka za koje države članice odrede da su ključni na temelju nacionalnih procjena rizika.

2. Među subjektima na koje se ova Direktiva primjenjuje, sljedeći se smatraju važnima:

(i) vrsta subjekata predviđenih u Prilogu I. ovoj Direktivi koji se smatraju srednjim poduzećima u smislu Preporuke Komisije 2003/361/EZ i vrsta subjekata predviđenih u Prilogu II. koji ispunjavaju ili premašuju gornje granice za srednja poduzeća u smislu Preporuke Komisije 2003/361/EZ[32];

(ii) subjekti iz članka 2. stavka 2. točke (a) podtočke iii. ove Direktive, bez obzira na njihovu veličinu;

(iii) mali subjekti i mikrosubjekti iz članka 2. stavka 2. točke (a) podtočke i.;

(iv) mali subjekti i mikrosubjekti za koje države članice odrede da su važni subjekti na temelju članka 2. stavka 3. točaka od (c) do (e).

---

[32] **Preporuka Komisije 2003/361/EZ od 6. svibnja 2003. o definiciji mikropoduzeća te malih i srednjih poduzeća (SL L 124, 20.5.2003., str. 36.).**

Članak 2.a

Mehanizmi obavješćivanja

1. **Države članice mogu uspostaviti nacionalni mehanizam za samostalno obavješćivanje kojim se od svih subjekata obuhvaćenih područjem primjene ove Direktive zahtijeva da nadležnim tijelima iz ove Direktive ili tijelima koja su u tu svrhu imenovale države članice dostave barem svoje ime, adresu i podatke za kontakt te sektor u kojem posluju ili vrstu usluge koju pružaju i, prema potrebi, popis država članica u kojima pružaju usluge koje podliježu ovoj Direktivi.**

2. Države članice [...] dostavljaju Komisiji, **u odnosu na subjekte koje su utvrdile na temelju članka 2. stavka 2. točaka od (b) do (e), barem relevantne informacije o broju utvrđenih subjekata, sektoru kojem pripadaju ili vrsti usluge koju pružaju u skladu s prilozima, te određenu odredbu ili odredbe članka 2. stavka 2. na temelju kojih su utvrđeni do [12 mjeseci nakon roka za prenošenje ove Direktive].** Države članice redovito i najmanje svake dvije godine preispituju [...] **ove informacije** [...] te ih prema potrebi ažuriraju.

Članak 2.b

Sektorski akti Unije

1. Ako se [...] **sektorskim pravnim** aktima [...] **Unije** od ključnih ili važnih subjekata zahtijeva donošenje mjera upravljanja kibersigurnosnim rizicima ili obavješćivanje o **ozbiljnim** incidentima ili [...] kiberprijetnjama i ako su ti zahtjevi po učinku barem istovjetni obvezama utvrđenima u ovoj Direktivi, relevantne odredbe ove Direktive, **uključujući odredbe o nadzoru i provedbi utvrđene u poglavlju VI.,** ne primjenjuju se na **te subjekte**. **Ako sektorski pravni akti Unije ne obuhvaćaju sve subjekte u određenom sektoru koji su obuhvaćeni područjem primjene ove Direktive, relevantne odredbe ove Direktive i dalje se primjenjuju na subjekte koji nisu obuhvaćeni tim sektorskim odredbama.**

2. Za zahtjeve iz stavka 1. ovog članka smatra se da su po učinku istovjetni obvezama utvrđenima u ovoj Direktivi ako je odgovarajućim sektorskim pravnim aktom Unije predviđen trenutačan i neposredan pristup, prema potrebi automatski i izravan, obavijestima o incidentima koje dostavljaju nadležna tijela na temelju ove Direktive ili imenovani CSIRT-ovi i ako:

(a) mjere upravljanja kibersigurnosnim rizicima barem su istovjetne po učinku mjerama utvrđenima u članku 18. stavcima 1. i 2. ove Direktive; ili

(b) zahtjevi za obavješćivanje o ozbiljnim incidentima barem su istovjetni po učinku zahtjevima utvrđenima u članku 20. stavcima od 1. do 6.

3. Komisija periodički preispituje primjenu zahtjeva s istovjetnim učinkom predviđenih u stavcima 1. i 2. ovog članka u odnosu na sektorske odredbe pravnih akata Unije. Komisija se pri pripremi tih periodičkih preispitivanja savjetuje sa skupinom za suradnju i ENISA-om.

Članak 3.

Minimalno usklađivanje

Ne dovodeći u pitanje svoje ostale obveze na temelju prava Unije, države članice mogu [...] donijeti ili zadržati odredbe kojima se osigurava viša razina kibersigurnosti **u područjima obuhvaćenima ovom Direktivom**.

Članak 4.

Definicije

Za potrebe ove Direktive, primjenjuju se sljedeće definicije:

(1) „mrežni i informacijski sustav” znači:

(a) elektronička komunikacijska mreža u smislu članka 2 stavka 1. Direktive (EU) 2018/1972;

(b) svaki uređaj ili skupina povezanih ili srodnih uređaja, od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka;

(c) digitalni podaci koji se pohranjuju, obrađuju, dobivaju ili prenose elementima opisanima u točkama (a) i (b) u svrhu njihova rada, uporabe, zaštite i održavanja;

(2) „sigurnost mrežnih i informacijskih sustava” znači sposobnost mrežnih i informacijskih sustava da na određenoj razini pouzdanosti odolijevaju svim **događajima** koji **mogu** ugroziti **[...]** dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih ili prenesenih ili obrađenih podataka ili usluga koje ti mrežni i informacijski sustavi nude ili kojima omogućuju pristup;

(2a) „elektroničke komunikacijske usluge” znači elektroničke [...] komunikacijske usluge u smislu članka 2 stavka 4. Direktive (EU) 2018/1972;

(3) „kibersigurnost” znači kibersigurnost u smislu članka 2. stavka 1. Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća[33];

(4) „nacionalna strategija za kibersigurnost” znači usklađen okvir države članice kojim se pružaju smjernice za ostvarenje strateških ciljeva i prioriteta **u području** [...] **kibersigurnosti** [...] u toj državi članici;

(5) „incident” znači svaki događaj koji ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili [...] usluga koje mrežni i informacijski sustavi nude ili kojima omogućuju pristup;

(5a) „kiberincident velikih razmjera” znači incident s ozbiljnim učinkom na barem dvije države članice ili čiji učinci premašuju sposobnost države članice da na njega odgovori;

---

33 Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15.).

(6) „rješavanje incidenta” znači sve radnje i postupci čiji je cilj otkrivanje, analiza i zaustavljanje incidenta te odgovor na njega;

(6a) „rizik” znači mogućnost gubitka ili poremećaja prouzročenog incidentom i izražen je kao kombinacija opsega takvog gubitka ili poremećaja i vjerojatnosti pojave tog incidenta;

(7) „kiberprijetnja” znači kiberprijetnja u smislu članka 2. stavka 8. Uredbe (EU) 2019/881;

(7**a**) **„ozbiljna kiberprijetnja” znači kiberprijetnja za koju se, na temelju njezinih tehničkih obilježja, može pretpostaviti da može ozbiljno utjecati na mrežne i informacijske sustave nekog subjekta ili njegovih korisnika uzrokovanjem znatnih materijalnih ili nematerijalnih gubitaka;**

(8) „ranjivost” znači slabost, osjetljivost ili nedostatak nekog IKT resursa ili sustava [...] koje kiberprijetnja može iskoristiti;

(8a) „izbjegnuti incident” znači neki događaj koji je mogao prouzročiti štetu mrežnim i informacijskim sustavima nekog subjekta ili njegovih korisnika, ali je njegovo nastajanje uspješno spriječeno;

(9) „predstavnik” znači svaka fizička ili pravna osoba s poslovnim nastanom u Uniji koju su i. pružatelj DNS usluga, registar naziva vršnih domena, pružatelj usluga računalstva u oblaku, pružatelj usluga podatkovnog centra, pružatelj mreža za isporuku sadržaja kako je navedeno u točki 8. Priloga I. ili ii. subjekti iz točke [...] **6.** Priloga II. koji nemaju poslovni nastan u Uniji izričito imenovali da djeluje u njihovo ime i kojoj se nacionalno nadležno tijelo ili CSIRT mogu obratiti umjesto tom subjektu u pogledu obveza tog subjekta na temelju ove Direktive;

(10) „norma” znači norma u smislu članka 2. stavka 1. Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća[34];

(11) „tehnička specifikacija” znači tehnička specifikacija u smislu članka 2. stavka 4. Uredbe (EU) br. 1025/2012;

(12) „središte za razmjenu internetskog prometa (IXP)” znači mrežni instrument koji omogućuje međusobno povezivanje više od dviju neovisnih mreža (autonomnih sustava), prvenstveno u svrhu olakšavanja razmjene internetskog prometa; IXP omogućuje međusobno povezivanje samo za autonomne sustave; za IXP nije potrebno da internetski promet između bilo kojih dvaju autonomnih sustava sudionika prođe kroz bilo koji treći autonomni sustav, on takav promet ne mijenja i ne utječe na njega ni na koji drugi način;

(13) „sustav naziva domena (DNS)” znači hijerarhijsko raspoređeni sustav imenovanja koji krajnjim korisnicima omogućuje pristup uslugama i resursima na internetu;

(14) „pružatelj DNS usluga” znači subjekt koji pruža rekurzivne ili mjerodavne usluge razlučivanja naziva domena **za** [...] **upotrebu od strane trećih strana, uz iznimku korijenskih poslužitelja naziva** [...];

---

34 Uredba (EU) br. 1025/2012 Europskog parlamenta i Vijeća od 25. listopada 2012. o europskoj normizaciji, o izmjeni direktiva Vijeća 89/686/EEZ i 93/15/EEZ i direktiva 94/9/EZ, 94/25/EZ, 95/16/EZ, 97/23/EZ, 98/34/EZ, 2004/22/EZ, 2007/23/EZ, 2009/23/EZ i 2009/105/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Odluke Vijeća 87/95/EEZ i Odluke br. 1673/2006/EZ Europskog parlamenta i Vijeća (SL L 316, 14.11.2012., str. 12.).

(15) „registar naziva vršnih domena” znači subjekt kojem je delegirana određena vršna domena i koji je odgovoran za upravljanje njome, uključujući registraciju naziva domena u okviru vršne domene i tehničko upravljanje vršnom domenom zajedno s upravljanjem njezinim poslužiteljima naziva, održavanje njezinih baza podataka i distribuciju datoteka iz zone vršne domene u poslužitelje naziva, **a pritom su isključene situacije u kojima se registar koristi nazivima vršnih domena samo za vlastitu upotrebu**;

(15a) „subjekti koji pružaju usluge registracije naziva domena za vršnu domenu” znači registri naziva vršnih domena, registrari za nazive vršnih domena i zastupnici registrara kao što su preprodavatelji i pružatelju usluga proxy poslužitelja;

(16) „digitalna usluga” znači usluga u smislu članka 1. stavka 1. točke (b) Direktive (EU) 2015/1535 Europskog parlamenta i Vijeća[35];

(16a) „usluge povjerenja” znači usluge povjerenja u smislu članka 3. stavka 16. Uredbe (EU) br. 910/2014;

[35] Direktiva (EU) 2015/1535 Europskog parlamenta i Vijeća od 9. rujna 2015. o utvrđivanju postupka pružanja informacija u području tehničkih propisa i pravila o uslugama informacijskog društva (SL L 241, 17.9.2015., str. 1.).

(16b) „kvalificirani pružatelj usluga povjerenja” znači kvalificirani pružatelj usluga povjerenja u smislu članka 3. stavka 20. Uredbe (EU) 910/2014;

(17) „internetsko tržište” znači digitalna usluga u smislu članka 2. točke (n) Direktive 2005/29/EZ Europskog parlamenta i Vijeća[36];

(18) „internetska tražilica” znači digitalna usluga u smislu članka 2. stavka 5. Uredbe (EU) 2019/1150 Europskog parlamenta i Vijeća[37];

(19) „usluga računalstva u oblaku” znači digitalna usluga koja omogućuje administraciju na zahtjev i široki daljinski pristup nadogradivom i elastičnom skupu djeljivih [...] računalnih resursa**, među ostalim kad se one distribuiraju na nekoliko lokacija**;

(20) „usluga podatkovnog centra” znači usluga koja uključuje strukture ili skupine struktura namijenjenih centraliziranom smještaju, međupovezivanju i radu opreme informacijskih tehnologija i mreža za usluge pohrane, obrade i prijenosa podataka, uključujući sve objekte i infrastrukturu za distribuciju električne energije i kontrolu okoliša;

---

36 Direktiva 2005/29/EZ Europskog parlamenta i Vijeća od 11. svibnja 2005. o nepoštenoj poslovnoj praksi poslovnog subjekta u odnosu prema potrošaču na unutarnjem tržištu i o izmjeni Direktive Vijeća 84/450/EEZ, direktiva 97/7/EZ, 98/27/EZ i 2002/65/EZ Europskog parlamenta i Vijeća, kao i Uredbe (EZ) br. 2006/2004 Europskog parlamenta i Vijeća („Direktiva o nepoštenoj poslovnoj praksi”) (SL L 149, 11.6.2005., str. 22.).

37 Uredba (EU) 2019/1150 Europskog parlamenta i Vijeća od 20. lipnja 2019. o promicanju pravednosti i transparentnosti za poslovne korisnike usluga internetskog posredovanja (SL L 186, 11.7.2019., str. 57.).

(21) „mreža za isporuku sadržaja” znači mreža zemljopisno raspoređenih poslužitelja u svrhu osiguravanja visoke dostupnosti, pristupačnosti ili brze isporuke digitalnog sadržaja i usluga korisnicima interneta u ime pružateljâ sadržaja i usluga;

(22) „platforma za usluge društvenih mreža” znači platforma koja krajnjim korisnicima omogućuje da se međusobno povežu, dijele i otkrivaju sadržaj te da komuniciraju na više uređaja, a posebno putem razgovora, objava, videozapisa i preporuka[...];

(23) „subjekt javne uprave” znači subjekt koji je **kao takav priznat u državi članici u skladu s nacionalnim pravom i** [...] koji ispunjava sljedeće kriterije:

(a) uspostavljen je u svrhu zadovoljavanja potreba od općeg interesa i nije industrijske ili komercijalne naravi;

(b) ima pravnu osobnost **ili ima zakonsko pravo djelovati u ime drugog subjekta s pravnom osobnošću**;

(c) većim dijelom financiraju ga državna, regionalna ili druga javnopravna tijela; ili podliježe upravljačkom nadzoru tih tijela; ili ima upravni, upravljački ili nadzorni odbor u kojem su više od polovine članova imenovala državna, regionalna ili druga javnopravna tijela;

(d) ovlašten je fizičkim ili pravnim osobama upućivati upravne ili regulatorne odluke koje utječu na njihova prava u prekograničnom kretanju osoba, robe, usluga ili kapitala.

(24) „subjekt” znači svaka fizička ili pravna osoba osnovana i priznata kao takva na temelju nacionalnog prava mjesta svojeg poslovnog nastana, koja može, djelujući u vlastito ime, ostvarivati prava i preuzimati obveze;

(a) (25) „ključni subjekt” znači svaka vrsta subjekta [...] **predviđena u Prilogu I. i određena kao „ključna” u skladu s člankom 2.a stavkom 1.**;

(b) (26) „važni subjekt” znači svaka vrsta subjekta [...] **predviđena u prilozima I. i II. te određena kao „važna” u skladu s člankom 2.a stavkom 2.**;

(c) **(26a) „IKT proizvod” znači IKT proizvod u smislu članka 2. stavka 12. Uredbe (EU) 2019/881;**

(d) **(26aa) „IKT usluga” znači IKT usluga u smislu članka 2. stavka 13. Uredbe (EU) 2019/881;**

(e) **(26ab) „IKT proces” znači IKT proces u smislu članka 2. stavka 14. Uredbe (EU) 2019/881;**

(f) **(26ac) „pružatelj upravljanih usluga” znači svaki subjekt koji pruža usluge, kao što su mreža, aplikacija, infrastruktura i sigurnost, stalnim i redovitim upravljanjem, potporom i aktivnom administracijom u prostorima klijenata, u svojem podatkovnom centru pružatelja upravljanih usluga (domaćin) ili u podatkovnom centru treće strane;**

(g) **(26ad) „pružatelj upravljanih sigurnosnih usluga” znači svaki subjekt koji osigurava eksternalizirano praćenje sigurnosnih uređaja i sustava te upravljanje njima. Zajedničke usluge uključuju upravljani vatrozid, otkrivanje neovlaštenog ulaska, virtualnu privatnu mrežu, pregledavanje ranjivosti i antivirusne usluge.**

- **To uključuje i upotrebu centara za sigurnosne operacije visoke dostupnosti (iz vlastitih objekata ili iz drugih pružatelja podatkovnog centra) za pružanje usluga 24 sata dnevno sedam dana u tjednu namijenjenih smanjenju broja osoblja za operativnu sigurnost koje poduzeće treba zaposliti, osposobiti i zadržati radi održavanja prihvatljive razine sigurnosti.**

POGLAVLJE II.

Koordinirani regulatorni okviri za kibersigurnost

Članak 5.

Nacionalna strategija za kibersigurnost

(h) 1. Svaka država članica donosi nacionalnu strategiju za kibersigurnost kojom se utvrđuju strateški ciljevi i odgovarajuće mjere politike i regulatorne mjere radi postizanja i održavanja visoke razine kibersigurnosti. Nacionalna strategija za kibersigurnost posebno uključuje sljedeće:

(a) [...] ciljeve i prioritete strategije država članica za kibersigurnost;

(b) upravljački okvir za postizanje tih ciljeva i prioriteta, uključujući politike iz stavka 2. te uloge i odgovornosti različitih tijela i aktera uključenih u provedbu strategije [...];

(c) [...] **smjernice** radi utvrđivanja relevantne imovine i **procjene** kibersigurnosnih rizika u toj državi članici [...];

(d) određivanje mjera za osiguravanje pripravnosti, odgovora i oporavka od incidenata, uključujući suradnju javnog i privatnog sektora;

(e) [...]

(f) okvir politike za bolju koordinaciju između nadležnih tijela iz ove Direktive i Direktive (EU) XXXX/XXXX Europskog parlamenta i Vijeća[38] [Direktiva o otpornosti kritičnih subjekata] u svrhu razmjene informacija o **kibersigurnosnim rizicima,** [...] kiberprijetnjama **i kiberincidentima, kao i o rizicima, prijetnjama i incidentima izvan kiberprostora** te**, prema potrebi,** izvršavanja nadzornih zadaća.

(fa) okvir politike za koordinaciju i suradnju između nadležnih tijela iz ove Direktive i nadležnih tijela određenih na temelju sektorskog zakonodavstva.

2. U okviru nacionalne strategije za kibersigurnost države članice posebno donose sljedeće politike:

(a) politiku za rješavanje kibersigurnosnih pitanja u lancu opskrbe IKT proizvodima i uslugama kojima se koriste [...] subjekti za pružanje svojih usluga;

(b) **politiku** [...] za uključivanje i određivanje kibersigurnosnih zahtjeva za IKT proizvode i usluge u području javne nabave**, uključujući kibersigurnosnu certifikaciju**;

(c) politiku **za upravljanje ranjivostima, koja obuhvaća promicanje i olakšavanje** [...] **dobrovoljnog** koordiniranog otkrivanja ranjivosti u smislu članka 6. **stavka 1.**;

(d) politiku koja se odnosi na održavanje opće dostupnosti**,** [...] cjelovitosti **i povjerljivosti** javne jezgre otvorenog interneta;

(e) politiku promicanja i razvoja **obrazovanja i osposobljavanja,** vještina, informiranja te istraživačkih i razvojnih inicijativa u području kibersigurnosti;

---

38 *[Upisati puni naslov i upućivanje na objavu u SL-u kada budu poznati.]*

(f) politiku potpore akademskim i istraživačkim institucijama u razvoju alata za kibersigurnost i sigurne mrežne infrastrukture;

(g) politiku, relevantne postupke i odgovarajuće alate za razmjenu informacija u cilju podupiranja dobrovoljne razmjene informacija o kibersigurnosti među poduzećima u skladu s pravom Unije;

(h) politiku za rješavanje posebnih potreba MSP-ova, osobito onih izuzetih iz područja primjene ove Direktive, u pogledu smjernica i potpore za poboljšanje njihove otpornosti na kiberprijetnje.

3. Države članice obavješćuju Komisiju o svojim nacionalnim strategijama za kibersigurnost u roku od tri mjeseca od njihova donošenja. **Pritom** države članice mogu izostaviti **elemente strategije koji se odnose na** [...] nacionalnu sigurnost.

4. Države članice **redovito, a** najmanje svakih [...] **pet** godina ocjenjuju svoje nacionalne strategije za kibersigurnost na temelju ključnih pokazatelja uspješnosti te ih prema potrebi izmjenjuju. Agencija Europske unije za kibersigurnost (ENISA) pomaže državama članicama, na njihov zahtjev, u razvoju nacionalne strategije i ključnih pokazatelja uspješnosti za ocjenjivanje strategije.

Članak 6.

Koordinirano otkrivanje ranjivosti i europski registar ranjivosti

1. Svaka država članica imenuje jednog od svojih CSIRT-ova iz članka 9. koordinatorom za potrebe koordiniranog otkrivanja ranjivosti. Imenovani CSIRT djeluje kao pouzdani posrednik koji, prema potrebi, olakšava interakciju između subjekta koji podliježe obvezi obavješćivanja, **potencijalnog vlasnika ranjivosti** i proizvođača ili pružatelja IKT proizvoda ili IKT usluga. **Svaka fizička ili pravna osoba imenovanom CSIRT-u može prijaviti, po mogućnosti anonimno, ranjivosti iz članka 4. stavka 8. Imenovani CSIRT osigurava savjesno daljnje postupanje na temelju prijave i povjerljivost identiteta osobe koja prijavljuje ranjivost.** Ako bi prijavljena ranjivost [...] **potencijalno mogla imati znatan učinak na subjekte u više država članica**, imenovani CSIRT svake dotične države članice **prema potrebi** surađuje s **drugim imenovanim CSIRT-ovima u okviru** mreže CSIRT-ova.

2. ENISA razvija i vodi europski registar ranjivosti**, pritom se savjetujući sa skupinom za suradnju**. U tu svrhu ENISA uspostavlja i održava odgovarajuće informacijske sustave, politike i postupke osobito kako bi omogućila važnim i ključnim subjektima te njihovim dobavljačima mrežnih i informacijskih sustava da otkriju i registriraju**, na dobrovoljnoj osnovi, javnosti poznate** ranjivosti prisutne u IKT proizvodima ili IKT uslugama te da svim zainteresiranim stranama omoguće pristup informacijama o ranjivostima sadržanima u registru. Registar osobito uključuje informacije o ranjivosti, IKT proizvodu ili IKT uslugama na koje ona utječe i ozbiljnosti ranjivosti s obzirom na okolnosti u kojima se može iskoristiti, dostupnosti odgovarajućih popravaka i, ako nisu dostupni, smjernica **koje izdaju nacionalna nadležna tijela ili CSIRT-ovi** i koje su namijenjene korisnicima ranjivih proizvoda i usluga u vezi s načinom na koji se mogu ublažiti rizici koji proizlaze iz otkrivenih ranjivosti. **ENISA osigurava da se u okviru europskog registra ranjivosti upotrebljava sigurna i otporna komunikacijska i informacijska infrastruktura.**

Članak 7.

Nacionalni okviri za upravljanje kiberkrizama

1. Svaka država članica imenuje jedno ili više nadležnih tijela odgovornih za upravljanje **kiber**incidentima i **kiber**krizama velikih razmjera. Države članice osiguravaju da nadležna tijela imaju odgovarajuće resurse za djelotvorno i učinkovito obavljanje zadaća koje su im dodijeljene. **Države članice osiguravaju usklađenost s postojećim okvirima za opće upravljanje krizama.**

2. Svaka država članica utvrđuje kapacitete, sredstva i postupke koji se mogu primijeniti u slučaju krize za potrebe ove Direktive.

3. Svaka država članica donosi nacionalni plan za odgovor na kiberincidente i kiberkrize u kojem se utvrđuju ciljevi i načini upravljanja kiberincidentima i kiberkrizama velikih razmjera. Planom se osobito utvrđuje sljedeće:

   (a) ciljevi mjera i aktivnosti za nacionalnu pripravnost;

   (b) zadaće i odgovornosti nacionalnih nadležnih tijela;

   (c) postupci upravljanja krizama**, uključujući njihovu integraciju u opći nacionalni okvir za upravljanje krizama,** i kanali za razmjenu informacija;

   (d) mjere pripravnosti, uključujući redovite vježbe i aktivnosti osposobljavanja;

   (e) relevantne javne i privatne [...] strane i uključena infrastruktura;

   (f) nacionalni postupci i dogovori između relevantnih nacionalnih vlasti i tijela kako bi se osiguralo djelotvorno sudjelovanje država članica u koordiniranom upravljanju kiberincidentima i kiberkrizama velikih razmjera na razini Unije i njihova potpora takvom upravljanju.

4. Države članice obavješćuju Komisiju o imenovanju svojih nadležnih tijela iz stavka 1. i dostavljaju **relevantne informacije o zahtjevima iz stavka 3. ovog članka o** njihovim nacionalnim planovima za odgovor na kiberincidente i kiberkrize [...] u roku od tri mjeseca od takvog imenovanja i donošenja tih planova. Države članice mogu izostaviti određene informacije [...] ako je to nužno i u mjeri u kojoj je to nužno za nacionalnu sigurnost**, javnu sigurnosti ili obranu**.

Članak 8.

Nacionalna nadležna tijela i jedinstvene kontaktne točke

1. Svaka država članica imenuje jedno ili više nadležnih tijela odgovornih za kibersigurnost i nadzorne zadaće iz poglavlja VI. ove Direktive. Države članice u tu svrhu mogu imenovati postojeće tijelo ili postojeća tijela.

2. Nadležna tijela iz stavka 1. prate primjenu ove Direktive na nacionalnoj razini.

3. Svaka država članica imenuje jednu nacionalnu jedinstvenu kontaktnu točku za kibersigurnost („jedinstvena kontaktna točka”). Ako država članica imenuje samo jedno nadležno tijelo, to nadležno tijelo ujedno je jedinstvena kontaktna točka te države članice.

4. Svaka jedinstvena kontaktna točka izvršava funkciju povezivanja kako bi osigurala prekograničnu suradnju tijela svoje države članice s relevantnim tijelima u drugim državama članicama te međusektorsku suradnju s drugim nacionalnim nadležnim tijelima u svojoj državi članici.

5. Države članice osiguravaju da nadležna tijela iz stavka 1. i jedinstvene kontaktne točke imaju odgovarajuće resurse za djelotvornu i učinkovitu provedbu zadaća koje su im dodijeljene te da time ispune ciljeve ove Direktive. Države članice osiguravaju djelotvornu, učinkovitu i sigurnu suradnju imenovanih predstavnika u skupini za suradnju iz članka 12.

6. Svaka država članica bez nepotrebne odgode obavješćuje Komisiju o imenovanju nadležnog tijela iz stavka 1. i jedinstvene kontaktne točke iz stavka 3. te o njihovim zadaćama i svim naknadnim promjenama. Svaka država članica objavljuje imenovanje. Komisija objavljuje popis imenovanih jedinstvenih kontaktnih točaka.

Članak 9.

Timovi za odgovor na računalne sigurnosne incidente (CSIRT-ovi)

1. Svaka država članica imenuje jedan ili više CSIRT-ova koji udovoljavaju zahtjevima iz članka 10. stavka 1. i koji obuhvaćaju barem sektore, podsektore ili subjekte iz priloga I. i II. te su odgovorni za rješavanje incidenata u skladu s točno propisanim postupkom. CSIRT se može osnovati u okviru nadležnog tijela iz članka 8.

2. Države članice svakom CSIRT-u osiguravaju odgovarajuće resurse za djelotvorno izvršavanje zadaća iz članka 10. stavka 2. **Pri obavljanju tih zadaća CSIRT-ovi mogu dati prednost pružanju određenih usluga subjektima na osnovi pristupa utemeljenog na riziku.**

3. Države članice osiguravaju da svaki CSIRT raspolaže odgovarajućom, sigurnom i otpornom komunikacijskom i informacijskom infrastrukturom za razmjenu informacija s ključnim i važnim subjektima, kao i drugim relevantnim zainteresiranim stranama. Države članice u tu svrhu osiguravaju da CSIRT-ovi doprinose uvođenju sigurnih alata za razmjenu informacija.

4. CSIRT-ovi surađuju i prema potrebi razmjenjuju relevantne informacije u skladu s člankom 26. s pouzdanim sektorskim ili međusektorskim zajednicama ključnih i važnih subjekata.

5. CSIRT-ovi sudjeluju u [...] **uzajamnim učenjima** organiziranima u skladu s člankom 16.

6. Države članice osiguravaju djelotvornu, učinkovitu i sigurnu suradnju svojih CSIRT-ova u mreži CSIRT-ova iz članka 13.

7. Države članice bez nepotrebne odgode obavješćuju Komisiju o CSIRT-ovima imenovanima u skladu sa stavkom 1., koordinatoru CSIRT-ova imenovanom u skladu s člankom 6. stavkom 1. i zadaćama koje obavljaju u odnosu na subjekte iz priloga I. i II.

8. Države članice mogu zatražiti podršku ENISA-e u razvijanju nacionalnih CSIRT-ova.

Članak 10.

Zahtjevi u pogledu CSIRT-ova i njihove zadaće

1. CSIRT-ovi ispunjavaju sljedeće zahtjeve:

   (a) CSIRT-ovi osiguravaju visoku razinu dostupnosti svojih komunikacijskih [...] **kanala** izbjegavanjem jedinstvenih točki prekida te u svakom trenutku imaju na raspolaganju više sredstava za dvosmjerno kontaktiranje. CSIRT-ovi jasno određuju komunikacijske kanale i o njima obavješćuju klijente i suradnike;

   (b) prostori CSIRT-ova i informacijski sustavi za potporu smješteni su na sigurnim lokacijama;

(c) CSIRT-ovi su opremljeni odgovarajućim sustavom za upravljanje zahtjevima i njihovim preusmjeravanjem, posebno kako bi se olakšale djelotvorne i učinkovite primopredaje;

(d) CSIRT-ovi imaju dovoljno zaposlenika kako bi se osigurala dostupnost u svako doba;

(e) CSIRT-ovi su opremljeni redundantnim sustavima i rezervnim radnim prostorom kako bi se osigurao kontinuitet njihovih usluga;

(f) CSIRT-ovi imaju mogućnost sudjelovanja u međunarodnim mrežama za suradnju.

2. CSIRT-ovi obavljaju sljedeće zadaće:

(a) raćenje kiberprijetnji, ranjivosti i incidenata na nacionalnoj razini;

(b) pružanje ranih upozorenja i najava te informiranje ključnih i važnih subjekata te **nadležnih tijela i** drugih relevantnih zainteresiranih strana o kiberprijetnjama, ranjivostima i incidentima;

(c) odgovaranje na incidente;

(d) prikupljanje i analiza forenzičkih podataka te osiguravanje dinamičke analize rizika i incidenata te informiranosti o stanju u pogledu kibersigurnosti;

(e) osiguravanje **[...]** proaktivnog pregledavanja mrežnih i informacijskih sustava [...] **radi otkrivanja ranjivosti s potencijalnim znatnim učinkom pod uvjetom da, ako taj subjekt nije dao suglasnost, nije došlo do neovlaštenog upada u mrežne i informacijske sustave niti se negativno utječe na njihovo funkcioniranje;**

(f) sudjelovanje u mreži CSIRT-ova i pružanje uzajamne pomoći **u skladu s njihovim kapacitetima i kompetencijama** drugim članovima mreže na njihov zahtjev;

(fa) ako je to primjenjivo, djelujući kao koordinator za potrebe postupka koordiniranog otkrivanja ranjivosti na temelju članka 6. stavka 1. koji posebno uključuje olakšavanje interakcije između subjekata koji podliježu obvezi obavješćivanja, potencijalnog vlasnika ranjivosti i proizvođača ili pružatelja IKT proizvoda ili IKT usluga u slučajevima kada je to potrebno, utvrđivanje i kontaktiranje dotičnih subjekata, pružanje potpore subjektima koji podliježu obvezi obavješćivanja, pregovaranje o rokovima za objavu i upravljanje ranjivostima koje utječu na više organizacija (otkrivanje ranjivosti koje koordinira više strana).

3. CSIRT-ovi uspostavljaju suradnju s relevantnim akterima u privatnom sektoru radi uspješnijeg ostvarenja ciljeva Direktive.

3.a CSIRT-ovi mogu uspostaviti suradnju s nacionalnim CSIRT-ovima trećih zemalja. U okviru te suradnje mogu razmjenjivati relevantne informacije, uključujući osobne podatke u skladu s pravom Unije o zaštiti podataka.

4. CSIRT-ovi radi lakše suradnje promiču donošenje i primjenu zajedničkih ili standardiziranih praksi, planova za klasifikaciju i taksonomija u odnosu na sljedeće:

(a) postupke rješavanja incidenata;

(b) upravljanje kiberkrizama;

(c) koordinirano otkrivanje ranjivosti.

Članak 11.

Suradnja na nacionalnoj razini

1. Ako su odvojeni, nadležna tijela iz članka 8., jedinstvena kontaktna točka i CSIRT ili CSIRT-ovi iste države članice surađuju u ispunjavanju obveza utvrđenih u ovoj Direktivi.

2. Države članice osiguravaju da njihova nadležna tijela ili njihovi CSIRT-ovi primaju obavijesti o incidentima, kao i ozbiljnim kiberprijetnjama i izbjegnutim incidentima, podnesene na temelju ove Direktive. Ako država članica odluči da njezini CSIRT-ovi ne primaju te obavijesti, CSIRT-ovima se, u mjeri u kojoj je to potrebno za izvršavanje njihovih zadaća, omogućuje pristup podacima o incidentima koje su prijavili ključni ili važni subjekti na temelju članka 20.

3. Svaka država članica osigurava da njezina nadležna tijela ili CSIRT-ovi obavješćuju njezinu jedinstvenu kontaktnu točku o obavijestima o incidentima, ozbiljnim kiberprijetnjama i izbjegnutim incidentima koje su im dostavljene na temelju ove Direktive.

4. U mjeri u kojoj je to potrebno za djelotvorno izvršavanje zadaća i obveza utvrđenih u ovoj Direktivi, države članice osiguravaju odgovarajuću suradnju između nadležnih tijela, **CSIRT-ova,** jedinstvenih kontaktnih točaka te tijela za izvršavanje zakonodavstva, tijela za zaštitu podataka i **nadležnih** tijela **imenovanih** [...] na temelju Direktive (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata], **nadležnih tijela iz Provedbene uredbe Komisije 2019/1583, nacionalnih regulatornih tijela imenovanih u skladu s Direktivom (EU) 2018/1972, nacionalnih tijela imenovanih na temelju članka 17. Uredbe (EU) br. 910/2014,** [...] nacionalnih financijskih tijela imenovanih u skladu s Uredbom (EU) XXXX/XXXX Europskog parlamenta i Vijeća [Uredba DORA] **te nadležnih tijela imenovanih na temelju drugih sektorskih pravnih akata Unije** unutar te države članice.

5. Države članice osiguravaju da njihova nadležna tijela **iz ove Direktive i nadležna tijela imenovana na temelju Direktive (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata]** redovito **razmjenjuju** [...] informacije [...] **o utvrđivanju kritičnih subjekata,** kibersigurnosnih rizika, kiber**prijetnji i kiberincidenata te rizika, prijetnji i incidenata izvan kiberprostora** koji utječu na ključne subjekte koji su utvrđeni kao kritični **[**ili kao subjekti istovjetni kritičnim subjektima,**]** na temelju Direktive (EU) XXXX/XXXX [Direktiva o otpornosti ključnih subjekata], kao i o mjerama koje su [...] poduzete kao odgovor na te rizike i incidente. **Države članice ujedno osiguravaju da nadležna tijela iz ove Direktive** [...] **i nadležna tijela imenovana na temelju Uredbe XXXX/XXXX [Uredba DORA], Direktive 2018/1972 i Uredbe (EU) 910/2014 redovito razmjenjuju relevantne informacije.**

Kad je riječ o pružateljima usluga povjerenja i [...]posebno[...] u slučajevima kada je ta nadzorna uloga iz ove Direktive dodijeljena tijelu različitom od nadzornih tijela imenovanih na temelju Uredbe (EU) 910/2014, nacionalna nadležna tijela iz ove Direktive pravodobno blisko surađuju razmjenjujući relevantne informacije kako bi se osigurao djelotvoran nadzor i usklađenost pružatelja usluga povjerenja sa zahtjevima utvrđenima u ovoj Direktivi i Uredbi [XXXX/XXXX] **i prema potrebi, nacionalno nadležno tijelo iz ove Direktive, bez nepotrebne odgode, obavješćuje nadzorno tijelo eIDAS-a o svim prijavljenim znatnim kiberprijetnjama ili kiberincidentima s učinkom na usluge povjerenja**.

5.a U svrhu [...] pojednostavnjenja izvješćivanja o incidentima, države članice mogu uspostaviti jedinstvenu ulaznu točku za sve obavijesti koje se zahtijevaju ovom Direktivom te, prema potrebi, Uredbom (EU) 2016/679 i Direktivom 2002/58/EZ. Države članice mogu upotrebljavati jedinstvenu ulaznu točku za obavijesti koje se zahtijevaju na temelju drugih sektorskih pravnih akata Unije. Ta jedinstvena ulazna točka ne utječe na primjenu odredaba Uredbe (EU) 2016/679 i Direktive 2002/58/EZ, posebno onih koje se odnose na neovisna nadzorna tijela.

POGLAVLJE III.

*Suradnja **EU-a***

Članak 12.

Skupina za suradnju

1. U svrhu podupiranja i olakšavanja strateške suradnje i razmjene informacija među državama članicama [...] **te jačanja povjerenja i pouzdanja** [...], osniva se skupina za suradnju.

2. Skupina za suradnju izvršava svoje zadaće na temelju dvogodišnjih programa rada iz stavka 6.

3. Skupina za suradnju sastoji se od predstavnika država članica, Komisije i ENISA-e. Europska služba za vanjsko djelovanje sudjeluje u aktivnostima skupine za suradnju kao promatrač. Europska nadzorna tijela **i nadležna tijela imenovana na temelju Uredbe (EU) XXXX/XXXX [Uredba DORA]** [...] mogu sudjelovati u aktivnostima skupine za suradnju **u skladu s člankom 42. stavkom 1 Uredbe (EU) XXXX/XXXX [Uredba DORA]**.

   Skupina za suradnju može, prema potrebi, pozvati predstavnike relevantnih dionika da sudjeluju u njezinu radu.

   Komisija osigurava tajništvo.

4. Zadaće su skupine za suradnju:

   (a) pružanje smjernica nadležnim tijelima za prenošenje i provedbu ove Direktive;

   (aa) **pružanje smjernica u vezi s razvojem i provedbom politika o koordiniranom otkrivanju ranjivosti kako je navedeno u članku 5. stavku 2. točki (c) i članku 6. stavku 1.;**

(b) razmjena najbolje prakse i informacija povezanih s provedbom ove Direktive, među ostalim u pogledu kiberprijetnji, incidenata, ranjivosti, izbjegnutih incidenata, inicijativa za informiranje, osposobljavanja, vježbi i vještina, izgradnje kapaciteta, kao i normi i tehničkih specifikacija;

(c) savjetovanje i suradnja s Komisijom u pogledu novih inicijativa kibersigurnosne politike;

(d) savjetovanje i suradnja s Komisijom u pogledu nacrta provedbenih [...] akata Komisije donesenih na temelju ove Direktive;

(e) razmjena najbolje prakse i informacija s relevantnim institucijama, tijelima, uredima i agencijama Unije;

(ea) razmjena mišljenja o provedbi sektorskog zakonodavstva s aspektima kibersigurnosti;

(f) rasprava o izvješćima o [...] **uzajamnim učenjima** iz članka 16. stavka 7.;

(g) rasprava o **iskustvima** [...] zajedničkih nadzornih aktivnosti u prekograničnim slučajevima iz članka 34.;

(h) pružanje strateških smjernica mreži CSIRT-ova **i EU–CyCLONe-u** o određenim novonastalim pitanjima;

(ha) razmjena mišljenja o daljnjim koracima u vezi s politikama o kiberincidentima velikih razmjera na temelju iskustava stečenih u okviru mreže CSIRT-ova i EU–CyCLONe-a;

(i) doprinos kibersigurnosnim kapacitetima u cijeloj Uniji olakšavanjem razmjene nacionalnih službenika putem programa za izgradnju kapaciteta koji uključuje osoblje iz nadležnih tijela država članica ili CSIRT-ova;

(j) organiziranje redovitih zajedničkih sastanaka s relevantnim privatnim zainteresiranim stranama iz cijele Unije u svrhu rasprave o aktivnostima skupine za suradnju i prikupljanja informacija o novim izazovima u pogledu politike;

(k) rasprava o radu obavljenom u vezi s vježbama u području kibersigurnosti, uključujući rad ENISA-e**;**

(ka) uspostava mehanizma uzajamnog učenja u skladu s člankom 16. ove Direktive.

5. Skupina za suradnju može od mreže CSIRT-ova zatražiti tehničko izvješće o odabranim temama.

6. Do … 24 mjeseca od datuma stupanja na snagu ove Direktive, a nakon toga svake dvije godine, skupina za suradnju sastavlja program rada u pogledu djelovanja koje treba poduzeti za provedbu svojih ciljeva i zadaća. Vremenski okvir prvog programa donesenog na temelju ove Direktive usklađuje se s vremenskim okvirom posljednjeg programa donesenog na temelju Direktive (EU) 2016/1148.

7. Komisija može donijeti provedbene akte kojima se utvrđuju postupovni aranžmani potrebni za funkcioniranje skupine za suradnju. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 37. stavka 2.

8. Skupina za suradnju sastaje se redovito, a najmanje jednom godišnje, sa skupinom za otpornost kritičnih subjekata osnovanom na temelju Direktive (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] radi promicanja strateške suradnje i **olakšavanja** razmjene informacija.

Članak 13.

Mreža CSIRT-ova

1. S ciljem doprinosa razvoju povjerenja i pouzdanja te promicanja brze i djelotvorne operativne suradnje među državama članicama, osniva se mreža nacionalnih CSIRT-ova.

2. Mreža CSIRT-ova sastoji se od predstavnika CSIRT-ova država članica **imenovanih u skladu s člankom 9.** i CERT-EU-a. Komisija u mreži CSIRT-ova sudjeluje kao promatrač. ENISA osigurava tajništvo i aktivno podupire suradnju među CSIRT-ovima.

3. Zadaće su mreže CSIRT-ova:

   (a) razmjena informacija o kapacitetima CSIRT-ova;

   (b) razmjena relevantnih informacija o incidentima, izbjegnutim incidentima, kiberprijetnjama, rizicima i ranjivostima;

(ba) razmjena informacija o publikacijama i preporukama u području kibersigurnosti;

(bb) razmjena tehničkih rješenja kojima se olakšava tehničko rješavanje incidenata;

(bc) razmjena najboljih praksi, alata i postupaka u pogledu zadaća CSIRT-ova;

(c) na zahtjev [...] **člana** mreže CSIRT-ova na koju bi incident mogao utjecati, razmjena i rasprava o informacijama o tom incidentu te povezanim kiberprijetnjama, rizicima i ranjivostima;

(d) na zahtjev [...] **člana** mreže CSIRT-ova, razmatranje i, ako je moguće, provedba koordiniranog odgovora na incident koji je utvrđen u području za koje je nadležna ta država članica;

(e) pružanje potpore državama članicama u rješavanju prekograničnih incidenata na temelju ove Direktive;

(f) suradnja, **razmjena najboljih praksi** i pružanje pomoći imenovanim CSIRT-ovima iz članka 6. u pogledu upravljanja [...] koordiniranim otkrivanjem ranjivosti koje utječu na brojne proizvođače ili pružatelje IKT proizvoda, IKT usluga i IKT procesa s poslovnim nastanom u različitim državama članicama;

(g) rasprava o daljnjim oblicima operativne suradnje te njihovo utvrđivanje, među ostalim u odnosu na:

i. kategorije kiberprijetnji i incidenata;
ii. rana upozorenja;
iii. uzajamnu pomoć;

iv. načela i načine koordinacije u odgovoru na prekogranične rizike i incidente;
v. doprinos nacionalnom planu za odgovor na kiberincidente i kiberkrize iz članka 7. stavka 3. na zahtjev države članice;

(h) obavješćivanje skupine za suradnju o svojim aktivnostima i daljnjim oblicima operativne suradnje razmotrenima na temelju točke (g) te prema potrebi traženje smjernica u tom pogledu;

(i) razmatranje vježbi u području kibersigurnosti, među ostalim onih koje organizira ENISA;

(j) na zahtjev pojedinačnog CSIRT-a, rasprava o kapacitetima i pripravnosti tog CSIRT-a;

(k) suradnja i razmjena informacija s centrima za sigurnosne operacije (SOC-ovi) na regionalnoj razini i na razini Unije kako bi se poboljšala zajednička informiranost o stanju s obzirom na incidente i prijetnje u cijeloj Uniji;

(l) rasprava o izvješćima o [...] **uzajamnom učenju** iz članka 16. stavka 7.;

(m) izdavanje smjernica radi olakšavanja konvergencije operativnih praksi u cilju primjene odredaba ovog članka o operativnoj suradnji.

4. Za potrebe preispitivanja iz članka 35. i do □24 mjeseca od datuma stupanja na snagu ove Direktive□, a nakon toga svake dvije godine, mreža CSIRT-ova ocjenjuje napredak ostvaren u operativnoj suradnji i priprema izvješće. U izvješću se posebno donose zaključci o ishodima **uzajamnog učenja** [...] iz članka 16. provedenog u pogledu nacionalnih CSIRT-ova, uključujući zaključke i preporuke na temelju tog članka. To se izvješće dostavlja i skupini za suradnju.

5. Mreža CSIRT-ova donosi vlastiti poslovnik.

6. Mreža CSIRT-ova surađuje s EU-CyCLONe-om na temelju dogovorenih postupovnih aranžmana.

Članak 14.

Europska mreža organizacija za vezu za kiberkrize (EU-CyCLONe)

1. Kako bi se poduprlo koordinirano upravljanje kiberincidentima i kiberkrizama velikih razmjera na operativnoj razini i osigurala redovita razmjena informacija između institucija, tijela i agencija država članica i Unije, uspostavlja se Europska mreža organizacija za vezu za kiberkrize (EU-CyCLONe).

2. EU-CyCLONe čine predstavnici tijela država članica za upravljanje **kiber**krizama koja su imenovana u skladu s člankom 7.[...] **Komisija u aktivnostima mreže sudjeluje kao promatrač.** ENISA osigurava tajništvo mreže i podupire sigurnu razmjenu informacija **te osigurava potrebne alate za potporu suradnji među državama članicama osiguravajući pritom sigurnu razmjenu informacija**.

EU-CyCLONe može, prema potrebi, pozvati predstavnike relevantnih dionika da sudjeluju u njezinu radu.

3. Zadaće su EU-CyCLONe-a:

(a) povećanje razine pripravnosti za upravljanje [...] kiberincidentima i kiberkrizama velikih razmjera;

(b) poboljšanje zajedničke informiranosti o stanju [...] za kiberincidente i kiberkrize velikih razmjera;

(ba) procjena posljedica i učinka relevantnih kiberincidenata velikih razmjera i predlaganje mogućih mjera ublažavanja;

(c) koordinacija upravljanja kiberincidentima i kiberkrizama velikih razmjera [...] te pomoć pri donošenju odluka na političkoj razini u pogledu takvih incidenata i kriza;

(d) **na zahtjev države članice,** rasprava o **njezinim** nacionalnim planovima za odgovor na kiberincidente i kiberkrize iz članka 7. stavka **3**.[...]

4. EU-CyCLONe donosi vlastiti poslovnik.

5. EU-CyCLONe redovito izvješćuje skupinu za suradnju o **upravljanju kiberincidentima i kiberkrizama velikih razmjera** [...], posvećujući pritom posebnu pažnju njihovu utjecaju na ključne i važne subjekte.

6. EU-CyCLONe surađuje s mrežom CSIRT-ova na temelju dogovorenih postupovnih aranžmana.

7. EU-CyCLONe Europskom parlamentu i Vijeću podnosi izvješće o ocjeni svojeg rada do [24 mjeseca nakon datuma stupanja na snagu ove Direktive].

Članak 14.a

Međunarodna suradnja

Unija može, prema potrebi, sklapati međunarodne sporazume s trećim zemljama ili međunarodnim organizacijama, u skladu s člankom 218. UFEU-a, kojima im se omogućuje i organizira sudjelovanje u nekim aktivnostima skupine za suradnju, mreže CSIRT-ova i EU-CyCLONe-a, u skladu s pravom Unije o zaštiti podataka.

Članak 15.

Izvješće o stanju kibersigurnosti u Uniji

1. ENISA, u suradnji s Komisijom **i skupinom za suradnju**, izdaje dvogodišnje izvješće o stanju kibersigurnosti u Uniji. Izvješćem je posebno obuhvaćeno [...] sljedeće:

   (aa) procjena rizika u području kibersigurnosti na razini Unije, uzimajući u obzir prijetnje;

   (a) [...] **ocjena** razvoja kibersigurnosnih kapaciteta u javnim i privatnim sektorima širom Unije;

   (b) [...]

   (c) **skupna ocjena na temelju kvantitativnih i kvalitativnih pokazatelja** [...] kibersigurnosti kojom se pruža [...] **pregled** razine razvijenosti kibersigurnosnih kapaciteta**, uključujući sektorske kapacitete**.

2. Izvješće sadržava posebne preporuke o politikama za povećanje razine kibersigurnosti u cijeloj Uniji i sažetak nalaza za određeno razdoblje iz tehničkih izvješća o stanju kibersigurnosti u EU-u koje izdaje ENISA u skladu s člankom 7. stavkom 6. Uredbe (EU) 2019/881.

Članak 16.

Uzajamna učenja

1. **S ciljem jačanja uzajamnog povjerenja, postizanja visoke zajedničke razine kibersigurnosti te jačanja kibersigurnosnih kapaciteta i politika država članica potrebnih za djelotvornu provedbu ove Direktive,** [...] **skupina za suradnju,** [...] **uz potporu Komisije i** nakon savjetovanja s [...] ENISA-om **i, prema potrebi, mrežom CSIRT-ova,** a najkasnije **24** [...] mjeseca nakon stupanja na snagu ove Direktive, utvrđuje metodologiju [...] za **objektivan, nediskriminirajući i pravedan** sustav **uzajamnog učenja** [...] **u vezi s** [...] **provedbom ove Direktive od strane** država članica. **Sudjelovanje u uzajamnom učenju dobrovoljno je. Sustav se sastoji od krugova ocjenjivanja** [...] koje provode [...] stručnjaci za kibersigurnost iz država članica [...] i obuhvaćaju [...] **jedan ili više** sljedećih aspekata:

   i. [...] provedbu zahtjeva za upravljanje kibersigurnosnim rizicima i obveze izvješćivanja iz članaka 18. i 20.;

   ii. [...] kapacitete, uključujući dostupne [...] resurse te [...] izvršavanje zadaća nacionalnih nadležnih tijela **iz članka 8. i CSIRT-ova iz članka 9.**;

[...]

iii. [...] [...] **provedbu** uzajamne pomoći iz članka 34.;

iv. [...] **provedbu** okvira za razmjenu informacija iz članka 26. [...].

2. **Kriteriji na temelju kojih države članice trebaju imenovati stručnjake prihvatljive za sudjelovanje u krugovima uzajamnog učenja** [...] objektivni su, nediskriminirajući, pošteni i transparentni [...] **te su uključeni u metodologiju iz stavka 1**. ENISA i Komisija [...] **mogu** imenovati stručnjake koji kao promatrači sudjeluju u [...] **krugovima uzajamnog učenja**. [...]

3. [...].

3.a Prije početka krugova uzajamnog učenja, države članice mogu provesti samoprocjenu aspekata obuhvaćenih tim određenim krugom uzajamnog učenja i dostaviti samoprocjenu imenovanim stručnjacima iz stavka 2.

4. **Uzajamna** [...] **učenja** [...] **mogu** uključivati [...] **fizičke** ili virtualne provjere na lokaciji i razmjene izvan lokacije. S obzirom na načelo dobre suradnje, države članice [...] **koje sudjeluju u uzajamnom učenju** dostavljaju imenovanim stručnjacima [...] informacije potrebne za procjenu [...]**, ne dovodeći u pitanje nacionalno pravo ili pravo Unije u vezi sa zaštitom povjerljivih ili klasificiranih informacija ili zaštitom ključnih državnih funkcija, kao što je nacionalna sigurnost.** Informacije dobivene u postupku [...] **uzajamnog učenja** upotrebljavaju se isključivo u tu svrhu. Stručnjaci koji sudjeluju u [...] **uzajamnom učenju** ne otkrivaju trećim stranama osjetljive ili povjerljive informacije dobivene [...] **u tom kontekstu**. **Države članice koje sudjeluju u uzajamnom učenju mogu se usprotiviti imenovanju određenih stručnjaka iz opravdanih razloga dostavljenih skupini za suradnju.**

5. Nakon š**to budu obuhvaćeni krugom uzajamnog učenja** [...], isti aspekti ne podvrgavaju se daljnjim [...] **krugovima uzajamnog učenja** [...] za države članice **sudionice** tijekom [...] **četiri** godine nakon završetka **tog** [...] **kruga** [...] **uzajamnog učenja**, **osim ako dotična država članica to zatraži ili ako se složi s prijedlogom** [...] **skupine za suradnju** [...].

6. [...]

7. Stručnjaci koji sudjeluju u [...] **krugovima uzajamnog učenja** sastavljaju izvješća o nalazima i zaključcima [...] **ocjena**. **Države članice mogu dostaviti komentare o svojim nacrtima izvješća, koji se prilažu izvješću. Završna** izvješća dostavljaju se [...] skupini za suradnju [...]. **Države članice mogu odlučiti javno objaviti svoja izvješća.**

POGLAVLJE IV.

Obveze upravljanja kibersigurnosnim rizicima i izvješćivanja o njima

ODJELJAK I.

Upravljanje kibersigurnosnim rizicima i izvješćivanje o njima

Članak 17.

Upravljanje

1. Države članice osiguravaju da upravljačka tijela ključnih i važnih subjekata odobravaju mjere upravljanja kibersigurnosnim rizicima koje su ti subjekti poduzeli radi usklađivanja s člankom 18., nadziru njegovu provedbu i [...] **mogu se smatrati** odgovornima za neusklađenost subjekata s obvezama iz ovog članka.

   Primjenom ovog stavka ne dovodi se u pitanje nacionalno pravo država članica u pogledu pravila o odgovornosti u javnim institucijama, kao ni odgovornosti javnih službenika te izabranih i imenovanih dužnosnika.

2. Države članice osiguravaju da se **od članova upravljačkog tijela** [...] **zahtijeva da** redovito pohađaju [...] osposobljavanja kako bi stekli dovoljno znanja i vještina za razumijevanje i procjenu kibersigurnosnih rizika i praksi upravljanja, kao i njihova učinka na poslovanje subjekta.

Članak 18.

Mjere upravljanja kibersigurnosnim rizicima

1**.a** **Ovom Direktivom primjenjuje se pristup kojim se uzimaju u obzir sve opasnosti koji obuhvaća zaštitu mrežnih i informacijskih sustava i njihovog fizičkog okruženja od svakog događaja koji može ugroziti dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koje mrežni i informacijski sustavi nude ili kojima omogućuju pristup.**

1. Države članice osiguravaju da ključni i važni subjekti poduzimaju odgovarajuće i razmjerne tehničke i organizacijske mjere upravljanja rizicima za sigurnost mrežnih i [...] informacijskih sustava kojima se ti subjekti služe u pružanju svojih usluga. Uzimajući u obzir najnovija dostignuća i **trošak provedbe**, tim se mjerama osigurava razina sigurnosti mrežnih i informacijskih sustava koja odgovara postojećem riziku. **Pri procjeni razmjernosti tih mjera u obzir se uzima stupanj izloženosti subjekta rizicima, njegova veličina, vjerojatnost nastanka incidenata i njihova ozbiljnost. Uzimajući u obzir razinu i vrstu rizika za društvo u slučaju incidenata koji utječu na ključne ili važne subjekte, mjere upravljanja kibersigurnosnim rizicima uvedene važnim subjektima mogu biti blaže od onih uvedenih ključnim subjektima.**

2. Mjere iz stavka 1. uključuju najmanje sljedeće:

(a) politike analize rizika i sigurnosti informacijskih sustava;

(b) rješavanje incidenata (sprečavanje, otkrivanje, [...] odgovor na incidente **i oporavak od** [...] incidenata);

(c) kontinuitet poslovanja i upravljanje krizama;

(d) sigurnost lanca opskrbe, uključujući sigurnosne aspekte u pogledu odnosa između svakog subjekta i njegovih **izravnih** dobavljača ili pružatelja usluga kao što su pružatelji usluga pohrane i obrade podataka ili upravljanih sigurnosnih usluga;

(e) sigurnost u nabavi, razvoju i održavanju mrežnih i informacijskih sustava, uključujući rješavanje ranjivosti i njihovo otkrivanje;

(f) politike i postupke [...] za procjenu djelotvornosti mjera upravljanja kibersigurnosnim rizicima;

(g) **politiku** o primjeni kriptografije i šifriranja;

(ga) sigurnost ljudskih resursa, politike kontrole pristupa i upravljanje imovinom.

3. Države članice osiguravaju da se od subjekata [...] **zahtijeva da** pri razmatranju odgovarajućih mjera iz stavka 2. točke (d) uzimaju u obzir ranjivosti specifične za svakog **izravnog** dobavljača i pružatelja usluge te opću kvalitetu proizvoda i kibersigurnosnu praksu svojih dobavljača i pružatelja usluga, uključujući njihove sigurne razvojne postupke. **Države članice također osiguravaju da se od subjekata zahtijeva da pri razmatranju odgovarajućih mjera iz stavka 2. točke (d) u obzir uzmu rezultate koordiniranih procjena rizika provedenih u skladu s člankom 19. stavkom 1.**

4. Države članice osiguravaju da subjekt, ako utvrdi da njegove usluge odnosno zadaće nisu u skladu sa zahtjevima utvrđenima u stavku 2., bez nepotrebne odgode poduzme sve potrebne korektivne mjere kako bi uskladio dotičnu uslugu.

5. Komisija može donijeti provedbene akte kako bi utvrdila tehničke i metodološke specifikacije, **kao i sektorske posebnosti, prema potrebi,** elemenata iz stavka 2. **ovog članka**. **Komisija do [18 mjeseci nakon stupanja na snagu ove Direktive] donosi provedbene akte kako bi se utvrdile tehničke i metodološke specifikacije za subjekte iz članka 24. stavka 2. i pružatelje usluga povjerenja iz točke 8. Priloga I. Ti provedbeni akti donose se u skladu s postupkom ispitivanja iz članka 37. stavka 2.** U [...] pripremi [...] **tih provedbenih** akata Komisija [...] u najvećoj mogućoj mjeri **slijedi** međunarodne i europske norme, kao i relevantne tehničke specifikacije **te razmjenjuje savjete sa skupinom za suradnju i ENISA-om o nacrtu provedbenog akta u skladu s člankom 12. stavkom 4. točkom (d).**

6. [...]

Članak 19.

Koordinirane procjene rizika ključnih lanaca opskrbe na razini EU-a

1. Skupina za suradnju, zajedno s Komisijom i ENISA-om, može provoditi koordinirane procjene sigurnosnih rizika za određene ključne lance opskrbe IKT uslugama, sustavima ili proizvodima, uzimajući u obzir tehničke i, prema potrebi, netehničke čimbenike rizika.

2. Komisija, nakon savjetovanja sa skupinom za suradnju i ENISA-om, utvrđuje posebne ključne IKT usluge, sustave ili proizvode koji mogu biti predmet koordinirane procjene rizika iz stavka 1.

Članak 20.

Obveze izvješćivanja

1. Države članice osiguravaju da ključni i važni subjekti bez nepotrebne odgode obavješćuju nadležna tijela ili CSIRT u skladu sa stavcima 3. i 4. o svakom incidentu koji ima znatan učinak na pružanje njihovih usluga. Prema potrebi, ti subjekti bez nepotrebne odgode obavješćuju primatelje svojih usluga o **tim** incidentima koji bi mogli negativno utjecati na pružanje tih usluga. Države članice osiguravaju da ti subjekti, među ostalim, prijavljuju sve informacije koje nadležnim tijelima ili CSIRT-ovima omogućuju da utvrde sve prekogranične učinke incidenta. **Čin slanja obavijesti sam po sebi ne uzrokuje to da subjekt koji šalje obavijest podliježe povećanoj odgovornosti.**

2. [...]

Ako je primjenjivo, [...] **ključni i važni** subjekti bez nepotrebne odgode obavješćuju primatelje svojih usluga na koje bi mogla utjecati ozbiljna kiberprijetnja o svim mjerama ili pravnim lijekovima koje ti primatelji mogu poduzeti kao odgovor na tu prijetnju. Prema potrebi, subjekti isto tako obavješćuju te primatelje o samoj prijetnji. **Čin slanja** obavijesti **sam po sebi** ne uzrokuje to da subjekt koji šalje obavijest podliježe povećanoj odgovornosti.

3. Incident se smatra ozbiljnim:

(a) ako je uzrokovao ili može uzrokovati **ozbiljne** [...] poremećaje u radu **usluge** ili financijske gubitke za dotični subjekt;

(b) ako je utjecao ili bi mogao utjecati na druge fizičke ili pravne osobe uzrokovanjem znatnih materijalnih ili nematerijalnih gubitaka.

4. Države članice osiguravaju da, za potrebe obavješćivanja iz stavka 1., dotični subjekti podnose nadležnim tijelima ili CSIRT-u:

(a) bez nepotrebne odgode, a u svakom slučaju u roku od 24 sata od primitka informacije o incidentu, prvu obavijest **kao rano upozorenje** u kojoj se, prema potrebi, navodi pretpostavlja li se da je incident uzrokovan nezakonitim ili zlonamjernim djelovanjem;

(b) na zahtjev nadležnog tijela ili CSIRT-a, privremeno izvješće o relevantnim ažuriranjima statusa;

(c) **završno** izvješće najkasnije mjesec dana nakon podnošenja [...] **početne obavijesti** iz točke (a), koje uključuje najmanje sljedeće:

i. detaljni opis incidenta, njegovu ozbiljnost i učinak;

ii. vrstu prijetnje ili temeljnog uzroka koji je vjerojatno prouzročio incident;

iii. provedene i tekuće mjere ublažavanja.

Države članice osiguravaju da u opravdanim slučajevima i u dogovoru s nadležnim tijelima ili CSIRT-om dotični subjekt može odstupiti od rokova utvrđenih u točkama (a) i (c). **Osobito, odstupanje od toka iz točke (c) može se opravdati u slučajevima u kojima je incident još u tijeku.**

5. Nadležna nacionalna tijela ili CSIRT [...] **bez nepotrebne odgode** nakon primitka prve obavijesti iz stavka 4. točke (a) dostavljaju odgovor subjektu koji podnosi obavijest, uključujući početne povratne informacije o incidentu i, na zahtjev subjekta, smjernice za provedbu mogućih mjera ublažavanja. Ako CSIRT nije primio obavijest iz stavka 1., smjernice pruža nadležno tijelo u suradnji s CSIRT-om. CSIRT pruža dodatnu tehničku potporu ako to zatraži dotični subjekt. Ako se sumnja da je incident kriminalne naravi, nadležna nacionalna tijela ili CSIRT pružaju i smjernice o prijavi incidenta tijelima za izvršavanje zakonodavstva.

6. Nadležno tijelo, CSIRT ili **jedinstvena kontaktna točka** prema potrebi o incidentu obavješćuju ostale pogođene države članice i ENISA-u, a osobito ako se incident iz stavka 1. odnosi na dvije države članice ili više njih. **Te informacije obuhvaćaju barem elemente predviđene u stavku 4. ovog članka.** Pritom nadležna tijela, CSIRT-ovi i jedinstvene kontaktne točke, u skladu s pravom Unije ili nacionalnim zakonodavstvom usklađenim s pravom Unije, čuvaju sigurnost i komercijalne interese subjekta te povjerljivost dostavljenih informacija.

7. Ako je za sprečavanje incidenta ili rješavanje incidenta koji je u tijeku nužno obavijestiti javnost ili ako je otkrivanje incidenta u javnom interesu zbog nekog drugog razloga, nadležno tijelo ili CSIRT te, prema potrebi, tijela ili CSIRT-ovi drugih pogođenih država članica mogu, nakon savjetovanja s dotičnim subjektom, obavijestiti javnost o incidentu ili zatražiti od subjekta da to učini.

8. Na zahtjev nadležnog tijela ili CSIRT-a jedinstvena kontaktna točka prosljeđuje obavijesti primljene na temelju stavka [...] 1. [...]jedinstvenim kontaktnim točkama drugih pogođenih država članica.

9. Jedinstvena kontaktna točka [...] **svakih šest mjeseci podnosi** ENISA-i sažeto izvješće koje uključuje anonimizirane i agregirane podatke o incidentima, ozbiljnim kiberprijetnjama i izbjegnutim incidentima prijavljenima u skladu sa stavkom [...] 1. [...] i u skladu s člankom 27. Kako bi se doprinijelo tome da dostavljeni podaci budu usporedivi, ENISA može izdati tehničke smjernice o parametrima za informacije uključene u sažeto izvješće. **ENISA svakih šest mjeseci obavješćuje skupinu za suradnju i mrežu CSIRT-ova o svojim nalazima o primljenim obavijestima.**

10. Nadležna tijela dostavljaju nadležnim tijelima imenovanima na temelju Direktive (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] informacije o incidentima i kiberprijetnjama koje su u skladu sa stavcima 1. i 2. prijavili ključni subjekti koji su identificirani kao kritični subjekti **[**ili kao subjekti istovjetni kritičnim subjektima**]**, na temelju Direktive (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata].

11. Komisija može donijeti provedbene akte kojima se dodatno utvrđuju vrsta informacija te oblik i postupak podnošenja obavijesti na temelju stavaka 1. i 2. Komisija isto tako može donijeti provedbene akte kako bi dodatno utvrdila slučajeve u kojima se incident smatra ozbiljnim kako je navedeno u stavku 3. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 37. stavka 2.

Članak 21.

Primjena europskih programa kibersigurnosne certifikacije

1. Kako bi dokazale usklađenost s određenim zahtjevima iz članka 18., **države članice mogu zahtijevati da subjekti upotrebljavaju određene IKT proizvode,** [...] **usluge i** [...] **procese certificirane** u okviru posebnih europskih programa kibersigurnosne certifikacije donesenih na temelju članka 49. Uredbe (EU) 2019/881. **IKT** proizvode, usluge i procese koji podliježu certifikaciji mogu razviti ključni ili važni subjekti ili se mogu nabaviti od trećih strana.

2. Komisija može [...] donijeti [...] **provedbene** akte kojima se određuje koje kategorije ključnih **ili važnih** subjekata moraju **upotrebljavati određene certificirane IKT proizvode, usluge i procese ili** pribaviti certifikat [...] u okviru [...] europskih programa kibersigurnosne certifikacije **donesenih na temelju članka 49. Uredbe (EU) 2019/881.** [...] **Ti provedbeni akti donose se u skladu s postupkom ispitivanja iz članka 37. stavka 2. Pri pripremi tih provedbenih akata Komisija u skladu s člankom 56. Uredbe (EU) 2019/881:**

   i. uzima u obzir utjecaj mjera na proizvođače ili pružatelje takvih IKT proizvoda, usluga ili procesa te na korisnike u smislu troška tih mjera, kao i društvenih ili gospodarskih koristi koje proizlaze iz očekivane poboljšane razine sigurnosti ciljanih IKT proizvoda, usluga ili procesa kao i dostupnost njihovih alternativa na tržištu;

   ii. provodi otvoren, transparentan i uključiv postupak savjetovanja sa svim relevantnim dionicima i državama članicama;

iii. uzima u obzir sve rokove za provedbu, prijelazne mjere i razdoblja, posebno vodeći računa o mogućem učinku mjera na proizvođače ili pružatelje IKT proizvoda, usluga ili procesa, ili na njihove korisnike, posebice mala i srednja poduzeća;

iv. uzima u obzir postojanje i provedbu relevantnog prava država članica.

3. Ako nije dostupan odgovarajući europski program kibersigurnosne certifikacije za potrebe stavka 2. **ovog članka**, Komisija može zatražiti od ENISA-e da izradi prijedlog programa certifikacije **ili da preispita postojeći europski program kibersigurnosne certifikacije** na temelju članka 48. stavka 2. Uredbe (EU) 2019/881.

Članak 22.

Normizacija

1. Države članice, u cilju promicanja konvergentne provedbe članka 18. stavaka 1. i 2., bez nametanja ili diskriminacije određene vrste tehnologije, potiču primjenu europskih ili međunarodno priznatih normi i specifikacija relevantnih za sigurnost mrežnih i informacijskih sustava.

2. ENISA u suradnji s državama članicama izrađuje savjete i smjernice u pogledu tehničkih područja koja treba razmotriti u odnosu na stavak 1. te u odnosu na postojeće norme, uključujući nacionalne norme država članica, kojima bi se ta područja mogla obuhvatiti.

Članak 23.

Baze podataka s nazivima domena i registracijskim podacima

1. Kako bi se doprinijelo sigurnosti, stabilnosti i otpornosti DNS-a, države članice osiguravaju da registri **naziva** vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu prikupljaju i održavaju točne **[...]** i potpune podatke o registraciji naziva domena u posebnoj bazi podataka uz dužnu pažnju **u skladu s** [...] pravom Unije o zaštiti osobnih podataka.

2. Države članice osiguravaju da baze podataka o registraciji naziva domena iz stavka 1. sadržavaju relevantne informacije za identifikaciju i kontakt nositelja naziva domena te kontaktnih točaka koje upravljaju nazivima domena u okviru vršnih domena**, uključujući barem sljedeće podatke:**

   a) naziv domene

   b) datum registracije

   c) podatke o korisniku domene, uključujući:

      i. za pojedince – ime, prezime i adresu e-pošte;

      ii. za pravne osobe – naziv i adresu e-pošte.

3. Države članice osiguravaju da registri **naziva** vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu uspostave politike i postupke kojima se osigurava da baze podataka sadržavaju točne i potpune informacije. Države članice osiguravaju da su takve politike i postupci javno dostupni.

4. Države članice osiguravaju da registri **naziva** vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu bez nepotrebne odgode nakon registracije naziva domene objave podatke o registraciji domene koji nisu osobni podaci.

5. Države članice osiguravaju da registri **naziva** vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu omoguće pristup određenim podacima o registraciji naziva domena na temelju zakonitih i opravdanih zahtjeva legitimnih tražitelja pristupa, u skladu s pravom Unije o zaštiti podataka. Države članice osiguravaju da registri **naziva** vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu bez nepotrebne odgode **i u svakom slučaju u roku od 72 sata** odgovaraju na sve zahtjeve za pristup. Države članice osiguravaju javnu dostupnost politika i postupaka za objavljivanje takvih podataka.

Odjeljak II.

Nadležnost i registracija

Članak 24.

Nadležnost i teritorijalnost

1.a Smatra se da su subjekti obuhvaćeni ovom Direktivom u nadležnosti države članice u kojoj pružaju svoje usluge. Smatra se da su subjekti iz točaka od 1. do 7. i točke 10. Priloga I., pružatelji usluga povjerenja i pružatelji središta za razmjenu internetskog prometa iz točke 8. Priloga I. te točaka od 1. do 5. Priloga II. u nadležnosti države članice na čijem državnom području imaju poslovni nastan.

1. Smatra se da su pružatelji DNS usluga, registri naziva vršnih domena [...] **i subjekti koji pružaju usluge registracije naziva domena ta vršnu domenu**, pružatelji usluga računalstva u oblaku, pružatelji usluga podatkovnog centra, [...] pružatelji mreža za isporuku sadržaja**, pružatelji upravljanih usluga i pružatelji upravljanih sigurnosnih usluga** iz točke 8. **i točke 8.a** Priloga I. te pružatelji digitalnih usluga iz točke 6. Priloga II. u nadležnosti države članice u kojoj imaju glavni poslovni nastan u Uniji.

2. Za potrebe ove Direktive smatra se da subjekti iz stavka 1. imaju glavni poslovni nastan u Uniji u državi članici u kojoj se **pretežno** donose odluke povezane s mjerama upravljanja kibersigurnosnim rizicima. Ako **se mjesto na kojem se takve odluke pretežno donose ne može odrediti ili** se takve odluke ne donose bilo kojoj poslovnoj jedinici u Uniji, trebalo bi smatrati da se glavni poslovni nastan nalazi u državama članicama u kojima subjekt ima poslovnu jedinicu s najvećim brojem zaposlenika u Uniji. **Ako usluge pruža grupa poduzeća, glavni poslovni nastan smatra se glavnim poslovnim nastanom grupe poduzeća.**

3. Ako subjekt iz stavka 1. nema poslovni nastan u Uniji, ali nudi usluge unutar Unije, imenuje predstavnika u Uniji. Predstavnik ima poslovni nastan u jednoj od država članica u kojima subjekt nudi svoje usluge. Smatra se da takav subjekt pripada nadležnosti one države članice u kojoj njegov predstavnik ima poslovni nastan. Ako predstavnik unutar Unije nije imenovan u skladu s ovim člankom, svaka država članica u kojoj subjekt pruža usluge može poduzeti pravne radnje protiv subjekta zbog nepoštovanja obveza iz ove Direktive.

4. Imenovanjem predstavnika koje obavlja subjekt iz stavka 1. ne dovode se u pitanje pravne radnje koje bi se mogle poduzeti protiv tog subjekta.

4.a Države članice koje su primile zahtjev za uzajamnu pomoć u vezi sa subjektima iz stavka 1. mogu, u okvirima zahtjeva, poduzeti odgovarajuće nadzorne i provedbene mjere u odnosu na dotični subjekt koji pruža usluge ili koji ima mrežni i informacijski sustav na njihovu državnom području.

Članak 25.

Registar za određene subjekte u području digitalne strukture i pružatelje digitalnih usluga

1. [...] **Države članice osiguravaju da** [...] se od subjekata **iz članka 24. stavka 1. koji imaju glavni** poslovni **nastan na njihovu državnom području ili, ako nemaju poslovni nastan u Uniji, imaju imenovanog predstavnika u Uniji s poslovnim nastanom na njihovu državnom području zahtijeva da** [...] podnesu sljedeće informacije **nadležnim tijelima** [...] do [12 mjeseci nakon stupanja na snagu ove Direktive]:

(a) naziv subjekta;

(aa) vrstu subjekta u skladu s prilozima I. i II. ove Direktive;

(b) adresu svojega glavnog poslovnog nastana i drugih zakonitih poslovnih jedinica u Uniji ili, ako nemaju poslovni nastan u Uniji, svojega predstavnika imenovanog na temelju članka 24. stavka 3.;

(c) ažurirane podatke za kontakt, uključujući e-adrese i telefonske brojeve subjekata **i njihovih predstavnika;**

(d) **države članice u kojima subjekt pruža svoje usluge.**

Prema potrebi, ove informacije podnose se putem nacionalnih mehanizama za samostalno obavješćivanje iz članka 2.a.

2. **Države** članice **osiguravaju da** [...] subjekti iz stavka 1. bez odgode, a u svakom slučaju u roku od tri mjeseca od datuma na koji je promjena počela proizvoditi učinke, [...] **također obavješćuju** o svim promjenama podataka koje su dostavili na temelju stavka 1.

3. [...] **Jedinstvene kontaktne točke država članica** prosljeđuju **informacije iz stavaka 1. i 2.** [...] [...] **ENISA-i**. [...]

3.a Na temelju informacija primljenih u skladu sa stavkom 3. ovog članka ENISA uspostavlja i održava registar za subjekte iz stavka 1. ENISA na zahtjev država članica relevantnim nadležnim tijelima omogućuje pristup registru, osiguravajući pritom potrebna jamstva za zaštitu povjerljivosti informacija, prema potrebi.

4. [...]

POGLAVLJE V.

Razmjena informacija

Članak 26.

Mehanizmi za razmjenu informacija o kibersigurnosti

1. [...] Države članice osiguravaju da ključni i važni subjekti mogu **na dobrovoljnoj osnovi** međusobno razmjenjivati relevantne informacije o kibersigurnosti, uključujući informacije koje se odnose na kiberprijetnje, **izbjegnute incidente,** ranjivosti, pokazatelje ugroženosti, taktike, tehnike i postupke, kibersigurnosna upozorenja i konfiguracijske alate, ako takva razmjena informacija:

   (a) ima za cilj sprečavanje ili otkrivanje incidenata, odgovaranje na incidente ili njihovo ublažavanje;

(b) povećava razinu kibersigurnosti, posebno povećanjem informiranosti o kiberprijetnjama, ograničavanjem ili ometanjem mogućnosti širenja takvih prijetnji, podupiranjem niza obrambenih sposobnosti, otklanjanjem i otkrivanjem ranjivosti, tehnikama otkrivanja prijetnji, strategijama ublažavanja ili fazama odgovora i oporavka.

2. Države članice osiguravaju da se razmjena informacija odvija unutar [...] zajednica ključnih i važnih subjekata. S obzirom na potencijalno osjetljivu prirodu razmijenjenih informacija, takva se razmjena provodi putem mehanizama za razmjenu informacija [...].

3. Države članice [...] **mogu** utvrditi pravila kojima se određuju postupak, operativni elementi (uključujući upotrebu namjenskih IKT platformi), sadržaj i uvjeti mehanizama za razmjenu informacija iz stavka 2. Takvim se pravilima [...] **mogu** utvrditi i pojedinosti o sudjelovanju javnih tijela u takvim mehanizmima, kao i operativni elementi, uključujući upotrebu namjenskih informatičkih platformi. Države članice nude potporu primjeni takvih mehanizama u skladu sa svojim politikama iz članka 5. stavka 2. točke (g).

4. Ključni i važni subjekti obavješćuju nadležna tijela o svojem sudjelovanju u mehanizmima za razmjenu informacija iz stavka 2. nakon početka sudjelovanja u takvim mehanizmima ili, ako je primjenjivo, o svojem povlačenju iz takvih mehanizama nakon što povlačenje stupi na snagu.

5. [...] ENISA podupire uspostavu mehanizama za razmjenu informacija o kibersigurnosti iz stavka 2. pružanjem primjera najbolje prakse i smjernica.

Članak 27.

Dobrovoljno obavješćivanje o relevantnim informacijama

1. Ne dovodeći u pitanje članak 20., države članice osiguravaju da ključni i važni subjekti mogu na dobrovoljnoj osnovi obavijestiti nadležna tijela ili CSIRT-ove o svim relevantnim incidentima, kiberprijetnjama ili izbjegnutim incidentima.

2. Ne dovodeći u pitanje članak 3., države članice osiguravaju da subjekti koji nisu obuhvaćeni područjem primjene ove Direktive mogu dobrovoljno podnositi obavijesti o ozbiljnim incidentima, kiberprijetnjama ili izbjegnutim incidentima. Pri obradi obavijesti države članice djeluju u skladu s postupkom utvrđenim u članku 20. Države članice obradi obveznih obavijesti mogu dati prednost pred obradom obavijesti na dobrovoljnoj osnovi. **Ne dovodeći u pitanje istragu, otkrivanje i progon kaznenih djela,** [...] **s**ubjektu koji je obavijest podnio dobrovoljno ne nameću se zbog tog obavješćivanja dodatne obveze kojima ne bi podlijegao da nije podnio tu obavijest.

3. Obavijesti na dobrovoljnoj osnovi obrađuju se samo ako takva obrada ne predstavlja nerazmjerno ili nepotrebno opterećenje za dotične države članice.

POGLAVLJE VI.

Nadzor i provedba

Članak 28.

Opći aspekti nadzora i provedbe

1. Države članice osiguravaju da nadležna tijela djelotvorno prate i poduzimaju mjere potrebne za osiguravanje usklađenosti s ovom Direktivom, posebno s obvezama utvrđenima u člancima 18.**,** [...] 20. **i 23. Države članice mogu omogućiti nadležnim tijelima da daju prednost nadzoru koji se temelji na pristupu utemeljenom na procjeni rizika.**

2. Nadležna tijela u rješavanju kiberincidenata blisko surađuju s tijelima za zaštitu podataka, **nadležnim tijelima imenovanima na temelju Direktive (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata], nadzornim tijelima imenovanima na temelju Uredbe (EU) 910/2014 i drugim nadležnim tijelima imenovanima na temelju sektorskih zakonodavnih akata Unije.** [...]

3. Ne dovodeći u pitanje nacionalne zakonodavne i institucionalne okvire, države članice osiguravaju da, pri nadzoru usklađenosti tijela javne uprave s ovom Direktivom i provedbe mogućih sankcija za neusklađenost, nadležna tijela imaju odgovarajuće ovlasti za izvršavanje takvih zadaća uz operativnu neovisnost u odnosu na subjekte koji se nadziru. Države članice mogu odlučiti o uvođenju odgovarajućih, razmjernih i djelotvornih mjera nadzora i provedbe u odnosu na te subjekte u skladu s nacionalnim okvirima i pravnim poretkom.

Članak 29.

Nadzor i provedba za ključne subjekte

1. Države članice osiguravaju da su mjere nadzora ili provedbe određene ključnim subjektima s obzirom na obveze utvrđene u ovoj Direktivi učinkovite, razmjerne i odvraćajuće, uzimajući u obzir okolnosti svakog pojedinog slučaja.

2. Države članice osiguravaju da nadležna tijela pri izvršavanju svojih nadzornih zadaća u odnosu na ključne subjekte **slijede pristup utemeljen na procjeni rizika i** imaju ovlasti da te subjekte obvežu **barem** na sljedeće:

   (a) izravni i neizravni nadzor, uključujući nasumične provjere;

   (b) redovite revizije **sigurnosti**;

   (c) ciljane revizije sigurnosti na temelju procjena rizika ili dostupnih informacija povezanih s rizikom;

   (d) analize sigurnosti na temelju objektivnih, nediskriminirajućih, pravednih i transparentnih kriterija za procjenu rizika**, ako je to potrebno iz tehničkih razloga, u suradnji s dotičnim subjektom**;

   (e) zahtjeve za informacije potrebne za ocjenjivanje kibersigurnosnih mjera koje je donio subjekt, uključujući dokumentirane kibersigurnosne politike [...];

   (f) zahtjeve za pristup podacima, dokumentima ili bilo kojim informacijama potrebnima za obavljanje njihovih nadzornih zadaća;

   (g) zahtjeve za dokaze o provedbi kibersigurnosnih politika, kao što su rezultati revizija sigurnosti koje je proveo kvalificirani revizor i odgovarajući temeljni dokazi.

2.a Pri izvršavanju svojih nadzornih zadaća iz stavka 2. ovog članka nadležna tijela mogu uspostaviti nadzorne metodologije kojima se omogućuje određivanje prioriteta tih zadaća primjenom pristupa utemeljenog na procjeni rizika.

3. Pri izvršavanju svojih ovlasti iz stavka 2. točaka od (e) do (g), nadležna tijela navode svrhu zahtjeva i pobliže određuju tražene informacije.

4. Države članice osiguravaju da nadležna tijela pri izvršavanju svojih provedbenih ovlasti u odnosu na ključne subjekte imaju **barem** sljedeće ovlasti:

(a) izdavati upozorenja o neusklađenosti subjekata s obvezama utvrđenima u ovoj Direktivi;

(b) izdavati obvezujuće upute ili nalog kojim se od tih subjekata zahtijeva da uklone utvrđene nedostatke ili povrede obveza utvrđenih u ovoj Direktivi;

(c) naložiti tim subjektima da prestanu s postupanjem koje nije u skladu s obvezama utvrđenima u ovoj Direktivi i da ne ponavljaju takvo postupanje;

(d) naložiti tim subjektima da svoje mjere upravljanja rizicima i/ili obveze izvješćivanja usklade s obvezama iz članaka 18. i 20. na utvrđeni način i u utvrđenom roku;

(e) naložiti tim subjektima da obavijeste fizičke ili pravne osobe kojima pružaju usluge ili obavljaju aktivnosti na koje bi mogla utjecati ozbiljna kiberprijetnja o **prirodi prijetnje te o** svim mogućim zaštitnim ili korektivnim mjerama koje te fizičke ili pravne osobe mogu poduzeti kao odgovor na tu prijetnju;

(f) naložiti tim subjektima da u razumnom roku provedu preporuke dane na temelju revizije sigurnosti;

(g) [...]

(h) naložiti tim subjektima da objave aspekte nepoštovanja obveza predviđenih ovom Direktivom na utvrđeni način **ako takvo javno objavljivanje ne dovodi do štetne izloženosti dotičnog subjekta**;

(i) [...]

(j) odrediti ili zahtijevati da relevantna tijela ili sudovi u skladu s nacionalnim pravom izreknu upravnu novčanu kaznu na temelju članka 31. uz mjere iz točaka od (a) do (i) ovog stavka ili umjesto njih, ovisno o okolnostima svakog pojedinog slučaja.

5. Ako se provedbena djelovanja donesena na temelju stavka 4. točaka od (a) do (d) i točke (f) pokažu nedjelotvornima, države članice osiguravaju da nadležna tijela imaju ovlast utvrditi rok u kojem se od ključnog subjekta zahtijeva da poduzme radnje potrebne za ispravljanje nedostataka ili da ispuni zahtjeve tih tijela. Ako zatražene radnje nisu poduzete u zadanom roku, države članice osiguravaju da nadležna tijela imaju ovlasti:

(a) suspendirati ili zatražiti od certifikacijskog tijela ili tijela koje izdaje ovlaštenja **ili sudova u skladu s nacionalnim pravom** da suspendira certificiranje ili izdavanje ovlaštenja povezanih s dijelom ili svim uslugama koje ključni subjekt pruža ili s djelatnostima koje obavlja;

(b) nametnuti ili zahtijevati da relevantna tijela ili sudovi u skladu s nacionalnim pravom propišu privremenu zabranu obavljanja rukovoditeljskih dužnosti u tom ključnom subjektu svakoj osobi koja te dužnosti obavlja na razini glavnog izvršnog direktora ili pravnog zastupnika u tom ključnom subjektu te svakoj drugoj fizičkoj osobi koja se smatra odgovornom za povredu.

Te se sankcije primjenjuju samo dok subjekt ne poduzme potrebna djelovanja za otklanjanje nedostataka ili dok ne ispuni zahtjeve nadležnog tijela za koje su takve sankcije primijenjene.

Sankcije predviđene ovim stavkom ne primjenjuju se na subjekte javne uprave koji podliježu ovoj Uredbi.

6. Države članice osiguravaju da svaka fizička osoba koja je odgovorna za ključni subjekt ili djeluje kao njegov predstavnik na temelju ovlasti za zastupanje, ovlasti za donošenje odluka u njegovo ime ili ovlasti za izvršavanje kontrole nad tim subjektom ima ovlasti osigurati njegovu usklađenost s obvezama utvrđenima u ovoj Direktivi. Države članice osiguravaju da se te fizičke osobe mogu smatrati odgovornima za kršenje svojih dužnosti da osiguraju ispunjenje obveza utvrđenih u ovoj Direktivi. **U pogledu tijela javne uprave, ovom odredbom ne dovodi se u pitanje pravo država članica u pogledu odgovornosti javnih službenika te izabranih i imenovanih dužnosnika.**

7. Ako poduzimaju bilo koje provedbeno djelovanje ili primjenjuju bilo koju od sankcija na temelju stavaka 4. i 5., nadležna tijela poštuju prava na obranu i uzimaju u obzir okolnosti svakog pojedinačnog slučaja te propisno uzimaju u obzir barem:

   (a) ozbiljnost povrede i važnost prekršenih odredaba. Među povredama koje bi trebalo smatrati ozbiljnima nalaze se: opetovane povrede, neprijavljivanje ili neispravljanje incidenata sa znatnim negativnim učinkom, neuklanjanje nedostataka u skladu s obvezujućim uputama nadležnih tijela, ometanje revizija ili aktivnosti praćenja koje je naložilo nadležno tijelo nakon utvrđivanja povrede, pružanje lažnih ili izrazito netočnih informacija povezanih sa zahtjevima za upravljanje rizicima ili obvezama izvješćivanja iz članaka 18. i 20.;

(b) trajanje povrede, uključujući element ponovljenih povreda;

(c) stvarno prouzročenu štetu ili nastale gubitke ili potencijalnu štetu ili gubitke, u mjeri u kojoj ih je moguće utvrditi. Pri evaluaciji tog aspekta u obzir se uzimaju, među ostalim, stvarni ili potencijalni financijski ili gospodarski gubici, učinci na druge usluge, broj pogođenih ili potencijalno pogođenih korisnika;

(d) ima li povreda obilježje namjere ili nepažnje;

(e) mjere koje je subjekt poduzeo radi sprečavanja ili ublažavanja štete i/ili gubitaka;

(f) poštovanje odobrenih kodeksa ponašanja ili odobrenih mehanizama certificiranja;

(g) razinu suradnje fizičkih ili pravnih osoba koje nadležna tijela smatraju odgovornima.

8. Nadležna tijela detaljno obrazlažu svoje provedbene odluke. Prije donošenja takvih odluka nadležna tijela obavješćuju dotične subjekte o svojim preliminarnim nalazima i pružaju im razuman rok za podnošenje primjedaba**, osim u slučaju neposredne opasnosti**.

9. Države članice osiguravaju da njihova nadležna tijela **iz ove Direktive** obavješćuju relevantna nadležna tijela **unutar te iste** [...] države članice [...] imenovana na temelju Direktive (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] pri izvršavanju svojih nadzornih i provedbenih ovlasti kojima je cilj osigurati da ključni subjekt koji je utvrđen kao kritičan **[**ili kao subjekt istovjetan kritičnom subjektu**]** na temelju Direktive (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] ispunjava obveze na temelju ove Direktive. **Prema potrebi,**[...] nadležna tijela iz Direktive (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata][...] **mogu zatražiti** od nadležnih tijela **iz ove Direktive** [...] **da** izvršavaju svoje nadzorne i provedbene ovlasti nad ključnim subjektom iz područja primjene ove Direktive koji je ujedno utvrđen kao kritičan **[**ili istovjetan kritičnom subjektu**] na temelju Direktive (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata]**.

10. Države članice osiguravaju da njihova nadležna tijela iz ove Direktive obavješćuju Nadzorni forum na temelju članka 29. stavka 1. Uredbe (EU) XXXX/XXXX [DORA] pri izvršavanju svojih nadzornih i provedbenih ovlasti usmjerenih na osiguravanje usklađenosti ključnog subjekta imenovanog kao kritična treća strana pružatelj IKT usluga na temelju članka 28. Uredbe (EU) XXXX/XXXX [DORA], s obvezama na temelju ove Direktive.

10.a Države članice osiguravaju da njihova nadležna tijela iz ove Direktive obavješćuju relevantna nadležna tijela imenovana na temelju Uredbe (EU) 910/2014 pri izvršavanju svojih nadzornih i provedbenih ovlasti usmjerenih na osiguravanje usklađenosti subjekta imenovanog kao pružatelj usluga povjerenja na temelju Uredbe (EU) 910/2014, s obvezama na temelju ove Direktive.

Članak 30.

Nadzor i provedba za važne subjekte

1. Kada dobiju dokaz ili naznaku **ili informaciju** da važan subjekt **navodno** ne ispunjava obveze utvrđene u ovoj Direktivi, a posebno u člancima 18. i 20., države članice osiguravaju da nadležna tijela, ako je potrebno, poduzmu *ex post* nadzorne mjere.

2. Države članice osiguravaju da nadležna tijela pri izvršavanju svojih nadzornih zadaća u odnosu na važne subjekte **slijede pristup utemeljen na riziku i** imaju ovlasti da te subjekte obvežu **barem** na sljedeće:

   (a) izravni nadzor i neizravni *ex post* nadzor;

   (b) ciljane revizije sigurnosti na temelju procjena rizika ili dostupnih informacija povezanih s rizikom;

   (c) analize sigurnosti na temelju objektivnih, **nediskriminirajućih,** pravednih i transparentnih kriterija za procjenu rizika**, ako je to potrebno iz tehničkih razloga, u suradnji s dotičnim subjektom**;

   (d) zahtjeve za informacije potrebne za *ex post* ocjenjivanje kibersigurnosnih mjera [...];

   (e) zahtjeve za pristup podacima, dokumentima i/ili informacijama potrebnima za obavljanje njihovih nadzornih zadaća;

   (ea) zahtjeve za dokaze o provedbi kibersigurnosnih politika, kao što su rezultati revizija sigurnosti koje je proveo kvalificirani revizor i odgovarajući temeljni dokazi.

2.a Pri izvršavanju svojih nadzornih zadaća iz stavka 2. ovog članka nadležna tijela mogu uspostaviti nadzorne metodologije kojima se omogućuje određivanje prioriteta tih zadaća primjenom pristupa utemeljenog na procjeni rizika.

3. Pri izvršavanju svojih ovlasti iz stavka 2. točaka od (d) **do (ea)** nadležna tijela navode svrhu zahtjeva i pobliže određuju tražene informacije.

4. Države članice osiguravaju da nadležna tijela pri izvršavanju svojih provedbenih ovlasti u pogledu važnih subjekata imaju **barem** sljedeće ovlasti:

(a) izdavati upozorenja o neusklađenosti subjekata s obvezama utvrđenima u ovoj Direktivi;

(b) izdavati obvezujuće upute ili nalog kojim se od tih subjekata zahtijeva da uklone utvrđene nedostatke ili povrede obveza utvrđenih u ovoj Direktivi;

(c) naložiti tim subjektima da prestanu s postupanjem koje nije u skladu s obvezama utvrđenima u ovoj Direktivi i da ne ponavljaju takvo postupanje;

(d) naložiti tim subjektima da svoje mjere upravljanja rizicima ili obveze izvješćivanja usklade s obvezama iz članaka 18. i 20. na utvrđeni način i u utvrđenom roku;

(e) naložiti tim subjektima da obavijeste fizičke ili pravne osobe kojima pružaju usluge ili obavljaju aktivnosti na koje bi mogla utjecati ozbiljna kiberprijetnja o **prirodi te prijetnje te o** svim mogućim zaštitnim ili korektivnim mjerama koje te fizičke ili pravne osobe mogu poduzeti kao odgovor na tu prijetnju;

(f) naložiti tim subjektima da u razumnom roku provedu preporuke dane na temelju revizije sigurnosti;

(g) naložiti tim subjektima da objave aspekte nepoštovanja obveza predviđenih ovom Direktivom na utvrđeni način **ako takvo javno objavljivanje ne dovodi do štetne izloženosti dotičnog subjekta**;

(h) [...]

(i) odrediti ili zahtijevati da relevantna tijela ili sudovi u skladu s nacionalnim pravom izreknu upravnu novčanu kaznu na temelju članka 31. uz mjere iz točaka od (a) do (h) ovog stavka ili umjesto njih, ovisno o okolnostima svakog pojedinog slučaja.

5. Članak 29. stavci od 6. do 8. primjenjuju se i na nadzorne i provedbene mjere predviđene ovim člankom za važne subjekte [...].

— *Članak 31.*

Opći uvjeti za izricanje upravnih novčanih kazni ključnim i važnim subjektima

1. Države članice osiguravaju da je izricanje upravnih novčanih kazni ključnim i važnim subjektima na temelju ovog članka u pogledu povreda obveza utvrđenih u ovoj Direktivi u svakom pojedinačnom slučaju učinkovito, razmjerno i odvraćajuće.

2. Upravne novčane kazne izriču se uz mjere iz članka 29. stavka 4. točaka od (a) do (i), članka 29. stavka 5. i članka 30. stavka 4. točaka od (a) do (h) ili umjesto njih, ovisno o okolnostima svakog pojedinog slučaja.

3. Pri odlučivanju o izricanju upravne novčane kazne i o njezinu iznosu dužna se pažnja u svakom pojedinom slučaju posvećuje barem elementima predviđenima u članku 29. stavku 7.

4. Države članice osiguravaju da povrede obveza utvrđenih u članku 18. ili članku 20. **koje su počinili ključni subjekti** podliježu, u skladu sa stavcima 2. i 3. ovog članka, upravnim novčanim kaznama u maksimalnom iznosu od najmanje **4**[...] 000 000 EUR ili**, u slučaju pravne osobe,** [...] 2 % ukupnog godišnjeg prometa na svjetskoj razini poduzeća kojem pripada ključni [...] subjekt u prethodnoj financijskoj godini, ovisno o tome koji je iznos veći.

4.a Države članice osiguravaju da povrede obveza utvrđenih u članku 18. ili članku 20. koje su počinili važni subjekti podliježu, u skladu sa stavcima 2. i 3. ovog članka, upravnim novčanim kaznama u maksimalnom iznosu od najmanje 2 000 000 EUR ili, u slučaju pravne osobe, 1 % ukupnog godišnjeg prometa na svjetskoj razini poduzeća kojem pripada važni subjekt u prethodnoj financijskoj godini, ovisno o tome koji je iznos veći.

5. Države članice mogu predvidjeti ovlast izricanja periodičnih novčanih kazni kako bi se ključni ili važni subjekt primorao da prestane vršiti povredu u skladu s prethodnom odlukom nadležnog tijela.

6. Ne dovodeći u pitanje ovlasti nadležnih tijela u skladu s člancima 29. i 30., svaka država članica može utvrditi pravila o tome mogu li se i u kojoj mjeri subjektima javne uprave iz članka 4. stavka 23. izreći upravne novčane kazne, prema obvezama predviđenima ovom Direktivom.

6.a Ako pravnim sustavom države članice nisu predviđene upravne novčane kazne, države članice osiguravaju da se ovaj članak može primjenjivati na način da novčanu kaznu pokreće nadležno tijelo, a izriču je nadležni nacionalni sudovi, osiguravajući pritom da su ti pravni lijekovi djelotvorni i imaju istovjetan učinak kao upravne novčane kazne koje izriču nadležna tijela. U svakom slučaju novčane kazne koje se izriču moraju biti učinkovite, razmjerne i odvraćajuće. Te države članice do […] obavješćuju Komisiju o odredbama svojih zakona koje donesu na temelju ovog stavka te, bez odgode, o svim daljnjim izmjenama zakona ili izmjeni koja na njih utječe.

Članak 32.

Povrede koje uključuju povredu osobnih podataka

1. Ako **tijekom nadzora ili provedbe** nadležna tijela [...] **saznaju** da povreda obveza utvrđenih u člancima 18. i 20. **ove Direktive** koju je počinio ključni ili važni subjekt **može** obuhvaćati [...] povredu osobnih podataka iz članka 4. stavka 12. Uredbe (EU) 2016/679 o kojoj se obavješćuje na temelju članka 33. te uredbe, u razumnom roku**, bez nepotrebne odgode,** obavješćuju nadzorna tijela nadležna na temelju 55. i 56. te uredbe [...].

2. Ako nadzorna tijela nadležna u skladu s člancima 55. i 56. Uredbe (EU) 2016/679 odluče izvršiti svoje ovlasti na temelju članka 58. **stavka 2.** točke (i) te uredbe i izreći upravnu novčanu kaznu, nadležna tijela **iz članka 8. ove Direktive** ne izriču upravnu novčanu kaznu za [...] povredu **istim djelom iz** [...] članka 31. ove Direktive. Međutim, nadležna tijela mogu primijeniti provedbena djelovanja ili izvršiti ovlasti sankcioniranja predviđene u članku 29. stavku 4. točkama od (a) do (i), članku 29. stavku 5. i članku 30. stavku 4. točkama od (a) do (h) ove Direktive.

3. Ako je nadzorno tijelo nadležno na temelju Uredbe (EU) 2016/679 osnovano u državi članici drugačijoj od one u kojoj je osnovano nadležno tijelo, nadležno tijelo može obavijestiti nadzorno tijelo osnovano u istoj državi članici.

Članak 33.

Sankcije

1. Države članice utvrđuju pravila o sankcijama koje se primjenjuju na kršenja nacionalnih odredaba donesenih na temelju ove Direktive i poduzimaju sve potrebne mjere kako bi osigurale njihovu provedbu. Predviđene sankcije moraju biti učinkovite, razmjerne i odvraćajuće.

2. Države članice u roku od [dvije] godine od stupanja na snagu ove Direktive obavješćuju Komisiju o tim pravilima i mjerama te joj bez nepotrebne odgode priopćuju sve naknadne izmjene koje utječu na ta pravila i mjere.

Članak 34.

Uzajamna pomoć

1. Ako ključni ili važni subjekt pruža usluge u više od jedne države članice ili [...] **pruža usluge u jednoj ili više država članica**, ali se njegovi mrežni i informacijski sustavi nalaze u drugoj državi članici ili u više njih, [...] **nadležna tijela dotičnih država članica** [...] surađuju i međusobno si pomažu ako je potrebno. Ta suradnja podrazumijeva najmanje sljedeće:

(a) nadležna tijela koja primjenjuju nadzorne ili provedbene mjere u državi članici preko jedinstvene kontaktne točke obavješćuju nadležna tijela u drugim dotičnim državama članicama o poduzetim nadzornim i provedbenim mjerama [...] te se savjetuju s njima;

(b) nadležno tijelo može zatražiti od drugog nadležnog tijela da poduzme nadzorne ili provedbene mjere [...];

(c) nakon primitka opravdanog zahtjeva drugog nadležnog tijela, nadležno tijelo pruža tom tijelu pomoć **razmjernu resursima s kojima raspolaže** kako bi se nadzorne ili provedbene aktivnosti [...] mogle provesti na djelotvoran, učinkovit i dosljedan način. Takva uzajamna pomoć može obuhvaćati zahtjeve za informacije i nadzorne mjere, uključujući zahtjeve za provođenje izravnog ili neizravnog nadzora ili ciljanih revizija sigurnosti. Nadležno tijelo kojem je upućen zahtjev za pomoć ne može odbiti taj zahtjev osim u slučaju da se, nakon konzultacija s drugim dotičnim tijelima, [...] utvrdi da to tijelo nije nadležno za pružanje zatražene pomoći **ili da nema potrebne resurse** ili da zatražena pomoć nije razmjerna nadzornim zadaćama nadležnog tijela koje se obavljaju [...] **ili se zahtjev odnosi na informacije ili uključuje aktivnosti koje su u sukobu s nacionalnom sigurnošću ili javnom sigurnošću ili obranom te države članice**.

2. Prema potrebi i uz međusobnu suglasnost, nadležna tijela iz različitih država članica mogu provoditi zajedničke nadzorne aktivnosti [...].

POGLAVLJE VII.

Prijelazne i završne odredbe

Članak 35.

Preispitivanje

Komisija periodično preispituje funkcioniranje ove Direktive te podnosi izvješće Europskom parlamentu i Vijeću. U izvješću se posebno ocjenjuje relevantnost sektora, podsektora, veličine i vrste subjekata iz priloga I. i II. za funkcioniranje gospodarstva i društva u pogledu kibersigurnosti. U [...] svrhu **preispitivanja** [...] Komisija uzima u obzir izvješća [...] mreže CSIRT-ova o iskustvu stečenom na [...] operativnoj razini. Prvo izvješće podnosi se do …□54 mjeseca od datuma stupanja na snagu ove Direktive□.

Članak 36.

[...]

[...]

[...]

Članak 37.

Postupak odbora

1. Komisiji pomaže odbor. Navedeni odbor je odbor u smislu Uredbe (EU) br. 182/2011.

2. Pri upućivanju na ovaj stavak primjenjuje se članak 5. Uredbe (EU) br 182/2011.

3. Kada se mišljenje odbora treba dobiti pisanim postupkom, navedeni postupak završava bez rezultata kada u roku za davanje mišljenja to odluči predsjednik odbora ili to zahtijeva član odbora.

Članak 38.

Prenošenje

1. Države članice najkasnije do … [...]**24** mjeseca nakon dana stupanja na snagu ove Direktive donose i objavljuju zakone i druge propise koji su potrebni radi usklađivanja s ovom Direktivom. One o tome odmah obavješćuju Komisiju. Primjenjuju te mjere od … [jedan dan nakon datuma iz prvog podstavka].

2. Kada države članice donose te mjere, one sadržavaju upućivanje na ovu Direktivu ili se na nju upućuje prilikom njihove službene objave. Načine tog upućivanja određuju države članice.

Članak 39.

Izmjena Uredbe (EU) br. 910/2014

U Uredbi (EU) br. 910/2014 briše se članak 19. [...] **s učinkom od … [datum roka za prenošenje ove Direktive]**.

Članak 40.

Izmjena Direktive (EU) 2018/1972

U Direktivi (EU) 2018/1972 brišu se članci 41. i 41. [...] **s učinkom od … [datum roka za prenošenje ove Direktive]**.

Članak 41.

Stavljanje izvan snage

Direktiva (EU) 2016/1148 stavlja se izvan snage s učinkom od ... [datum roka za prenošenje ove Direktive].

Upućivanja na Direktivu (EU) 2016/1148 smatraju se upućivanjima na ovu Direktivu i tumače se u skladu s korelacijskom tablicom iz Priloga II[...].

Članak 42.

Stupanje na snagu

Ova Direktiva stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Članak 43.

Adresati

Ova je Direktiva upućena državama članicama.

Sastavljeno u Bruxellesu

Za Europski parlament	*Za Vijeće*
Predsjednik	*Predsjednik*

PRILOG I.

SEKTORI, PODSEKTORI I VRSTE SUBJEKATA

Sektor	Podsektor	Vrsta subjekta
1. Energetika	(a) električna energija	— elektroenergetska poduzeća iz članka 2. točke 57. Direktive (EU) 2019/944, koja obavljaju funkciju „opskrbe” iz članka 2. točke 12. te direktive ([39])
		— operatori distribucijskog sustava iz članka 2. točke 29. Direktive (EU) 2019/944
		— operatori prijenosnog sustava iz članka 2. točke 35. Direktive (EU) 2019/944
		— proizvođači iz članka 2. točke 38. Direktive (EU) 2019/944
		— nominirani operatori tržišta električne energije iz članka 2. točke 8. Uredbe (EU) 2019/943 ([40])
		— sudionici na tržištu električne energije iz članka 2. točke 25. Uredbe (EU) 2019/943 koji pružaju usluge agregiranja, upravljanja potrošnjom ili skladištenja energije iz članka 2. točaka 18., 20. i 59. Direktive (EU) 2019/944

[39] Direktiva (EU) 2019/944 Europskog parlamenta i Vijeća od 5. lipnja 2019. o zajedničkim pravilima za unutarnje tržište električne energije i izmjeni Direktive 2012/27/EU (SL L 158, 14.6.2019., str. 125.).

[40] Uredba (EU) 2019/943 Europskog parlamenta i Vijeća o unutarnjem tržištu električne energije (SL L 158, 14.6.2019., str. 54.).

	(b) centralizirano grijanje i hlađenje	— centralizirano grijanje ili centralizirano hlađenje iz članka 2. točke 19. Direktive (EU) 2018/2001 ([41]) o promicanju uporabe energije iz obnovljivih izvora
	(c) nafta	— operatori naftovoda
		— operatori proizvodnje nafte, rafinerija i tvornica nafte te njezina skladištenja i prijenosa
		— središnja tijela za zalihe nafte iz članka 2. točke (f) Direktive Vijeća 2009/119/EZ ([42])
	(d) plin	— poduzeća za opskrbu iz članka 2. točke 8. Direktive (EU) 2009/73/EZ ([43])
		— operatori distribucijskog sustava iz članka 2. točke 6. Direktive 2009/73/EZ
		— operatori transportnog sustava iz članka 2. točke 4. Direktive 2009/73/EZ
		— operatori sustava skladišta iz članka 2. točke 10. Direktive 2009/73/EZ

41 Direktiva (EU) 2018/2001 Europskog parlamenta i Vijeća od 11. prosinca 2018. o promicanju uporabe energije iz obnovljivih izvora (SL L 328, 21.12.2018., str. 82.).

42 Direktiva Vijeća 2009/119/EZ od 14. rujna 2009. o obvezi država članica da održavaju minimalne zalihe sirove nafte i/ili naftnih derivata (SL L 265, 9.10.2009., str. 9.).

43 Direktiva 2009/73/EZ Europskog parlamenta i Vijeća od 13. srpnja 2009. o zajedničkim pravilima za unutarnje tržište prirodnog plina i stavljanju izvan snage Direktive 2003/55/EZ (SL L 211, 14.8.2009., str. 94.).

		— operatori terminala za UPP iz članka 2. točke 12. Direktive 2009/73/EZ
		— poduzeća za prirodni plin iz članka 2. točke 1. Direktive 2009/73/EZ
		— operatori postrojenja za rafiniranje i obradu prirodnog plina
	(e) vodik	operatori proizvodnje, skladištenja i prijenosa vodika
2. Promet	(a) zračni promet	— zračni prijevoznici iz članka 3. točke 4. Uredbe (EZ) br. 300/2008 ([44]) **koji se upotrebljavaju u komercijalne svrhe**
		— upravna tijela zračne luke iz članka 2. točke 2. Direktive 2009/12/EZ ([45]), zračne luke iz članka 2. točke 1. te direktive, uključujući osnovne zračne luke navedene u odjeljku 2. Priloga II. Uredbi (EU) br. 1315/2013 ([46]) te tijela koja upravljaju pomoćnim objektima u zračnim lukama
		— operatori kontrole upravljanja prometom koji pružaju usluge kontrole zračnog prometa (ATC) iz

[44] Uredba (EZ) br. 300/2008 Europskog parlamenta i Vijeća od 11. ožujka 2008. o zajedničkim pravilima u području zaštite civilnog zračnog prometa i stavljanju izvan snage Uredbe (EZ) br. 2320/2002 (SL L 97, 9.4.2008., str. 72.).

[45] Direktiva 2009/12/EZ Europskog parlamenta i Vijeća od 11. ožujka 2009. o naknadama zračnih luka (SL L 70, 14.3.2009., str. 11.).

[46] Uredba (EZ) br. 1315/2013 Europskog parlamenta i Vijeća od 11. prosinca 2013. o smjernicama Unije za razvoj transeuropske prometne mreže i stavljanju izvan snage Odluke br. 661/2010/EU (SL L 348, 20.12.2013., str. 1.).

		članka 2. točke 1. Uredbe (EZ) br. 549/2004 ([47])
	(b) željeznički promet	— upravitelji infrastrukture iz članka 3. točke 2. Direktive 2012/34/EU ([48])
		— željeznički prijevoznici iz članka 3. točke 1. Direktive 2012/34/EU, među ostalim i operatori uslužnih objekata iz članka 3. točke 12. Direktive 2012/34/EU
	(c) vodeni promet	— kompanije za prijevoz putnika unutarnjim plovnim putovima, morem i duž obale te kompanije za prijevoz tereta unutarnjim plovnim putovima, morem i duž obale iz Priloga I. Uredbi (EZ) br. 725/2004([49]), ne uključujući pojedinačna plovila kojima upravljaju te kompanije
		— upravljačka tijela luka iz članka 3. točke 1. Direktive 2005/65/EZ ([50]), uključujući njihove luke iz članka 2. točke 11. Uredbe (EZ) br. 725/2004 te subjekti koji upravljaju postrojenjima i opremom u lukama

47 Uredba (EZ) br. 549/2004 Europskog parlamenta i Vijeća od 10. ožujka 2004. o utvrđivanju okvira za stvaranje jedinstvenog europskog neba (Okvirna uredba) (SL L 96, 31.3.2004., str. 1.).

48 Direktiva 2012/34/EU Europskog parlamenta i Vijeća od 21. studenoga 2012. o uspostavi jedinstvenog Europskog željezničkog prostora (SL L 343, 14.12.2012., str. 32.).

49 Uredba (EZ) br. 725/2004 Europskog parlamenta i Vijeća od 31. ožujka 2004. o jačanju sigurnosne zaštite brodova i luka (SL L 129, 29.4.2004., str. 6.).

50 Direktiva 2005/65/EZ Europskog parlamenta i Vijeća od 26. listopada 2005. o jačanju sigurnosne zaštite luka (SL L 310, 25.11.2005., str. 28.).

		— služba za nadzor i upravljanje pomorskim prometom iz članka 3. točke (o) Direktive 2002/59/EZ ([51])
	(d) cestovni promet	— tijela nadležna za ceste iz članka 2. točke 12. Delegirane uredbe Komisije (EU) 2015/962 ([52]) odgovorna za kontrolu upravljanja prometom**, osim javnih subjekata kojima upravljanje prometom ili operatori inteligentnih prometnih sustava nisu ključni dio njihove opće djelatnosti**
		— operatori inteligentnih prometnih sustava iz članka 4. točke 1. Direktive 2010/40/EU ([53])
3. Bankarstvo		— kreditne institucije iz članka 4. točke 1. Uredbe (EU) br. 575/2013 ([54]), **[osim onih iz članka 2. stavka 5. točke 8. Direktive 2013/36/EU koje su izuzete u skladu s člankom 2. stavkom 4. Uredbe XX [DORA]]**

51 Direktiva 2002/59/EZ Europskog parlamenta i Vijeća od 27. lipnja 2002. o uspostavi sustava nadzora plovidbe i informacijskog sustava Zajednice i stavljanju izvan snage Direktive Vijeća 93/75/EEZ (SL L 208, 5.8.2002., str. 10.).

52 Delegirana uredba Komisije (EU) 2015/962 od 18. prosinca 2014. o dopuni Direktive 2010/40/EU Europskog parlamenta i Vijeća u pogledu pružanja usluga prometnih informacija u cijeloj Europskoj uniji u realnom vremenu (SL L 157, 23.6.2015., str. 21.).

53 Direktiva 2010/40/EU Europskog parlamenta i Vijeća od 7. srpnja 2010. o okviru za uvođenje inteligentnih prometnih sustava u cestovnom prometu i za veze s ostalim vrstama prijevoza (SL L 207, 6.8.2010., str. 1.).

54 Uredba (EU) br. 575/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o bonitetnim zahtjevima za kreditne institucije i investicijska društva i o izmjeni Uredbe (EU) br. 648/2012 (SL L 176, 27.6.2013., str. 1.).

4. Infrastruktura financijskog tržišta		— operatori mjestâ trgovanja iz članka 4. točke 24. Direktive 2014/65/EU ([55])
		— središnje druge ugovorne strane (CCP-i) iz članka 2. točke 1. Uredbe (EU) br. 648/2012 ([56])
5. Zdravstvo		— pružatelji zdravstvene zaštite iz članka 3. točke (g) Direktive 2011/24/EU ([57])
		— referentni laboratoriji EU-a iz članka 15. Uredbe XXXX/XXXX o ozbiljnim prekograničnim prijetnjama zdravlju ([58])
		— subjekti koji obavljaju djelatnosti istraživanja i razvoja lijekova iz članka 1. točke 2. Direktive 2001/83/EZ ([59]) — subjekti koji proizvode osnovne farmaceutske proizvode i farmaceutske pripravke iz područja C odjeljka 21. NACE Rev. 2 — subjekti koji proizvode medicinske proizvode koji se smatraju ključnima tijekom izvanrednog stanja u području javnog zdravlja („popis ključnih medicinskih proizvoda u slučaju izvanrednog stanja u području javnog

[55] Direktiva 2014/65/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištu financijskih instrumenata i izmjeni Direktive 2002/92/EZ i Direktive 2011/61/EU (SL L 173, 12.6.2014., str. 349.).

[56] Uredba (EU) br. 648/2012 Europskog parlamenta i Vijeća od 4. srpnja 2012. o OTC izvedenicama, središnjoj drugoj ugovornoj strani i trgovinskom repozitoriju (SL L 201, 27.7.2012., str. 1.).

[57] Direktiva 2011/24/EU Europskog parlamenta i Vijeća od 9. ožujka 2011. o primjeni prava pacijenata u prekograničnoj zdravstvenoj skrbi (SL L 88, 4.4.2011., str. 45.).

[58] [Uredba Europskog parlamenta i Vijeća o ozbiljnim prekograničnim prijetnjama zdravlju i stavljanju izvan snage Odluke br. 1082/2013/EU, upućivanje će se ažurirati nakon donošenja prijedloga COM(2020) 727 final.]

[59] Direktiva 2001/83/EZ Europskog parlamenta i Vijeća od 6. studenoga 2001. o zakoniku Zajednice o lijekovima za humanu primjenu (SL L 311, 28.11.2001., str. 67.).

		zdravlja") iz članka 20. Uredbe XXXX ([60])
6. Voda za piće		dobavljači i distributeri vode namijenjene za ljudsku potrošnju iz članka 2. stavka 1. točke (a) Direktive Vijeća 98/83/EZ ([61]), ali isključujući distributere kojima distribucija vode za ljudsku potrošnju čini samo dio općenite djelatnosti distribucije druge robe i proizvoda **koja nije ključna** [...]
7. Otpadne vode		poduzeća koja prikupljaju, odlažu ili pročišćavaju komunalne otpadne vode, otpadne vode iz kućanstva i industrijske otpadne vode iz članka 2. točaka od 1. do 3. Direktive Vijeća 91/271/EEZ ([62])**, ali isključujući poduzeća kojima prikupljanje, odlaganje ili pročišćavanje komunalnih otpadnih voda, otpadnih voda iz kućanstva i industrijskih otpadnih voda nije ključni dio njihove općenite djelatnosti** [...]
8. Digitalna infrastruktura		— pružatelji središta za razmjenu internetskog prometa
		— pružatelji DNS usluga**, osim operatora korijenskih poslužitelja naziva**
		— registri naziva vršnih domena
		— pružatelji usluga računalstva u oblaku

60 [Uredba Europskog parlamenta i Vijeća o jačanju uloge Europske agencije za lijekove u pripravnosti za krizne situacije i upravljanju njima u području lijekova i medicinskih proizvoda, upućivanje će se ažurirati nakon donošenja prijedloga COM(2020) 725 final.]

61 Direktiva Vijeća 98/83/EZ od 3. studenoga 1998. o kvaliteti vode namijenjene za ljudsku potrošnju (SL L 330, 5.12.1998., str. 32.).

62 Direktiva Vijeća 91/271/EEZ od 21. svibnja 1991. o pročišćavanju komunalnih otpadnih voda (SL L 135, 30.5.1991., str. 40.).

		— pružatelji usluga podatkovnog centra
		— pružatelji mreže za isporuku sadržaja
		— pružatelji usluga povjerenja iz članka 3. točke 19. Uredbe (EU) br. 910/2014 ([63])
		— pružatelji javnih elektroničkih komunikacijskih mreža iz članka 2. točke 8. Direktive (EU) 2018/1972 ([64]) ili pružatelji elektroničkih komunikacijskih usluga iz članka 2. točke 4. Direktive (EU) 2018/1972 ako su njihove usluge javno dostupne
8.a Upravljanje IKT uslugama **(B2B)**		— **pružatelji upravljanih usluga (MSP)** — **pružatelji upravljanih sigurnosnih usluga (MSSP)**
9. **Tijela** javne uprave		— tijela središnje državne uprave **kako ih je definirala država članica u skladu s nacionalnim pravom** — [...][65][...] — [...]
10. Svemir		— operatori zemaljske infrastrukture, koji su u vlasništvu, kojima upravljaju i koje vode države članice ili privatne

63 Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (SL L 257, 28.8.2014., str. 73.).

64 Direktiva (EU) 2018/1972 Europskog parlamenta i Vijeća od 11. prosinca 2018. o Europskom zakoniku elektroničkih komunikacija (SL L 321, 17.12.2018., str. 36.).

65 [...]

		osobe te koji podupiru pružanje usluga u svemiru, isključujući pružatelje javnih elektroničkih komunikacijskih mreža iz članka 2. točke 8. Direktive (EU) 2018/1972

PRILOG II.

SEKTORI, PODSEKTORI I VRSTE SUBJEKATA

Sektor	Podsektor	Vrsta subjekta
1. Poštanske i kurirske usluge		pružatelji poštanskih usluga iz članka 2. točke 1. Direktive 97/67/EZ ([66]), **uključujući** [...] pružatelje kurirskih usluga
2. Gospodarenje otpadom		poduzeća koja se bave gospodarenjem otpadom iz članka 3. točke 9. Direktive 2008/98/EZ ([67]), ali isključujući poduzeća kojima gospodarenje otpadom nije glavna gospodarska djelatnost

[66] Direktiva 97/67/EZ Europskog parlamenta i Vijeća od 15. prosinca 1997. o zajedničkim pravilima za razvoj unutarnjeg tržišta poštanskih usluga u Zajednici i poboljšanje kvalitete usluga (SL L 15, 21.1.1998., str. 14.)**, kako je izmijenjena Direktivom 2008/6/EZ Europskog parlamenta i Vijeća od 20. veljače 2008. o izmjeni Direktive 97/67/EZ u pogledu potpunog postizanja unutarnjeg tržišta poštanskih usluga u Zajednici (SL L 52, 27.2.2008., str. 3.)**.

[67] Direktiva 2008/98/EZ Europskog parlamenta i Vijeća od 19. studenoga 2008. o otpadu i stavljanju izvan snage određenih direktiva (SL L 312, 22.11.2008., str. 3.).

3. Izrada, proizvodnja i distribucija kemikalija		poduzeća koja se bave izradom[...] i distribucijom tvari i [...] **pripravaka** iz članka 3. točaka[...] 9. i 14. Uredbe (EZ) br. 1907/2006 ([68]) **i poduzeća koja se bave proizvodnjom proizvoda iz članka 3. točke 3. te uredbe iz tvari ili pripravaka**
4. Proizvodnja, prerada i distribucija hrane		poduzeća za poslovanje s hranom iz članka 3. točke 2. Uredbe (EZ) br. 178/2002 ([69]) **koja se bave veleprodajom te industrijskom proizvodnjom i preradom**
5. Proizvodnja	(a) proizvodnja medicinskih proizvoda i *in vitro* dijagnostičkih medicinskih proizvoda	subjekti koji proizvode medicinske proizvode iz članka 2. točke 1. Uredbe (EU) 2017/745 ([70]) i subjekti koji proizvode *in vitro* dijagnostičke medicinske proizvode iz članka 2. točke 2. Uredbe (EU) 2017/746 ([71]), osim subjekata koji proizvode medicinske proizvode navedene u Prilogu 1. točki 5.

[68] Uredba (EZ) br. 1907/2006 Europskog parlamenta i Vijeća od 18. prosinca 2006. o registraciji, evaluaciji, autorizaciji i ograničavanju kemikalija (REACH) i osnivanju Europske agencije za kemikalije te o izmjeni Direktive 1999/45/EZ i stavljanju izvan snage Uredbe Vijeća (EEZ) br. 793/93 i Uredbe Komisije (EZ) br. 1488/94 kao i Direktive Vijeća 76/769/EEZ i direktiva Komisije 91/155/EEZ, 93/67/EEZ, 93/105/EZ i 2000/21/EZ (SL L 396, 30.12.2006., str. 1.).

[69] Uredba (EZ) br. 178/2002 Europskog parlamenta i Vijeća od 28. siječnja 2002. o utvrđivanju općih načela i uvjeta zakona o hrani, osnivanju Europske agencije za sigurnost hrane te utvrđivanju postupaka u područjima sigurnosti hrane (SL L 31, 1.2.2002., str. 1.).

[70] Uredba (EU) 2017/745 Europskog parlamenta i Vijeća od 5. travnja 2017. o medicinskim proizvodima, o izmjeni Direktive 2001/83/EZ, Uredbe (EZ) br. 178/2002 i Uredbe (EZ) br. 1223/2009 te o stavljanju izvan snage direktiva Vijeća 90/385/EEZ i 93/42/EEZ (SL L 117, 5.5.2017., str. 1.).

[71] Uredba (EU) 2017/746 Europskog parlamenta i Vijeća od 5. travnja 2017. o *in vitro* dijagnostičkim medicinskim proizvodima te o stavljanju izvan snage Direktive 98/79/EZ i Odluke Komisije 2010/227/EU (SL L 117, 5.5.2017., str. 176.).

	(b) proizvodnja računala te elektroničkih i optičkih proizvoda	poduzeća koja obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 26. NACE Rev. 2
	(c) proizvodnja električne opreme	poduzeća koja obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 27. NACE Rev. 2
	(d) proizvodnja strojeva i uređaja, d.n.	poduzeća koja obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 28. NACE Rev. 2
	(e) proizvodnja motornih vozila, prikolica i poluprikolica	poduzeća koja obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 29. NACE Rev. 2
	(f) proizvodnja ostale opreme za prijevoz	poduzeća koja obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 30. NACE Rev. 2
6. Pružatelji digitalnih usluga		— pružatelji internetskih tržišta
		— pružatelji internetskih tražilica
		— pružatelji platforme za usluge društvenih mreža