EUROPSKA UNIJA

EUROPSKI PARLAMENT **VIJEĆE**

Strasbourg, 14. prosinca 2022.
(OR. en)

2020/0359(COD)
LEX 2202

PE-CONS 32/2/22
REV 2

CYBER 239
TELECOM 295
CSC 290
CSCI 97
DATAPROTECT 202
JAI 946
MI 510
CODEC 991

DIREKTIVA EUROPSKOG PARLAMENTA I VIJEĆA O MJERAMA ZA VISOKU ZAJEDNIČKU RAZINU KIBERSIGURNOSTI ŠIROM UNIJE, IZMJENI UREDBE (EU) br. 910/2014 I DIREKTIVE (EU) 2018/1972 I STAVLJANJU IZVAN SNAGE DIREKTIVE (EU) 2016/1148 (DIREKTIVA NIS 2)

DIREKTIVA (EU) 2022/…
EUROPSKOG PARLAMENTA I VIJEĆA

od 14. prosinca 2022.

o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2)

(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 Europske središnje banke[1],

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora[2],

nakon savjetovanja s Odborom regija,

u skladu s redovnim zakonodavnim postupkom[3],

---

1 SL C 233, 16.6.2022., str. 22.
2 SL C 286, 16.7.2021., str. 170.
3 Stajalište Europskog parlamenta od 10. studenoga 2022. (još nije objavljeno u Službenom listu) i Odluka Vijeća od 28. studenoga 2022.

budući da:

(1) Cilj Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća[1] 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 incidenata, čime se doprinosi sigurnosti Unije i učinkovitom funkcioniranju njezina gospodarstva i društva.

(2) Od stupanja na snagu Direktive (EU) 2016/1148 ostvaren je znatan napredak u povećanju Unijine razine kiberotpornosti. 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 za sigurnost mrežnih i informacijskih sustava uvođenjem nacionalnih strategija za sigurnost mrežnih i informacijskih sustava te uspostavom nacionalnih kapaciteta i provedbom regulatornih mjera kojima su obuhvaćeni ključna infrastruktura i subjekti koje je utvrdila svaka država članica. Direktiva (EU) 2016/1148 doprinijela je i suradnji na razini Unije osnivanjem skupine za suradnju i mreže nacionalnih timova za odgovor na računalne sigurnosne incidente. Neovisno o tim postignućima, preispitivanjem Direktive (EU) 2016/1148 otkriveni su svojstveni nedostaci zbog kojih se njome ne može učinkovito odgovoriti na aktualne i nove izazove u području kibersigurnosti.

[1] 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, 19.7.2016., str. 1.).

(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 kiberprijetnji te time i novih izazova koji zahtijevaju prilagođene, koordinirane i inovativne odgovore u svim državama članicama. Incidenti su sve brojniji, sofisticiraniji, učestaliji, većih razmjera i utjecaja te predstavljaju veliku prijetnju funkcioniranju mrežnih i informacijskih sustava. Zbog toga incidenti mogu ugroziti obavljanje gospodarskih djelatnosti na unutarnjem tržištu, uzrokovati financijski gubitak, 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. Nadalje, kibersigurnost je ključan čimbenik koji brojnim kritičnim sektorima omogućuje da se uspješno prilagode na digitalnu transformaciju i u potpunosti iskoriste gospodarske, socijalne i održive koristi digitalizacije.

(4) Pravna osnova Direktive (EU) 2016/1148 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 djelatnosti koje su gospodarski važne 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 subjektima koji robu ili usluge nude prekogranično. 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 takve prekogranične djelatnosti. Nadalje, mogućnost neodgovarajuće definiranja ili provedbe kibersigurnosnih zahtjeva u jednoj državi članici može utjecati na razinu kibersigurnosti drugih država članica, posebno s obzirom na intenzitet prekograničnih razmjena. 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 razlike postoje i u provedbi odredaba Direktive (EU) 2016/1148 o nadzoru i izvršavanju.

(5) Sve te razlike dovode do fragmentacije unutarnjeg tržišta i mogu štetno utjecati na njegovo funkcioniranje, posebno na prekogranično pružanje usluga i razinu kiberotpornosti zbog primjene različitih mjera. Naposljetku, te razlike mogle bi dovesti do veće ranjivosti nekih država članica na kiberprijetnje, s mogućim učincima prelijevanja širom Unije. Cilj je ove Direktive ukloniti 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 sredstava i mjera izvršavanja ključnih za djelotvorno izvršavanje tih obveza. Stoga bi Direktivu (EU) 2016/1148 trebalo staviti izvan snage i zamijeniti ovom Direktivom.

(6) Stavljanjem izvan snage Direktive (EU) 2016/1148 područje primjene po sektorima trebalo bi proširiti na veći dio gospodarstva kako bi se osigurala sveobuhvatna pokrivenost sektora i usluga od velike važnosti za ključne društvene i gospodarske djelatnosti na unutarnjem tržištu. Ovom se Direktivom posebno nastoji prevladati nedostatke u razlikovanju operatora ključnih usluga od pružatelja digitalnih usluga, koje se pokazalo zastarjelim jer ne odražava važnost sektora ili usluga za društvene i gospodarske djelatnosti na unutarnjem tržištu.

(7) Na temelju Direktive (EU) 2016/1148, države članice bile su odgovorne za utvrđivanje subjekata koji ispunjavaju kriterije na temelju kojih ih se smatralo operatorima ključnih usluga. Kako bi se uklonile velike razlike među državama članicama u tom pogledu i osigurala pravna sigurnost za mjere upravljanja kibersigurnosnim 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 obuhvaćeni svi subjekti koji se smatraju srednjim poduzećima na temelju članka 2. Priloga Preporuci Komisije 2003/361/EZ[1] ili koji prelaze gornje granice za srednja poduzeća iz stavka 1. tog članka i koji posluju u sektorima i pružaju vrste usluga ili obavljaju djelatnosti obuhvaćene ovom Direktivom. Države članice također bi trebale osigurati da su područjem primjene ove Direktive obuhvaćena pojedina mala poduzeća i mikropoduzeća, kako su definirana u članku 2. stavku 2. i stavku 3. tog priloga i koja ispunjavaju posebne kriterije koji pokazuju da imaju ključnu ulogu za društvo, gospodarstvo ili za određene sektore ili vrste usluga.

[1] 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.).

(8) Isključenje subjekata javne uprave iz područja primjene ove Direktive trebalo bi se primjenjivati na subjekte čije se djelatnosti pretežno obavljaju u područjima nacionalne sigurnosti, javne sigurnosti, obrane ili izvršavanja zakonodavstva, uključujući sprečavanje, istragu, otkrivanje i progon kaznenih djela. Međutim, subjekti javne uprave čije su djelatnosti samo marginalno povezane s tim područjima ne bi trebali biti isključeni iz područja primjene ove Direktive. Za potrebe ove Direktive ne smatra se da subjekti s regulatornim ovlastima obavljaju djelatnosti u području izvršavanja zakonodavstva i stoga nisu isključeni iz područja primjene ove Direktive na toj osnovi. Subjekti javne uprave koji su zajednički osnovani s trećom zemljom u skladu s međunarodnim sporazumom isključeni su iz područja primjene ove Direktive. Ova se Direktiva ne primjenjuje na diplomatske i konzularne misije država članica u trećim zemljama ili na njihove mrežne i informacijske sustave ako se takvi sustavi nalaze u prostorijama misije ili ih koriste korisnici u trećoj zemlji.

(9) Države članice trebale bi moći poduzeti mjere potrebne za osiguranje zaštite osnovnih interesa nacionalne sigurnosti, za zaštitu javne politike i javne sigurnosti te za omogućivanje sprečavanja, istrage, otkrivanja i progona kaznenih djela**.** U tu svrhu države članice trebale bi moći izuzeti određene subjekte koji obavljaju djelatnosti u području nacionalne sigurnosti, javne sigurnosti, obrane ili izvršavanja zakonodavstva, uključujući sprečavanje, istragu, otkrivanje i progon kaznenih djela, od ispunjavanja određenih obveza utvrđenih u ovoj Direktivi u pogledu tih aktivnosti. Ako subjekt pruža usluge isključivo subjektu javne uprave koji je isključen iz područja primjene ove Direktive, države članice trebale bi moći izuzeti taj subjekt od ispunjavanja određenih obveza utvrđenih u ovoj Direktivi u pogledu tih usluga. Osim toga, nijedna država članica ne bi trebala biti obvezna davati informacije ako smatra da bi njihovo otkrivanje bilo suprotno osnovnim interesima njezine nacionalne sigurnosti, javne sigurnosti ili obrane. U tom kontekstu trebalo bi uzeti u obzir Unijina ili nacionalna pravila za zaštitu klasificiranih podataka, sporazume o povjerljivosti podataka i neformalne sporazume o povjerljivosti podataka kao što je Protokol o semaforu. Protokol o semaforu treba shvatiti kao sredstvo za pružanje informacija o svim ograničenjima u pogledu daljnjeg širenja informacija. Upotrebljava se u gotovo svim timovima za odgovor na računalne sigurnosne incidente (CSIRT-ovi) te u nekim centrima za analizu i razmjenu informacija.

(10) Iako se ova Direktiva primjenjuje na subjekte koji obavljaju djelatnosti proizvodnje električne energije iz nuklearnih elektrana, neke od tih djelatnosti mogu biti povezane s nacionalnom sigurnošću. Ako je to slučaj, država članica trebala bi moći izvršavati svoju odgovornost za zaštitu nacionalne sigurnosti u pogledu tih djelatnosti, uključujući djelatnosti unutar nuklearnog vrijednosnog lanca, u skladu s Ugovorima.

(11) Neki subjekti obavljaju djelatnosti u područjima nacionalne sigurnosti, javne sigurnosti, obrane ili izvršavanja zakonodavstva, uključujući sprečavanje, istragu, otkrivanje i progon kaznenih djela istodobno pružajući usluge povjerenja. Pružatelji usluga povjerenja koji su obuhvaćeni područjem primjene Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća[1] trebali bi biti obuhvaćeni područjem primjene ove Direktive kako bi se osigurala razina sigurnosnih zahtjeva i nadzora jednaka onoj koja je prethodno utvrđena u toj uredbi u vezi pružatelja usluga povjerenja. U skladu s isključenjem određenih posebnih usluga iz Uredbe (EU) br. 910/2014, ova Direktiva ne bi se trebala primjenjivati na pružanje usluga povjerenja koje se isključivo koriste unutar zatvorenih sustava koji proizlaze iz nacionalnog prava ili iz sporazumâ među utvrđenom skupinom sudionika.

[1] 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.).

(12) Pružatelji poštanskih usluga, kako su definirani u Direktivi 97/67/EZ Europskog parlamenta i Vijeća[1], uključujući pružatelje kurirskih usluga, trebali bi podlijegati ovoj Direktivi ako poduzimaju barem jedan od koraka u poštanskom lancu dostave, posebno prikupljanje, razvrstavanjem prijevoz ili dostavu poštanskih pošiljaka, uključujući i usluge preuzimanja, uzimajući u obzir stupanj njihove ovisnosti o mrežnim i informacijskim sustavima. Usluge prijevoza koje se ne poduzimaju u kombinaciji s jednim od tih koraka trebale bi biti isključene iz opsega poštanskih usluga.

(13) S obzirom na jačanje i povećanu sofisticiranost kiberprijetnji, države članice trebale bi nastojati osigurati da subjekti isključeni iz područja primjene ove Direktive ostvare visoku razinu kibersigurnosti i poduprijeti provedbu jednakovrijednih mjera upravljanja kibersigurnosnim rizicima koje odražavaju osjetljivu prirodu tih subjekata.

[1] 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.).

(14) Pravo Unije o zaštiti podataka i pravo Unije o zaštiti privatnosti primjenjuje se na svaku obradu osobnih podataka na temelju ove Direktive. Posebno, ovom Direktivom ne dovodi se u pitanje Uredba (EU) 2016/679 Europskog parlamenta i Vijeća[1] i Direktiva 2002/58/EZ Europskog parlamenta i Vijeća[2]. Ova Direktiva stoga ne bi trebala utjecati, među ostalim, na zadaće i ovlasti tijela nadležnih za praćenje usklađenosti s primjenjivim pravom Unije o zaštiti podataka i pravom Unije o zaštiti privatnosti.

(15) Subjekti obuhvaćeni područjem primjene ove Direktive za potrebe usklađenosti s mjerama upravljanja kibersigurnosnim rizicima i obvezama izvješćivanja trebali bi biti razvrstani u dvije kategorije, ključne subjekte i važne subjekte, ovisno o mjeri u kojoj su kritični s obzirom na njihov sektor ili vrstu usluga koje pružaju, kao i njihovu veličinu. U tom bi pogledu nadležna tijela, ako je to primjenjivo, u obzir trebala uzeti sve relevantne sektorske procjene rizika ili smjernice. Sustavi nadzora i izvršavanja za te dvije kategorije subjekata trebali bi se razlikovati 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.

---

[1] 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.).

[2] 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.).

(16) Kako bi se izbjeglo da se subjekti koji imaju partnerska poduzeća ili povezana poduzeća smatraju ključnim ili važnim subjektima ako bi to bilo nerazmjerno, države članice pri primjeni članka 6. stavka 2. Priloga Preporuci 2003/361/EZ mogu uzeti u obzir stupanj neovisnosti subjekta u odnosu na njegova partnerska ili povezana poduzeća.
Posebno, države članice mogu uzeti u obzir činjenicu da je subjekt neovisan o svojim partnerskim ili povezanim poduzećima u pogledu mrežnih i informacijskih sustava kojima se taj subjekt koristi u pružanju svojih usluga i u pogledu usluga koje subjekt pruža.
Na temelju toga, države članice, prema potrebi, mogu zauzeti stav da se takav subjekt ne smatra srednjim poduzećem na temelju članka 2. Priloga Preporuci 2003/361/EZ ili da ne prelazi gornje granice za srednje poduzeće iz stavka 1. tog članka, ako se, nakon uzimanja u obzir stupnja neovisnosti tog subjekta, ne bi smatralo da je taj subjekt srednje poduzeće ili da premašuje te gornje granice da su u obzir uzeti samo njegovi vlastiti podaci. To ne utječe na obveze utvrđene u ovoj Direktivi za partnerska i povezana poduzeća koja su obuhvaćena područjem primjene ove Direktive.

(17) Države članice trebale bi moći odlučiti 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.

(18) Kako bi se osigurao jasan pregled subjekata obuhvaćenih područjem primjene ove Direktive, države članice trebale bi utvrditi popis ključnih i važnih subjekata te subjekata koji pružaju usluge registracije naziva domena. U tu bi svrhu države članice od subjekata trebale zahtijevati da nadležnim tijelima dostave barem sljedeće informacije, odnosno ime, adresu i ažurirane podatke za kontakt, uključujući e-adrese, IP raspone i telefonske brojeve subjekta, i, ako je to primjenjivo, relevantni sektor i podsektor iz prilogâ te, ako je to primjenjivo, popis država članica u kojima pružaju usluge obuhvaćene područjem primjene ove Direktive. U tu bi svrhu Komisija, uz pomoć Agencije Europske unije za kibersigurnost (ENISA), trebala bez nepotrebne odgode pružiti smjernice i predloške u vezi s obvezom dostavljanja informacija. Kako bi se olakšalo utvrđivanje i ažuriranje popisa ključnih i važnih subjekata te subjekata koji pružaju usluge registracije naziva domena, države članice trebale bi moći uspostaviti nacionalne mehanizme za registraciju subjekata. Ako na nacionalnoj razini postoje registri, države članice mogu odlučiti o odgovarajućim mehanizmima koji omogućuju utvrđivanje subjekata obuhvaćenih područjem primjene ove Direktive.

(19) Države članice trebale bi biti odgovorne za to da se Komisiji dostavi barem broj ključnih i važnih subjekata za svaki sektor i podsektor iz prilogâ, zajedno s relevantnim informacijama o broju utvrđenih subjekata te o odredbi iz ove Direktive na temelju koje su utvrđeni i vrsti usluge koju pružaju. Države članice potiču se da s Komisijom razmjenjuju informacije o ključnim i važnim subjektima te, u slučaju kibersigurnosnog incidenta velikih razmjera, relevantne informacije kao što je naziv predmetnog subjekta.

(20) Komisija bi, u suradnji sa skupinom za suradnju i nakon savjetovanja s relevantnim dionicima, trebala pružiti smjernice o provedbi kriterija koji se primjenjuju na mikropoduzeća i mala poduzeća u svrhu ocjenjivanja jesu li obuhvaćena područjem primjene ove Direktive. Komisija bi također trebala osigurati da se svim mikropoduzećima i malim poduzećima koja su obuhvaćena područjem primjene ove Direktive daju odgovarajuće smjernice. Komisija bi, uz pomoć država članica, mikropoduzećima i malim poduzećima trebala staviti na raspolaganje informacije u tom pogledu.

(21) Komisija bi, kako bi pomogla državama članicama u provedbi odredaba ove Direktive, mogla pružiti smjernice o području primjene i ocjenjivanju proporcionalnosti mjera koje treba poduzeti u skladu s ovom Direktivom, posebno u pogledu subjekata sa složenim poslovnim modelima ili poslovnim okruženjima, pri čemu subjekt može istodobno ispunjavati kriterije dodijeljene i ključnim i važnim subjektima ili istodobno obavljati djelatnosti od kojih su neke obuhvaćene područjem primjene ove Direktive, a neke isključene iz područja primjene ove Direktive.

(22) Ovom Direktivom utvrđuju se osnovna razina mjera upravljanja kibersigurnosnim rizicima i obveze izvješćivanja u svim sektorima koji su obuhvaćeni njezinim područjem primjene. Kako bi se izbjegla rascjepkanost odredaba o kibersigurnosti u pravnim aktima Unije, kada se dodatni sektorski pravni akti Unije koji se odnose na mjere upravljanja kibersigurnosnim rizicima i obveze izvješćivanja smatraju nužnima kako bi se osigurala visoka razina kibersigurnosti širom Unije, Komisija bi trebala procijeniti mogu li se takve dodatne odredbe propisati u provedbenom aktu na temelju ove Direktive. Ako takvi provedbeni akti nisu prikladni za tu svrhu, sektorski pravni akti Unije mogli bi doprinijeti osiguravanju visoke razine kibersigurnosti širom Unije, uzimajući pritom u potpunosti u obzir posebnosti i složenosti predmetnih sektora. U tu svrhu, ovom se Direktivom ne sprečava donošenje dodatnih sektorskih pravnih akata Unije koji se odnose na mjere upravljanja kibersigurnosnim rizicima i obveze izvješćivanja koji propisno uzimaju u obzir potrebu za sveobuhvatnim i dosljednim okvirom za kibersigurnost. Ovom se Direktivom ne dovode u pitanje postojeće provedbene ovlasti dodijeljene Komisiji u brojnim sektorima, uključujući promet i energetiku.

(23) Ako sektorski pravni akti sadržavaju odredbe kojima se od ključnih ili važnih subjekata zahtijeva donošenje mjera upravljanja kibersigurnosnim rizicima ili obavješćivanje o značajnim incidentima i ako su ti zahtjevi barem po učinku jednakovrijedni obvezama utvrđenima u ovoj Direktivi, te bi se odredbe, uključujući odredbe o nadzoru i izvršavanju, trebale primjenjivati na te subjekte. Ako sektorski pravni akt Unije ne obuhvaća sve subjekte u određenom sektoru koji su obuhvaćeni područjem primjene ove Direktive, relevantne odredbe ove Direktive i dalje bi se trebale primjenjivati na subjekte koji nisu obuhvaćeni tim aktom.

(24) Ako se odredbama sektorskog pravnog akta Unije od ključnih ili važnih subjekata zahtijeva ispunjavanje obveza izvješćivanja koje su barem po učinku jednakovrijedne obvezama izvješćivanja utvrđene u ovoj Direktivi, trebalo bi osigurati dosljednost i djelotvornost postupanja s obavijestima o incidentima. U tu bi svrhu odredbama sektorskog pravnog akta Unije u vezi s obavješćivanjem o incidentima CSIRT-ovima, nadležnim tijelima ili jedinstvenim kontaktnim točkama za kibersigurnost (jedinstvene kontaktne točke) na temelju ove Direktive trebalo omogućiti neposredan pristup obavijestima o incidentima podnesenima u skladu sa sektorskim pravnim aktom Unije. Konkretno, takav se neposredan pristup može osigurati ako se obavijesti o incidentima bez nepotrebne odgode prosljeđuju CSIRT-u, nadležnom tijelu ili jedinstvenoj kontaktnoj točki u skladu s ovom Direktivom. Prema potrebi, države članice trebale bi uspostaviti mehanizam automatskog i izravnog izvješćivanja kojim se osigurava sustavna i neposredna razmjena informacija s CSIRT-ovima, nadležnim tijelima ili jedinstvenim kontaktnim točkama u pogledu postupanja s takvim obavijestima o incidentima. U svrhu pojednostavnjenja izvješćivanja i provedbe mehanizma automatskog i izravnog izvješćivanja, države članice mogle bi se, u skladu sa sektorskim pravnim aktom Unije, koristiti jedinstvenom ulaznom točkom.

(25) Sektorskim pravnim aktima Unije kojima su predviđene mjere upravljanja kibersigurnosnim rizicima ili obveze izvješćivanja koje su barem po učinku jednakovrijedne onima utvrđenima u ovoj Direktivi moglo bi se predvidjeti da nadležna tijela na temelju takvih akata izvršavaju svoje nadzorne ovlasti i ovlasti izvršavanja u vezi s takvim mjerama ili obvezama uz pomoć nadležnih tijela na temelju ove Direktive. Predmetna 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 inspekcije na lokaciji u skladu s nacionalnim pravom te mehanizam za razmjenu relevantnih informacija o nadzoru i izvršavanju među nadležnim tijelima, uključujući pristup informacijama povezanima s kibersigurnošću koje zahtijevaju nadležna tijela na temelju ove Direktive.

(26) Ako se sektorskim pravnim aktima Unije zahtijeva ili se subjektima pružaju poticaji za obavješćivanje o ozbiljnim kiberprijetnjama, države članice trebale bi poticati i razmjenu ozbiljnih kiberprijetnji s CSIRT-ovima, nadležnim tijelima ili jedinstvenim kontaktnim točkama u skladu s ovom Direktivom kako bi se osigurala veća razina osviještenosti tih tijela o kiberprijetnjama i kako bi im se omogućilo da učinkovito i pravodobno odgovore u slučaju da se ozbiljne kiberprijetnje ostvare.

(27) U budućim sektorskim pravnim aktima Unije trebalo bi uzeti u obzir definicije te okvir za nadzor i izvršavanje utvrđen u ovoj Direktivi.

(28) Uredbu (EU) …/… Europskog parlamenta i Vijeća[1+] trebalo bi smatrati sektorskim pravnim aktom Unije u odnosu na ovu Direktivu u pogledu financijskih subjekata. Umjesto odredaba predviđenih ovom Direktivom trebale bi se primjenjivati odredbe Uredbe (EU) …/…[++] koje se odnose na upravljanje rizicima informacijskih i komunikacijskih tehnologija (IKT), upravljanje IKT incidentima, a posebno izvješćivanje o značajnim IKT 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 upravljanju kibersigurnosnim rizicima i obvezama izvješćivanja te nadzoru i izvršavanju na financijske subjekte obuhvaćene Uredbom (EU) …/…[++]. Istodobno je važno održavati blizak odnos i razmjenu informacija s financijskim sektorom na temelju ove Direktive. U tu svrhu Uredbom (EU) …/…[++] europskim nadzornim tijelima i nadležnim tijelima na temelju te uredbe omogućuje se sudjelovanje u aktivnostima skupine za suradnju te razmjena informacija i suradnja s jedinstvenim kontaktnim točkama, kao i s CSIRT-ovima i nadležnim tijelima na temelju ove Direktive. Nadležna tijela na temelju Uredbe (EU) …/…[++] trebala bi i podatke o značajnim IKT incidentima i, ako je to relevantno, ozbiljnim kiberprijetnjama slati CSIRT-ovima, nadležnim tijelima ili jedinstvenim kontaktnim točkama u skladu s ovom Direktivom. To se može postići pružanjem neposrednog pristupa obavijestima o incidentima i prosljeđivanjem tih obavijesti bilo izravno ili putem jedinstvene ulazne točke. Osim toga, države članice trebale bi nastaviti uključivati financijski sektor u svoje strategije za kibersigurnost, a CSIRT-ovi ga mogu obuhvatiti svojim aktivnostima.

---

1 Uredba (EU) .../... Europskog parlamenta i Vijeća od... digitalnoj operativnoj otpornosti za financijski sektor i o izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (SL L ..., ... str. ...).

[+] SL: molimo u tekst umetnuti broj uredbe iz dokumenta PE-CONS 41/22 (2020/0266(COD)), a u bilješku umetnuti broj, datum i upućivanje na SL za tu uredbu.

[++] SL: molimo u tekst umetnuti broj Uredbe iz dokumenta PE-CONS 41/22 (2020/0266(COD)).

(29) Kako bi se izbjegle praznine u području kibersigurnosnih obveza uvedenih subjektima u zrakoplovnom sektoru ili udvostručavanje tih obveza, nacionalna tijela na temelju uredbi (EZ) br. 300/2008[1] i (EU) 2018/1139[2] Europskog parlamenta i Vijeća te nadležna tijela na temelju ove Direktive trebala bi surađivati u vezi s provedbom mjera upravljanja kibersigurnosnim rizicima i nadzorom nad usklađenošću s tim mjerama na nacionalnoj razini. Nadležna tijela na temelju ove Direktive mogla bi smatrati da usklađenost subjekta sa sigurnosnim zahtjevima utvrđenima u uredbama (EZ) br. 300/2008 i (EU) 2018/1139 te relevantnim delegiranim i provedbenim aktima donesenima u skladu s tim uredbama predstavlja usklađenost s odgovarajućim zahtjevima utvrđenima u ovoj Direktivi.

---

[1] 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.).

[2] 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.).

(30) S obzirom na međupovezanost kibersigurnosti i fizičke sigurnosti subjekata, trebalo bi osigurati koherentan pristup između Direktive (EU) …/… Europskog parlamenta i Vijeća[1+] i ove Direktive. Kako bi se to postiglo, subjekti utvrđeni kao kritični na temelju Direktive (EU) …/…[++] trebali bi se smatrati ključnim subjektima na temelju ove Direktive. Osim toga, svaka države članica trebala bi osigurati da se njezinom nacionalnom strategijom za kibersigurnost osigurava okvir politike za bolju koordinaciju u toj državi članici između njezinih nadležnih tijela na temelju ove Direktive i nadležnih tijela na temelju Direktive …/…[++] u kontekstu razmjene informacija o rizicima, kiberprijetnjama i incidentima te rizicima, prijetnjama i incidentima izvan kiberprostora, kao i izvršavanje nadzornih zadaća. Nadležna tijela na temelju ove Direktive i nadležna tijela na temelju Direktive (EU) …/…[++] direktiva trebala bi bez nepotrebne odgode surađivati i razmjenjivati informacije, posebno u pogledu utvrđivanja kritičnih subjekata, rizika, kiberprijetnji i incidenata, kao i u vezi s rizicima, prijetnjama i incidentima izvan kiberprostora koji utječu na kritične subjekte, uključujući kibersigurnosne i fizičke mjere koje ti subjekti poduzimaju, kao i rezultate nadzornih aktivnosti provedenih u pogledu takvih subjekata.

---

1 Direktiva (EU) .../... Europskog parlamenta i Vijeća od... o otpornosti kritičnih subjekata i o stavljanju izvan snage Direktive Vijeća 2008/114/EZ (SL L ..., ..., str. ...).

\+ SL: molimo umetnuti broj Direktive iz dokumenta PE-CONS 51/22 (2020/0365(COD)), a u bilješku umetnuti broj, datum, naslov i upućivanje na SL za tu direktivu.

++ SL: molimo u tekst umetnuti broj Direktive iz dokumenta PE-CONS 51/22 (2020/0365(COD)).

Nadalje, kako bi se pojednostavnile nadzorne aktivnosti među nadležnim tijelima na temelju ove Direktive i nadležnih tijela na temelju Direktive (EU) …/…[+] te kako bi se smanjilo administrativno opterećenje za predmetne subjekte, ta nadležna tijela trebala bi nastojati uskladiti predloške za obavijesti o incidentima i nadzorne postupke. Prema potrebi, nadležna tijela na temelju Direktive (EU) …/…[+] trebala bi moći zatražiti od nadležnih tijela na temelju ove Direktive da izvršavaju svoje nadzorne ovlasti i ovlasti izvršavanja u vezi s subjektom koji je utvrđen kao kritičan subjekt na temelju Direktive (EU) …/…[+]. Nadležna tijela na temelju ove Direktive i nadležna tijela na temelju Direktive (EU) …/…[+], po mogućnosti u stvarnom vremenu, trebala bi surađivati i razmjenjivati informacije u tu svrhu.

(31) Subjekti koji pripadaju sektoru digitalne infrastrukture u suštini se temelje na mrežnim i informacijskim sustavima te bi se stoga obvezama koje su ovom Direktivom uvedene za te subjekte trebalo na sveobuhvatan način obuhvatiti fizičku sigurnost takvih sustava kao dio njihovih mjera upravljanja kibersigurnosnim rizicima i obveza izvješćivanja. S obzirom na to da su ta pitanja obuhvaćena ovom Direktivom, obveze utvrđene u poglavljima III., IV. i VI. Direktive (EU) …/…[+] ne primjenjuju se na takve subjekte.

[+] SL: molimo u tekst umetnuti broj Direktive iz dokumenta PE-CONS 51/22 (2020/0365(COD)).

(32) Podrška pouzdanom, otpornom i sigurnom sustavu naziva domena (DNS) i njegovo održavanje 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 registre naziva vršnih domena i pružatelje usluga DNS-a koje treba shvatiti kao subjekte koji pružaju javno dostupne rekurzivne usluge razlučivanja naziva domena za krajnje korisnike interneta ili mjerodavne usluge razlučivanja naziva domena za treće strane. Ova se Direktiva ne bi trebala primjenjivati na korijenske poslužitelje naziva.

(33) Usluge računalstva u oblaku trebale bi obuhvaćati digitalne usluge koje omogućuju administraciju na zahtjev i široki daljinski pristup nadogradivom i elastičnom skupu djeljivih računalnih resursa, među ostalim kada su takvi resursi raspoređeni na nekoliko lokacija. 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.
Usluga računalstva u oblaku i modeli 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 korištenja 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 pružaju 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.

(34) S obzirom na razvoj inovativnih tehnologija i novih poslovnih modela, očekuje se da će se na tržištu pojaviti novi modeli usluga računalstva u oblaku i uvođenja 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).

(35) 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 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 (IT) 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 bi se trebao primjenjivati na interne korporativne podatkovne centre kojima predmetni subjekt u čijem su vlasništvu upravlja za vlastite potrebe.

(36) Istraživačke aktivnosti imaju ključnu ulogu u razvoju novih proizvoda i procesa. Mnoge od tih aktivnosti provode subjekti koji rezultate svojih istraživanja dijele, šire ili iskorištavaju u komercijalne svrhe. Ti subjekti stoga mogu biti važni akteri u lancima vrijednosti, zbog čega je sigurnost njihovih mrežnih i informacijskih sustava sastavni dio cjelokupne kibersigurnosti unutarnjeg tržišta. Trebalo bi se podrazumijevati da istraživačke organizacije uključuju subjekte koji ključni dio svojih aktivnosti usmjeravaju na provođenje primijenjenog istraživanja ili eksperimentalnog razvoja, u smislu Priručnika Frascati Organizacije za gospodarsku suradnju i razvoj iz 2015.: Smjernice za prikupljanje podataka o istraživanju i eksperimentalnom razvoju i izvješćivanje o njima, s ciljem iskorištavanja njihovih rezultata u komercijalne svrhe, kao što su proizvodnja ili razvoj proizvoda ili procesa, pružanje usluge ili njihovo stavljanje na tržište.

(37) Rastuće međuovisnosti rezultat su sve veće prekogranične i međuovisne mreže pružanja usluga koja upotrebljava ključnu infrastrukturu u cijeloj Uniji u sektorima kao što su energetika, promet, digitalna infrastruktura, voda za piće i otpadne vode, zdravlje, određeni aspekti javne uprave, kao i u svemirski sektor 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 njezina svemirskog 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. Intenzivniji kibernapadi tijekom pandemije bolesti COVID-19 pokazali su ranjivost naših sve više međuovisnih društava suočenih s rizicima male vjerojatnosti.

(38) S obzirom na razlike u nacionalnim upravljačkim strukturama i radi zaštite postojećih sektorskih dogovora ili nadzornih i regulatornih tijela Unije, države članice trebale bi moći imenovati ili uspostaviti jedno ili više nadležnih tijela odgovornih za kibersigurnost i za nadzorne zadaće na temelju ove Direktive.

(39) 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 kontaktnu točku odgovornu za koordinaciju pitanja sigurnosti mrežnih i informacijskih sustava te za prekograničnu suradnju na razini Unije.

(40) Jedinstvene kontaktne točke trebale bi osigurati učinkovitu prekograničnu suradnju s relevantnim tijelima drugih država članica i, prema potrebi, s Komisijom i ENISA-om. Jedinstvene kontaktne točke stoga bi trebale biti zadužene za prosljeđivanje obavijesti o značajnim incidentima s prekograničnim učinkom jedinstvenim kontaktnim točkama drugih pogođenih država članica na zahtjev CSIRT-a ili nadležnog tijela. Na nacionalnoj razini jedinstvene kontaktne točke trebale bi omogućiti neometanu međusektorsku suradnju s drugim nadležnim tijelima. Jedinstvene kontaktne točke mogle bi također bi primati relevantne informacije o incidentima koji se odnose na subjekte financijskog sektora od nadležnih tijela na temelju Uredbe (EU) …/…[+], koje bi, prema potrebi, trebale moći proslijediti CSIRT-ovima ili nacionalnim nadležnim tijelima iz ove Direktive.

[+] SL: molimo u tekst umetnuti broj Uredbe iz dokumenta PE-CONS 41/22 (2020/0266(COD)).

(41) Države članice trebale bi biti dostatno opremljene, u smislu tehničkih i organizacijskih sposobnosti, za sprečavanje i otkrivanje incidenata i rizika, reagiranje na njih te za ublažavanje njihova učinka. Države članice stoga bi trebale uspostaviti ili imenovati jedan ili više CSIRT-ova na temelju ove Direktive i osigurati da imaju odgovarajuće resurse i tehničke sposobnosti. CSIRT-ovi bi trebali poštovati zahtjeve utvrđene u ovoj Direktivi kako bi se zajamčile djelotvorne i uskladive sposobnosti za rješavanje incidenata i rizika te kako bi se osigurala učinkovita suradnja na razini Unije. Države članice trebale bi moći kao CSIRT-ove imenovati postojeće timove za hitne računalne intervencije (CERT-ovi). U cilju jačanja odnosa povjerenja između subjekata i CSIRT-ova, u slučajevima kada je CSIRT dio nadležnog tijela, države članice trebale bi moći razmotriti funkcionalno odvajanje operativnih zadaća koje obavljaju CSIRT-ovi, posebno u vezi s razmjenom informacija i podrškom koja se pruža subjektima, te nadzornih aktivnosti nadležnih tijela.

(42) CSIRT-ovi su zaduženi za postupanje s incidentima. To uključuje obradu velikih količina ponekad osjetljivih podataka. Države članice trebale bi osigurati da CSIRT-ovi raspolažu infrastrukturom za razmjenu i obradu informacija kao i dobro opremljenim osobljem, čime se osigurava povjerljivost i pouzdanost njihovih operacija. CSIRT-ovi bi mogli donijeti i kodekse ponašanja u tom pogledu.

(43) Kad je riječ o osobnim podacima, CSIRT-ovi bi, u skladu s Uredbom (EU) 2016/679, na zahtjev ključnog ili važnog subjekta, trebali moći osigurati proaktivno skeniranje mrežnih i informacijskih sustava koji se upotrebljavaju za pružanje usluga subjekta. Ako je to primjenjivo, države članice trebale bi nastojati osigurati jednaku razinu tehničkih sposobnosti za sve sektorske CSIRT-ove. Države članice trebale bi moći zatražiti podršku ENISA-e u razvijanju svojih CSIRT-ova.

(44) CSIRT-ovi bi trebali imati mogućnost na zahtjev ključnog ili važnog subjekta pratiti imovinu subjekta s internetskim sučeljem, kako u fizičkim prostorima tako i izvan njih, kako bi utvrdili i razumjeli ukupne organizacijske rizike subjekta u pogledu novootkrivenih slučajeva ugrožavanja lanaca opskrbe ili kritičnih ranjivosti te upravljali njima. Subjekt bi trebalo poticati da obavijesti CSIRT o tome ima li povlašteno upravljačko sučelje jer bi to moglo utjecati na brzinu poduzimanja mjera ublažavanja.

(45) S obzirom na važnost međunarodne suradnje za kibersigurnost, CSIRT-ovi bi trebali moći, uz mrežu CSIRT-ova uspostavljenu ovom Direktivom, sudjelovati i u međunarodnim mrežama suradnje. Stoga bi CSIRT-ovi i nadležna tijela za potrebe obavljanja svojih zadaća trebali moći razmjenjivati informacije, uključujući osobne podatke, s nacionalnim timovima za odgovor na računalne sigurnosne incidente ili nadležnim tijelima trećih zemalja pod uvjetom da su ispunjeni uvjeti iz prava Unije o zaštiti podataka za prijenose osobnih podataka trećim zemljama, među ostalim uvjeti iz članka 49. Uredbe (EU) 2016/679.

(46) Ključno je osigurati odgovarajuće resurse za ispunjavanje ciljeva ove Direktive i omogućavanje nadležnim tijelima i CSIRT-ovima izvršavanje u njoj utvrđenih zadaća. Države članice mogu na nacionalnoj razini uvesti mehanizam financiranja za pokrivanje potrebnih rashoda povezanih s obavljanjem zadaća javnih tijela odgovornih za kibersigurnost u državi članici u skladu s ovom Direktivom. Takav mehanizam trebao bi biti u skladu s pravom Unije i trebao bi biti razmjeran i nediskriminirajući te uzeti u obzir različite pristupe pružanju sigurnih usluga.

(47) 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.

(48) U svrhu postizanja i održavanja visoke razine kibersigurnosti, nacionalne strategije za kibersigurnost koje se zahtijevaju ovom Direktivom trebale bi se sastojati od koherentnih okvira kojima se pružaju strateški ciljevi i prioriteti u području kibersigurnosti i upravljanja u cilju njihova postizanja. Te strategije mogu se sastojati od jednog ili više zakonodavnih ili nezakonodavnih instrumenata.

(49) Politikama o kiberhigijeni pružaju se temelji za zaštitu infrastruktura mrežnih i informacijskih sustava, sigurnost hardvera, softvera i internetskih aplikacija te poslovnih podataka ili podataka krajnjih korisnika na koje se subjekti oslanjaju. Politike o kiberhigijeni sastoje se od zajedničkog temeljnog skupa praksi koje uključuju ažuriranja softvera i hardvera, promjene lozinki, upravljanje novim instalacijama, ograničenje računa za pristup na razini administratora i sigurnosno kopiranje podataka, te se njima omogućuje stvaranje proaktivnog okvira za pripravnost i opću sigurnost u slučaju incidenata ili kiberprijetnji. ENISA bi trebala pratiti i analizirati politike država članica u području kiberhigijene.

(50) Svijest o kibersigurnosti i kiberhigijena ključni su za povećanje razine kibersigurnosti u Uniji, posebno s obzirom na sve veći broj povezanih uređaja koji se sve više upotrebljavaju u kibernapadima. Trebalo bi uložiti napore kako bi se povećala opća svijest o rizicima povezanima s takvim proizvodima, dok bi ocjenjivanja na razini Unije mogla pomoći u osiguravanju zajedničkog razumijevanja takvih rizika na unutarnjem tržištu.

(51) Države članice trebale bi poticati upotrebu svih inovativnih tehnologija čija bi upotreba mogla poboljšati otkrivanje i sprečavanje kibernapada, uključujući umjetnu inteligenciju, čime bi se omogućilo učinkovitije preusmjeravanje resursa na kibernapade. Stoga bi države članice u svojim nacionalnim strategijama za kibersigurnost trebale poticati aktivnosti u području istraživanja i razvoja kako bi olakšale upotrebu takvih tehnologija, posebno onih koje se odnose na automatizirane ili poluautomatizirane alate u području kibersigurnosti, i, prema potrebi, razmjenu podataka potrebnih za osposobljavanje korisnika takve tehnologije i njezino poboljšanje. Upotreba svih inovativnih tehnologija, uključujući umjetnu inteligenciju, trebala bi biti u skladu s pravom Unije o zaštiti podataka, uključujući načela zaštite podataka u pogledu točnosti podataka, smanjenja količine podataka, pravednosti i transparentnosti te sigurnosti podataka, kao što je najsuvremenije kriptiranje. Trebalo bi se u potpunosti koristiti zahtjevima za tehničku i integriranu zaštitu podataka utvrđenima u Uredbi (EU) 2016/679.

(52) Alatima i aplikacijama za kibersigurnost otvorenoga koda može se doprinijeti višem stupnju otvorenosti i stvarati pozitivan učinak na učinkovitost industrijskih inovacija. Otvoreni standardi olakšavaju interoperabilnost između sigurnosnih alata, pogodujući sigurnosti industrijskih dionika. Alati i aplikacije za kibersigurnost otvorenog koda mogu utjecati na širu zajednicu programera, omogućujući diversifikaciju dobavljača. Otvoreni kod može dovesti do transparentnijeg procesa provjere alata koji se odnose na kibersigurnost i procesa otkrivanja ranjivosti koji pokreće zajednica. Države članice stoga bi trebale moći promicati usvajanje softvera otvorenog koda i otvorenih standarda provođenjem politika koje se odnose na korištenje otvorenih podataka i otvorenog koda kao dijela sigurnosti pomoću transparentnosti. Politike koje promiču uvođenje i održivu upotrebu alata za kibersigurnost otvorenog koda od posebne su važnosti za mala i srednja poduzeća koja se suočavaju sa znatnim troškovima provedbe, koje bi mogli minimalizirati smanjenjem potrebe za posebnim aplikacijama ili alatima.

(53) Komunalne usluge sve su više povezane s digitalnim mrežama u gradovima u svrhu poboljšanja mreža gradskog prijevoza, nadogradnje infrastrukture za opskrbu vodom i zbrinjavanje otpada te povećanja učinkovitosti rasvjete i grijanja zgrada. Te digitalizirane komunalne usluge podložne su kibernapadima te, u slučaju da su ti napadi uspješni, građanima prijeti velika šteta zbog njihove međusobne povezanosti. Države članice trebale bi u okviru svojih nacionalnih strategija za kibersigurnost razviti politiku koja se bavi razvojem takvih povezanih ili pametnih gradova i njihovim mogućim učincima na društvo.

(54) Posljednjih se godina Unija suočila s eksponencijalnim porastom napada ucjenjivačkim softverom, u kojima zlonamjerni softver kriptira podatke i sustave te zahtijeva plaćanje otkupnine kako bi ih odblokirao. Sve veća učestalost i ozbiljnost napada ucjenjivačkim softverom može biti posljedica nekoliko čimbenika, kao što su različiti obrasci napada, kriminalni poslovni modeli povezani s „ucjenjivačkim softverom kao uslugom” i kriptovalutama, zahtjevi za otkupninu te porast napada u lancu opskrbe. Države članice trebale bi u okviru svojih nacionalnih strategija za kibersigurnost donijeti politike za rješavanje porasta napada ucjenjivačkim softverom.

(55) Javno-privatna partnerstva u području kibersigurnosti mogu pružiti odgovarajući okvir za razmjenu znanja i najbolje prakse te uspostavljanje zajedničke razine razumijevanja među dionicima. Države članice trebale bi promicati politike kojima se potiče uspostava javno-privatnih partnerstava za kibersigurnost. Kad je riječ o javno-privatnim partnerstvima, tim bi se politikama, među ostalim, trebali razjasniti područje primjene i uključeni dionici, model upravljanja, dostupne mogućnosti financiranja i interakcija među uključenim dionicima. Javno-privatna partnerstva mogu se koristiti stručnim znanjem subjekata iz privatnog sektora kako bi pomogla nadležnim tijelima u razvoju najsuvremenijih usluga i procesa koji uključuju razmjenu informacija, rana upozorenja, vježbe za slučajeve kiberprijetnji i kiberincidenata, upravljanje rizicima i planiranje otpornosti.

(56) U svojim nacionalnim strategijama za kibersigurnost, države članice trebale bi riješiti pitanje posebnih potreba malih i srednjih poduzeća u području kibersigurnosti. Mala i srednja poduzeća predstavljaju, širom Unije, velik postotak industrijskog i poslovnog tržišta i često nailaze na poteškoće u prilagodbi novim poslovnim praksama u povezanijem svijetu i digitalnom okruženju s obzirom na to da zaposlenici rade od kuće, a poslovanje se sve više vodi na internetu. Neka se mala i srednja poduzeća suočavaju s posebnim izazovima u području kibersigurnosti, kao što su slaba osviještenost o kibersigurnosti, nedostatak informatičke sigurnosti na daljinu, visok trošak kibersigurnosnih rješenja i povećana razina prijetnje, kao što su ucjenjivački softveri, te bi trebali primiti smjernice i potporu. Mala i srednja poduzeća sve više postaju meta napada u lancu opskrbe zbog svojih manje strogih mjera upravljanja kibersigurnosnim rizicima i upravljanja napadima te činjenice da imaju ograničene resurse za sigurnost. Takvi napadi u lancu opskrbe ne utječu samo na mala i srednja poduzeća i njihovo poslovanje, već mogu imati i kaskadni učinak na veće napade na subjekte kojima isporučuju robu. Države članice trebale bi kroz svoje nacionalne strategije za kibersigurnost pomoći malim i srednjim poduzećima u rješavanju izazova s kojima se suočavaju u svojim lancima opskrbe. Države članice trebale bi na nacionalnoj ili regionalnoj razini imati kontaktnu točku za mala i srednja poduzeća koja pruža smjernice i pomoć malim i srednjim poduzećima ili ih usmjerava na odgovarajuća tijela koja pružaju smjernice i pomoć u pogledu pitanja povezanih s kibersigurnošću. Države članice također se potiču da ponude usluge kao što su omogućavanje konfiguracije internetskih stranica i bilježenja podataka za mikropoduzeća i mala poduzeća kojima nedostaju te mogućnosti.

(57) U okviru svojih nacionalnih strategija za kibersigurnost države članice trebale bi donijeti politike o promicanju aktivne kiberzaštite kao dijela šire obrambene strategije. Umjesto reaktivnog odgovora, kiberzaštita podrazumijeva aktivno sprečavanje, otkrivanje, praćenje, analizu i ublažavanje povreda sigurnosti mreže, u kombinaciji s upotrebom kapaciteta koji se primjenjuju unutar i izvan mreže koja je žrtva kibernapada. To bi, među ostalim, moglo uključivati mogućnost da države članice određenim subjektima ponude besplatne usluge ili alate, uključujući samoposlužne provjere, alate za otkrivanje i usluge uklanjanja. Sposobnost brze i automatske razmjene i razumijevanja informacija o prijetnji i analize prijetnji, upozorenja o kiberaktivnostima i odgovora ključna je za omogućivanje udruženih napora za uspješno sprečavanje, otkrivanje, rješavanje i blokiranje napada na mrežne i informacijske sustave. Aktivna kiberzaštita temelji se na strategiji obrane u kojoj su isključene ofenzivne mjere.

(58) Budući da iskorištavanje ranjivosti u mrežnim i informacijskim sustavima može uzrokovati znatne poremećaje i štetu, brzo prepoznavanje i otklanjanje takvih ranjivosti važan je čimbenik u smanjenju rizika. Subjekti koji razvijaju mrežne i informacijske sustave ili upravljaju njima trebali bi stoga uspostaviti odgovarajuće postupke za postupanje s ranjivostima kada ih se otkrije. Budući da ranjivosti često prepoznaju i otkrivaju treće strane, proizvođač ili pružatelj IKT proizvoda ili IKT 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 otkrivanju ranjivosti. Jačanje koordinacije između fizičkih i pravnih osoba koji podliježu obvezi izvješćivanja i proizvođača ili pružatelja IKT proizvoda ili IKT usluga posebno je važno u svrhu olakšavanja dobrovoljnog okvira otkrivanja ranjivosti. Koordinirano otkrivanje ranjivosti odvija se strukturiranim postupkom u okviru kojeg se ranjivosti prijavljuju proizvođaču ili pružatelju potencijalno ranjivih IKT proizvoda ili IKT usluga na način kojim im se 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 fizičke ili pravne osobe koja podliježe obvezi izvješćivanja i proizvođača ili pružatelja potencijalno ranjivih IKT proizvoda ili IKT usluga u pogledu vremena otklanjanja i objave ranjivosti.

(59) Komisija, ENISA i države članice trebale bi nastaviti poticati usklađivanje s međunarodnim normama i postojećim najboljim praksama u industriji u području upravljanja kibersigurnosnim rizicima, na primjer u područjima procjene sigurnosti lanca opskrbe, razmjene informacija i otkrivanja ranjivosti.

(60) Države članice trebale bi, u suradnji s ENISA-om, poduzeti mjere za olakšavanje koordiniranog otkrivanja ranjivosti uspostavom relevantne nacionalne politike. U okviru svojih nacionalnih politika i u skladu s nacionalnim pravom države članice trebale bi, u mjeri u kojoj je to moguće, nastojati odgovoriti na izazove s kojima se suočavaju oni koji istražuju ranjivosti, uključujući njihovu moguću izloženost kaznenoj odgovornosti. S obzirom na to da bi fizičke i pravne osobe koje istražuju ranjivosti u nekim državama članicama mogle biti izložene kaznenoj i građanskopravnoj odgovornosti, države članice potiču se da donesu smjernice u pogledu neprovođenja kaznenog progona istraživača u području informacijske sigurnosti i izuzeća od građanskopravne odgovornosti za njihove aktivnosti.

(61) Države članice trebale bi jednog od svojih CSIRT-ova imenovati koordinatorom koji će prema potrebi djelovati kao pouzdani posrednik između fizičkih i pravnih osoba koje podliježu obvezi izvješćivanja i proizvođača ili pružatelja IKT proizvoda ili IKT usluga na koje će vjerojatno utjecati ranjivost. Zadaće CSIRT-a koji je imenovan koordinatorom trebale bi uključivati utvrđivanje predmetnih subjekata i kontaktiranje s njima, pomaganje fizičkim ili pravnim osobama koje prijavljuju ranjivost, pregovaranje o vremenskom okviru za otkrivanje i upravljanje ranjivostima koje utječu na više subjekata (koordinirano otkrivanje ranjivosti koje uključuje više strana). U slučajevima u kojima bi prijavljena ranjivost mogla imati znatan učinak na subjekte u više država članica, CSIRT-ovi koji su imenovani koordinatorima trebali bi, prema potrebi, surađivati u okviru mreže CSIRT-ova.

(62) Pristup točnim i pravodobnim informacijama o ranjivostima koje utječu na IKT proizvode i IKT usluge doprinosi boljem upravljanju kibersigurnosnim rizicima. Izvori javno dostupnih informacija o ranjivostima važan su alat za subjekte i korisnike njihovih usluga, ali i za nadležna tijela i CSIRT-ove. Zbog toga bi ENISA trebala uspostaviti europsku bazu podataka o ranjivosti u kojoj subjekti, neovisno o tome jesu li obuhvaćeni područjem primjene ove Direktive, i njihovi dobavljači mrežnih i informacijskih sustava, kao i nadležna tijela i CSIRT-ovi, mogu na dobrovoljnoj osnovi otkriti i registrirati javno poznate ranjivosti kako bi se korisnicima omogućilo da poduzmu odgovarajuće mjere ublažavanja. Cilj je te baze podataka riješiti jedinstvene izazove koje rizici predstavljaju za subjekte u Uniji. Nadalje, ENISA bi trebala uspostaviti odgovarajuću proceduru u vezi s postupkom objavljivanja kako bi subjektima dala vremena da poduzmu mjere za ublažavanje svojih ranjivosti i upotrijebe najsuvremenije mjere upravljanja kibersigurnosnim rizicima, kao i strojno čitljive skupove podataka i odgovarajuća sučelja. Kako bi se potaknula kultura otkrivanja ranjivosti, objavljivanje ne bi smjelo imati štetne učinke na fizičku ili pravnu osobu koja podliježe obvezi izvješćivanja.

(63) Iako slični registri ili baze podataka o ranjivosti postoje, na poslužitelju ih smještaju i vode subjekti koji nemaju poslovni nastan u Uniji. Europska baza podataka o ranjivosti koju bi vodila ENISA omogućila bi veću transparentnost u pogledu postupka objavljivanja prije javnog otkrivanja ranjivosti i otpornost u slučaju poremećaja ili prekida u pružanju sličnih usluga. Kako bi se, u mjeri u kojoj je to moguće, izbjeglo udvostručavanje napora i postigla komplementarnost, ENISA bi trebala istražiti mogućnost sklapanja sporazuma o strukturiranoj suradnji sa sličnim registrima ili bazama podataka koji su u nadležnosti trećih zemalja. ENISA bi posebno trebala istražiti mogućnost bliske suradnje s operatorima sustava čestih ranjivosti i izloženosti (CVE).

(64) Skupina za suradnju trebala bi podupirati i olakšavati stratešku suradnju i razmjenu informacija te jačati povjerenje među državama članicama. Skupina za suradnju trebala bi svake dvije godine uspostaviti program rada. Taj bi program rada trebao sadržavati mjere koje skupina mora poduzeti radi provedbe svojih ciljeva i zadaća. Vremenski okvir za donošenje prvog programa 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 za suradnju.

(65) Prilikom izrade smjernica, skupina za suradnju trebala bi biti dosljedna u mapiranju nacionalnih rješenja i iskustava, procjenjivanju učinka rezultata skupine za suradnju na nacionalne pristupe, raspravljanju o izazovima u provedbi i izradi posebnih preporuka koje će se nastojati ispuniti boljom provedbom postojećih pravila, osobito u pogledu lakšeg usklađivanja prilikom prenošenja ove Direktive u državama članicama. Skupina za suradnju mogla bi mapirati i nacionalna rješenja kako bi promicala kompatibilnost kibersigurnosnih rješenja koja se primjenjuju u svakom pojedinom sektoru širom Unije. To je od osobite važnosti za sektore međunarodne i prekogranične prirode.

(66) Skupina za suradnju trebala bi ostati fleksibilan forum i trebala bi moći odgovoriti na nove i promjenjive političke prioritete i izazove, uzimajući pritom u obzir raspoloživost resursa. Mogla bi organizirati redovite zajedničke sastanke s relevantnim privatnim dionicima širom Unije na kojima bi se raspravljalo o aktivnostima skupine za suradnju i prikupljali podaci i informacije o novim izazovima u pogledu politike. Osim toga, skupina za suradnju trebala bi provoditi redovitu procjenu stanja kiberprijetnji ili kiberincidenata, kao što je ucjenjivački softver. Kako bi se poboljšala suradnja na razini Unije, skupina za suradnju trebala bi razmotriti mogućnost pozivanja relevantnih institucija, tijela, ureda i agencija Unije uključenih u politiku kibersigurnosti, kao što su Europski parlament, Europol, Europski odbor za zaštitu podataka, Agencija Europske unije za sigurnost zračnog prometa osnovana Uredbom (EU) 2018/1139 i Agencija Europske unije za svemirski program, osnovana Uredbom (EU) 2021/696 Europskog parlamenta i Vijeća[1], da sudjeluju u njezinu radu.

(67) Nadležna tijela i CSIRT-ovi trebali bi moći sudjelovati u programima razmjene za službenike iz drugih država članica, unutar posebnog okvira i, ako je to primjenjivo, podložno potrebnoj sigurnosnoj provjeri službenika koji sudjeluju u takvim programima razmjene, u cilju poboljšanja suradnje i jačanja povjerenja među državama članicama. Nadležna tijela trebala bi poduzeti potrebne mjere kako bi službenicima iz drugih država članica omogućila da imaju djelotvornu ulogu u aktivnostima nadležnog tijela domaćina ili CSIRT-a domaćina.

[1] Uredba (EU) 2021/696 Europskog parlamenta i Vijeća od 28. travnja 2021. o uspostavi Svemirskog programa Unije i osnivanju Agencije Europske unije za svemirski program te o stavljanju izvan snage uredaba (EU) br. 912/2010, (EU) br. 1285/2013 i (EU) br. 377/2014 i Odluke br. 541/2014/EU (SL L 170, 12.5.2021., str. 69.).

(68) Države članice trebale bi doprinijeti uspostavi okvira EU-a za odgovor na kiberkrize utvrđenog u Preporuci Komisije (EU) 2017/1584[1] putem postojećih mreža suradnje, posebno Europske mreže organizacija za vezu za kiberkrize (mreža EU-CyCLONe), mreže CSIRT-ova i skupine za suradnju. Mreža EU-CyCLONe i mreža CSIRT-ova trebali bi surađivati na temelju postupovnih aranžmana kojima se utvrđuju detalji te suradnje i izbjegavati udvostručavanje zadaća. U poslovniku mreže EU-CyCLONe trebalo bi dodatno utvrditi načine funkcioniranja mreže, uključujući uloge te mreže, oblike suradnje, interakcije s drugim relevantnim akterima i predloške za razmjenu informacija, kao i sredstva komunikacije. Za upravljanje krizama na razini Unije relevantne stranke trebale bi se oslanjati na aranžmane EU-a za integrirani politički odgovor na krizu na temelju Provedbene odluke Vijeća (EU) 2018/1993[2] (aranžmani za 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, trebalo bi aktivirati mehanizam za odgovor na krize Europske službe za vanjsko djelovanje.

---

[1] 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.).

[2] Provedbena odluka Vijeća (EU) 2018/1993 od 11. prosinca 2018. o aranžmanima EU-a za integrirani politički odgovor na krizu (SL L 320, 17.12.2018., str. 28.).

(69) U skladu s Prilogom Preporuci (EU) 2017/1584, kibersigurnosni incident velikih razmjera trebao bi značiti incident koji uzrokuje razinu poremećaja koja premašuje sposobnost države članice da na njega odgovori ili koji ima znatan učinak na najmanje dvije države članice. Ovisno o svojem uzroku i utjecaju, kibersigurnosni incidenti velikih razmjera mogu se proširiti i pretvoriti u prave krize koje onemogućavaju pravilno funkcioniranje unutarnjeg tržišta ili predstavljaju ozbiljne rizike za javnu sigurnost i zaštitu za subjekte ili građane u nekoliko država članica ili u Uniji u cjelini. S obzirom na širok opseg i, u većini slučajeva, prekograničnu prirodu takvih incidenata, države članice i relevantne institucije, tijela, uredi i agencije Unije trebali bi surađivati na tehničkoj, operativnoj i političkoj razini kako bi pravilno koordinirali odgovor širom Unije.

(70) Kibersigurnosni incidenti velikih razmjera i krize na razini Unije zahtijevaju koordinirano djelovanje kako bi se osigurao brz i učinkovit odgovor zbog visokog stupnja međuovisnosti između sektora i država članica. Dostupnost mreža i informacijskih sustava otpornih na kibernapade te dostupnost, povjerljivost i cjelovitost podataka ključni su za sigurnost Unije i zaštitu njezinih građana, poduzeća i institucija od incidenata i kiberprijetnji, kao i za jačanje povjerenja pojedinaca i organizacija u sposobnost Unije da promiče i štiti globalan, otvoren, slobodan, stabilan i siguran kiberprostor utemeljen na ljudskim pravima, temeljnim slobodama, demokraciji i vladavini prava.

(71) Mreža EU-CyCLONe trebala bi djelovati kao posrednik između tehničke i političke razine tijekom kibersigurnosnih incidenata velikih razmjera i kriza te poboljšati suradnju na operativnoj razini i podupirati donošenje odluka na političkoj razini. U suradnji s Komisijom i s obzirom na njezinu nadležnost u području upravljanja krizama, mreža EU-CyCLONe trebala bi se nadovezati na nalaze mreže CSIRT-ova i koristiti se vlastitim kapacitetima pri izradi analize učinka kibersigurnosnih incidenata velikih razmjera i kriza.

(72) Kibernapadi su prekogranične naravi, a značajan incident može poremetiti i oštetiti ključne informacijske infrastrukture o kojima ovisi neometano funkcioniranje unutarnjeg tržišta. Preporuka (EU) 2017/1584 bavi se ulogom svih relevantnih dionika. Nadalje, Komisija je u okviru Mehanizma Unije za civilnu zaštitu uspostavljenog Odlukom br. 1313/2013/EU Europskog parlamenta i Vijeća[1] odgovorna za opća djelovanja u području pripravnosti, uključujući upravljanje Koordinacijskim centrom za odgovor na hitne situacije i Zajedničkim komunikacijskim i informacijskim sustavom za hitne situacije, održavanje i daljnji razvoj sposobnosti za informiranost o stanju i njegovu analizu te uspostavu i upravljanje sposobnošću za mobilizaciju i slanje timova stručnjaka u slučaju zahtjeva za pomoć države članice ili treće zemlje. Komisija je odgovorna i za dostavljanje analitičkih izvješća za aranžmane za politički odgovor na krizu (IPCR) u skladu s Provedbenom odlukom (EU) 2018/1993, među ostalim u pogledu informiranosti o stanju i pripravnosti u području kibersigurnosti, kao i za informiranost o stanju i odgovor na krizu u područjima poljoprivrede, nepovoljnih vremenskih uvjeta, mapiranja i predviđanja sukoba, sustava ranog upozoravanja na prirodne katastrofe, zdravstvenih hitnih stanja, nadzora zaraznih bolesti, zdravlja bilja, kemijskih incidenata, sigurnosti hrane i hrane za životinje, zdravlja životinja, migracija, carina, nuklearnih i radioloških hitnih stanja te energije.

---

[1] Odluka br. 1313/2013/EU Europskog parlamenta i Vijeća od 17. prosinca 2013. o Mehanizmu Unije za civilnu zaštitu (SL L 347, 20.12.2013., str. 924.).

(73) Unija prema potrebi može sklapati međunarodne sporazume s trećim zemljama ili međunarodnim organizacijama, u skladu s člankom 218. UFEU-a, kojima im se dopušta i organizira sudjelovanje u posebnim aktivnostima skupine za suradnju, mreže CSIRT-ova te mreže EU-CyCLONe. Takvim bi se sporazumima trebali osigurati interesi Unije i odgovarajuća zaštita podataka. Time se države članice ne bi trebalo spriječiti da ostvaruju pravo na suradnju s trećim zemljama u području upravljanja ranjivostima i kibersigurnosnim rizicima, čime se olakšava izvješćivanje i razmjena općih informacija u skladu s pravom Unije.

(74) Kako bi se olakšala djelotvorna provedba Direktive u pogledu, među ostalim, upravljanja ranjivostima, mjera upravljanja kibersigurnosnim rizicima, obveza izvješćivanja i mehanizama za razmjenu informacija u području kibersigurnosti, države članice mogu surađivati s trećim zemljama i poduzimati aktivnosti koje se smatraju primjerenima u tu svrhu, uključujući razmjenu informacija o kiberprijetnjama, incidentima, ranjivostima, alatima i metodama, taktikama, tehnikama i postupcima, pripravnosti i vježbama za upravljanje kibersigurnosnom krizom, osposobljavanju, izgradnji povjerenja i strukturiranim mehanizmima za razmjenu informacija.

(75) Trebalo bi uvesti istorazinska ocjenjivanja kako bi se pomoglo u stjecanju znanja iz zajedničkih iskustava, jačanju uzajamnog povjerenja i postizanju visoke zajedničke razine kibersigurnosti. Istorazinska ocjenjivanja mogu rezultirati dragocjenim uvidima i preporukama kojima se jačaju sveukupni kapaciteti u području kibersigurnosti, stvarajući još jedan funkcionalan način za razmjenu najboljih praksi među državama članicama i doprinoseći većim razinama zrelosti država članica u području kibersigurnosti. Nadalje, pri istorazinskom ocjenjivanju trebalo bi uzeti u obzir rezultate sličnih mehanizama, kao što je sustav istorazinskog ocjenjivanja mreže CSIRT-ova, te bi trebalo stvoriti dodatnu vrijednost i izbjeći udvostručavanje. Pri provedbi istorazinskog ocjenjivanja ne bi se trebalo dovesti u pitanje pravo Unije ili nacionalno pravo o zaštiti povjerljivih i klasificiranih podataka.

(76) Skupina za suradnju trebala bi uspostaviti metodologiju za samoocjenu za države članice kako bi obuhvatila čimbenike kao što su razina provedbe mjera upravljanja kibersigurnosnim rizicima i obveza izvješćivanja, razina sposobnosti i djelotvornosti izvršavanja zadaća nadležnih tijela, operativne sposobnosti CSIRT-ova, razina provedbe uzajamne pomoći, razina provedbe mehanizama za razmjenu informacija o kibersigurnosti ili specifična pitanja prekogranične ili međusektorske prirode. Države članice trebalo bi poticati da redovito provode samoocjene te da u okviru skupine za suradnju predstavljaju rezultate svoje samoocjene i raspravljaju o njima.

(77) 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 procjene rizika i provedbu mjera upravljanja kibersigurnosnim rizicima primjerenih rizicima s kojima se suočava.

(78) Mjerama upravljanja kibersigurnosnim rizicima trebalo bi uzeti u obzir stupanj ovisnosti ključnog ili važnog subjekta o mrežnim i informacijskim sustavima te bi one trebale uključivati mjere za utvrđivanje rizika od incidenata, sprečavanje i otkrivanje incidenata te odgovor na njih i oporavak od njih kao i ublažavanje njihova učinka. Sigurnost mrežnih i informacijskih sustava trebala bi uključivati sigurnost podataka koji se pohranjuju, prenose i obrađuju. Mjere upravljanja kibersigurnosnim rizicima trebale bi osigurati sustavnu analizu, uzimajući u obzir ljudski faktor, kako bi se stekla cjelovita slika sigurnosti mrežnog i informacijskog sustava.

(79) Budući da prijetnje sigurnosti mrežnih i informacijskih sustava mogu biti različitog podrijetla, mjere upravljanja kibersigurnosnim rizicima trebale bi se temeljiti na pristupu kojim se uzimaju u obzir sve opasnosti i čiji je cilj zaštita mrežnih i informacijskih sustava i fizičkog okruženja tih sustava od događaja kao što su krađa, požar, poplava, prekid u telekomunikacijama ili prekid opskrbe električnom energijom ili od bilo kojeg neovlaštenog fizičkog pristupa te oštećenja i ometanja podataka i objekata za obradu podataka ključnog ili važnog 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 upravljanja kibersigurnosnim rizicima trebale bi se stoga odnositi i na fizičku sigurnost i sigurnost okruženja mrežnih i informacijskih sustava tako što će uključivati mjere zaštite tih sustava od kvarova u sustavu, ljudske pogreške, zlonamjernih radnji ili prirodnih pojava u skladu s europskim ili međunarodnim normama, kao što su one iz serije ISO/IEC 27000. U tom pogledu ključni i važni subjekti bi se u okviru svojih mjera upravljanja kibersigurnosnim rizicima trebali baviti i sigurnošću ljudskih resursa te bi trebali uspostaviti odgovarajuće politike kontrole pristupa. Te bi mjere trebale biti u skladu s Direktivom (EU) …/….[+].

[+] SL: molimo u tekst umetnuti broj Direktive iz dokumenta PE-CONS 51/22 (2020/0365(COD)).

(80) Za potrebu dokazivanja usklađenosti s mjerama upravljanja kibersigurnosnim rizicima i u nedostatku odgovarajućih europskih programa kibersigurnosne certifikacije donesenih u skladu s Uredbom (EU) 2019/881 Europskog parlamenta i Vijeća[1], države članice trebale bi, uz savjetovanje sa skupinom za suradnju i Europskom skupinom za kibersigurnosnu certifikaciju, promicati upotrebu relevantnih europskih i međunarodnih normi od strane ključnih i važnih subjekata ili pak mogu od subjekata zahtijevati korištenje certificiranih IKT proizvoda, IKT usluga i IKT procesa.

(81) Kako bi se izbjeglo nerazmjerno financijsko i administrativno opterećenje za ključne i važne subjekte, mjere upravljanja kibersigurnosnim rizicima trebale bi biti razmjerne rizicima kojima je izložen predmetni mrežni i informacijski sustav, uzimajući u obzir suvremenost takvih mjera i, ako je to primjenjivo, relevantne europske i međunarodne norme, kao i trošak njihove provedbe.

[1] 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.).

(82) Mjere upravljanja kibersigurnosnim rizicima trebale bi biti razmjerne stupnju izloženosti ključnog ili važnog subjekta rizicima te društvenom i gospodarskom učinku koji bi incident imao. Pri utvrđivanju mjera upravljanja kibersigurnosnim rizicima prilagođenih ključnim i važnim subjektima trebalo bi uzeti u obzir različite izloženosti ključnih i važnih subjekata riziku, kao što su kritičnost subjekta, rizici, uključujući društvene rizike, kojima je subjekt izložen, veličina subjekta te vjerojatnost nastanka incidenata i njihova ozbiljnost, uključujući njihov društveni i gospodarski učinak.

(83) Ključni i važni subjekti trebali bi jamčiti sigurnost mrežnih i informacijskih sustava koje upotrebljavaju u svojim djelatnostima. Ti sustavi ponajprije su privatni mrežni i informacijski sustavi kojima upravlja interno osoblje u IT-u ključnih i važnih subjekata ili vanjsko osoblje koji se brinu o sigurnosti. Mjere upravljanja kibersigurnosnim rizicima i obveze izvješćivanja utvrđeni u ovoj Direktivi trebali bi se primjenjivati na relevantne ključne i važne subjekte bez obzira na to održavaju li ti subjekti sami svoje mrežne i informacijske sustave ili eksternaliziraju njihovo održavanje.

(84) Uzimajući u obzir njihovu prekograničnu prirodu, pružatelji usluga DNS-a, registri naziva vršnih domena, pružatelji usluga računalstva u oblaku, pružatelji usluga podatkovnog centra, pružatelji mreža za isporuku sadržaja, pružatelji upravljanih usluga, pružatelji upravljanih sigurnosnih usluga, pružatelji internetskih tržišta, pružatelji internetskih tražilica, pružatelji platformi za usluge društvenih mreža i pružatelji usluga povjerenja trebali bi podlijegati visokom stupnju usklađenosti na razini Unije. Stoga bi provedbu mjera upravljanja kibersigurnosnim rizicima u odnosu na te subjekte trebalo olakšati putem provedbenog akta.

(85) Suzbijanje rizika koji proizlaze iz lanca opskrbe subjekta i njegova odnosa s dobavljačima, kao što su pružatelji usluga pohrane i obrade podataka ili pružatelji upravljanih sigurnosnih usluga i proizvođači softvera, posebno je važno s obzirom na učestalost incidenata u kojima su subjekti postali žrtve kibernapada i u kojima su zlonamjerni počinitelji mogli ugroziti sigurnost mrežnih i informacijskih sustava subjekta iskorištavanjem ranjivosti koje utječu na proizvode i usluge trećih strana. Ključni i važni subjekti bi stoga trebali procijeniti i uzeti u obzir ukupnu kvalitetu i otpornost proizvoda i usluga, mjera upravljanja kibersigurnosnim rizicima koje su ugrađene u njih, i kibersigurnosnih praksi svojih dobavljača i pružatelja usluga, uključujući njihove sigurne razvojne postupke. Ključne i važne subjekte bi trebalo posebno poticati da uključe mjere upravljanja kibersigurnosnim rizicima u ugovorne aranžmane sa svojim izravnim dobavljačima i pružateljima usluga. Ti subjekti bi mogli razmotriti rizike koji proizlaze iz drugih razina dobavljača i pružatelja usluga.

(86) U područjima kao što su odgovor na incidente, penetracijska testiranja, revizije sigurnosti i savjetovanje, pružatelji upravljane sigurnosne usluge imaju posebno važnu ulogu među pružateljima usluga u pomaganju subjektima u njihovim nastojanjima da spriječe i otkriju incidente te odgovore na njih ili se oporave od njih. Pružatelji upravljane sigurnosne usluge i sami su, međutim, bili meta kibernapada te zbog svoje bliske integracije u rad operatora predstavljaju poseban kibersigurnosni rizik. Ključni i važni subjekti bi stoga trebali postupati s većom pažnjom pri odabiru pružatelja upravljane sigurnosne usluge.

(87) U kontekstu svojih nadzornih zadaća i nadležna tijela mogu imati koristi od kibersigurnosnih usluga kao što su revizije sigurnosti, penetracijska testiranja ili odgovori na incidente.

(88) Ključni i važni subjekti bi trebali odgovoriti na rizike koji proizlaze iz njihove interakcije i odnosa s drugim dionicima unutar šireg ekosustava, među ostalim u pogledu borbe protiv industrijske špijunaže i štićenja poslovne tajne. Konkretno, ti 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. Isto tako, s obzirom na važnost i vrijednost podataka za aktivnosti ključnih i važnih subjekata, pri oslanjanju na usluge transformacije i analize podataka koje pružaju treće strane ti subjekti bi trebali poduzeti sve odgovarajuće mjere upravljanja kibersigurnosnim rizicima.

(89) Ključni i važni subjekti bi trebali usvojiti niz osnovnih praksi računalne kiberhigijene, kao što su načela nultog povjerenja, ažuriranja softvera, konfiguracija uređaja, segmentacija mreže, upravljanje identitetima i pristupom ili informiranje korisnika, organizirati osposobljavanje svojeg osoblja i podizati razinu osviještenosti u području kiberprijetnji, phishinga ili tehnika društvenog inženjeringa. Nadalje, ti subjekti bi trebali procijeniti vlastite kibersigurnosne sposobnosti i, ako je prikladno, integrirati tehnologije kojima se jača kibersigurnost, kao što su umjetna inteligencija ili sustavi strojnog učenja u cilju jačanja svojih sposobnosti i zaštite mrežnih i informacijskih sustava.

(90) Kako bi se dodatno suzbili ključni rizici u lancu opskrbe i pomoglo ključnim i važnim subjektima koji djeluju u sektorima obuhvaćenima ovom Direktivom da na odgovarajući način upravljaju rizicima u lancu opskrbe i rizicima povezanima s dobavljačima, skupina za suradnju, u suradnji s Komisijom i ENISA-om te, prema potrebi, nakon savjetovanja s relevantnim dionicima, među ostalim iz industrije, trebala bi provoditi koordinirane procjene sigurnosnih rizika kritičnih lanaca opskrbe, kao što je učinjeno za 5G mreže u skladu s Preporukom Komisije (EU) 2019/534[1], u cilju utvrđivanja ključnih IKT usluga, IKT sustava ili IKT proizvoda, relevantnih prijetnji i ranjivosti za pojedini sektor. Takvim koordiniranim procjenama sigurnosnog rizika trebale bi se utvrditi mjere, planovi ublažavanja i najbolje prakse za borbu protiv ključnih ovisnosti, potencijalnih pojedinačnih točaka prekida, prijetnji, ranjivosti i drugih rizika povezanih s lancem opskrbe te bi se u okviru njih trebali istražiti načini za daljnje poticanje njihovog šireg usvajanja od strane kritičnih i važnih subjekata. Potencijalni netehnički čimbenici rizika, kao što je neprimjeren utjecaj treće zemlje na dobavljače i pružatelje usluga, posebno u slučaju alternativnih modela upravljanja, uključuju prikrivene slabosti ili pristup stražnjeg ulaza i moguće sistemske poremećaje u opskrbi, posebno u slučaju ovisnosti o određenoj tehnologiji ili ovisnosti pružatelja.

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

(91) U koordiniranim procjenama sigurnosnog rizika u kritičnom lancu opskrbe, s obzirom na značajke predmetnog sektora, trebalo bi uzeti u obzir i tehničke i, ako je to relevantno, netehničke čimbenike, uključujući one definirane u Preporuci (EU) 2019/534, u usklađenoj procjeni rizika kibersigurnosti 5G mreža EU-a i u paketu instrumenata EU-a za kibersigurnost 5G tehnologije oko kojih se suglasila skupina za suradnju. Pri utvrđivanju lanaca opskrbe koji bi trebali biti podložni koordiniranoj procjeni sigurnosnog rizika, u obzir bi trebalo uzeti sljedeće kriterije: (i) mjera u kojoj se ključni i važni subjekti koriste određenim ključnim IKT uslugama, IKT sustavima ili IKT proizvodima i oslanjaju na njih; (ii) važnost specifičnih ključnih IKT usluga, IKT sustava ili IKT proizvoda u obavljanju ključnih ili osjetljivih funkcija, uključujući obradu osobnih podataka; (iii) dostupnost alternativnih IKT usluga, IKT sustava ili IKT proizvoda; (iv) otpornost cjelokupnog lanca opskrbe IKT uslugama, IKT sustavima ili IKT proizvodima tijekom njihovog životnog ciklusa na ometajuće događaje i (v) potencijalna buduća važnost novih IKT usluga, IKT sustava ili IKT proizvoda za aktivnosti subjekata. Nadalje, poseban bi naglasak trebalo staviti na IKT usluge, IKT sustave ili IKT proizvode koji podliježu posebnim zahtjevima koji proizlaze iz trećih zemalja.

(92) Kako bi se pojednostavnile 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 nadležnim tijelima na temelju Direktive (EU) 2018/1972 Europskog parlamenta i Vijeća[1] odnosno Uredbe (EU) br. 910/2014 omogućilo ostvarivanje koristi od pravnog okvira uspostavljenog ovom Direktivom, uključujući imenovanje CSIRT-a odgovornog za postupanje s incidentima, sudjelovanje predmetnih nadležnih tijela u aktivnostima skupine za suradnju i mreže CSIRT-ova, ta bi tijela trebalo obuhvatiti područjem primjene ove Direktive. Stoga bi trebalo izbrisati odgovarajuće odredbe utvrđene Uredbom (EU) br. 910/2014 i Direktivom (EU) 2018/1972 koje se odnose na uvođenje zahtjeva u pogledu sigurnosti i obavješćivanja za te vrste subjekata. Pravilima o obvezama izvješćivanja utvrđenima u ovoj Direktivi ne bi se trebala dovoditi u pitanje Uredba (EU) 2016/679 i Direktiva 2002/58/EZ.

[1] 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.).

(93) Kibersigurnosne obveze utvrđene u ovoj Direktivi trebale bi se smatrati dopunom zahtjeva uvedenih za pružatelje usluga povjerenja na temelju Uredbe (EU) br. 910/2014.
Od pružatelja usluga povjerenja trebalo bi se zahtijevati 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 incidente na temelju ove Direktive. Takve kibersigurnosne obveze i obveze izvješćivanja trebale bi se odnositi i na fizičku zaštitu pruženih usluga. I dalje se primjenjuju zahtjevi za kvalificirane pružatelje usluga povjerenja utvrđeni u članku 24. Uredbe (EU) br. 910/2014.

(94) Države članice mogu dodijeliti ulogu nadležnih tijela za usluge povjerenja nadzornim tijelima u skladu s Uredbom (EU) br. 910/2014 kako bi se osigurao nastavak postojećih praksi i nadogradilo znanje i iskustvo stečeni u primjeni te uredbe. U takvom slučaju, nadležna tijela na temelju ove Direktive trebala bi blisko i pravodobno surađivati s tim nadzornim tijelima razmjenjujući relevantne informacije kako bi se osigurao djelotvoran nadzor i usklađenost pružatelja usluga povjerenja sa zahtjevima utvrđenima u ovoj Direktivi i Uredbi (EU) br. 910/2014. Ako je to primjenjivo, CSIRT ili nadležno tijelo iz ove Direktive trebali bi odmah obavijestiti nadzorno tijelo iz Uredbe (EU) br. 910/2014 o svim ozbiljnim kiberprijetnjama ili značajnim incidentima o kojima su obaviješteni, a koji utječu na usluge povjerenja te o svim povredama ove Direktive od strane pružatelja usluga povjerenja. Za potrebe izvješćivanja, države članice mogu se, ako je to primjenjivo, koristiti jedinstvenom kontaktnom točkom uspostavljenom kako bi se postiglo zajedničko i automatsko izvješćivanje i nadzornog tijela iz Uredbe (EU) br. 910/2014 i CSIRT-a ili nadležnog tijela iz ove Direktive o incidentima.

(95) Prema potrebi i kako bi se izbjegli nepotrebni poremećaji, pri prenošenju ove Direktive trebalo bi uzeti u obzir postojeće nacionalne smjernice donesene za prenošenje pravila povezanih sa sigurnosnim mjerama utvrđenima u člancima 40. i 41. Direktive (EU) 2018/1972, čime bi se nadogradilo znanje i vještine stečene na temelju Direktive (EU) 2018/1972 u pogledu sigurnosnih mjera i obavijesti o incidentima. ENISA ujedno može izraditi smjernice o sigurnosnim zahtjevima i obvezama 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 na temelju Direktive (EU) 2018/1972 mogu dodijeliti ulogu nadležnih tijela za elektroničke komunikacije kako bi se osigurao nastavak postojećih praksi i nadogradilo znanje i iskustvo stečeni kao rezultat primjene te direktive.

(96) S obzirom na sve veću važnost brojevno neovisnih interpersonalnih komunikacijskih usluga kako su definirane u Direktivi (EU) 2018/1972, potrebno je osigurati da se i na takve usluge primjenjuju odgovarajući sigurnosni zahtjevi u skladu s njihovim posebnostima i gospodarskom važnošću. Budući da se prostor za napad nastavlja širiti, brojevno neovisne interpersonalne komunikacijske usluge, kao što su usluge razmjene poruka, postaju raširene vektori napada. Zlonamjerni počinitelji služe se platformama za komuniciranje sa žrtvama i poticanje žrtava na otvaranje nesigurnih internetskih stranica, čime se povećava vjerojatnost incidenata koji uključuju iskorištavanje osobnih podataka, a time i sigurnosti mrežnih i informacijskih sustava. Stoga bi pružatelji brojevno neovisnih interpersonalnih komunikacijskih usluga trebali osigurati odgovarajuću razinu sigurnosti mrežnih i informacijskih sustava s obzirom na rizike kojima 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 kako su definirane u Direktivi (EU) 2018/1972 koje se koriste brojevima, a koje nemaju stvarnu kontrolu nad prijenosom signala mrežama.

(97) Unutarnje tržište ovisi o funkcioniranju interneta više nego ikad. Usluge gotovo svih ključnih i važnih subjekata ovise o uslugama koje se pružaju putem interneta. Kako bi se osiguralo neometano pružanje usluga koje pružaju ključni i važni subjekti, važno je da svi pružatelji javnih elektroničkih komunikacijskih mreža imaju uspostavljene odgovarajuće mjere upravljanja kibersigurnosnim rizicima i da prijave značajne incidente povezane s njima. Države članice trebale bi osigurati održavanje sigurnosti javnih elektroničkih komunikacijskih mreža i zaštitu svojih ključnih sigurnosnih interesa od sabotaže i špijunaže. Budući da međunarodna povezivost poboljšava i ubrzava konkurentnu digitalizaciju Unije i njezina gospodarstva, incidente koji utječu na podmorske komunikacijske kabele trebalo bi prijaviti CSIRT-u ili, ako je to primjenjivo, nadležnom tijelu. U nacionalnoj strategiji za kibersigurnost trebalo bi, prema potrebi, uzeti u obzir kibersigurnost podmorskih komunikacijskih kabela i uključiti mapiranje potencijalnih kibersigurnosnih rizika i mjera ublažavanja kako bi se osigurala najviša razina njihove zaštite.

(98) Kako bi se zaštitila sigurnost javnih elektroničkih komunikacijskih mreža i javno dostupnih elektroničkih komunikacijskih usluga, trebalo bi promicati upotrebu tehnologija šifriranja, posebno prolaznog kriptiranja, kao i sigurnosnih koncepata usmjerenih na podatke, kao što su kartografija, segmentacija, označivanje, politika pristupa i upravljanje pristupom te odluke o automatiziranom pristupu. Prema potrebi, uporaba kriptiranja, posebno prolaznog kriptiranja, trebala bi biti obvezna za pružatelje javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga u skladu s načelima zadane i integrirane sigurnosti i privatnosti za potrebe ove Direktive. Upotrebu prolaznog kriptiranja trebalo bi uskladiti s ovlastima država članica da osiguraju zaštitu svojih ključnih sigurnosnih interesa i javne sigurnosti te da dopuste sprečavanje, istragu, otkrivanje i progon kaznenih djela u skladu s pravom Unije. Međutim, to ne bi trebalo oslabiti prolazno kriptiranje, koje je kritična tehnologija za učinkovitu zaštitu podataka i privatnosti i sigurnost komunikacija.

(99) Kako bi se zaštitila sigurnost i spriječile zlouporaba javnih elektroničkih komunikacijskih mreža i javno dostupnih elektroničkih komunikacijskih usluga te manipulacija njima, trebalo bi promicati primjenu standarda sigurnog usmjeravanja kako bi se osigurale cjelovitost i pouzdanost funkcija usmjeravanja u cijelom ekosustavu pružatelja usluga pristupa internetu.

(100) Kako bi se zaštitila funkcionalnost i cjelovitost interneta te promicala sigurnost i otpornost DNS-a, relevantne dionike, uključujući subjekte iz privatnog sektora Unije, pružatelje javno dostupnih elektroničkih komunikacijskih usluga, posebno pružatelje usluga pristupa internetu, i pružatelje internetskih tražilica trebalo bi poticati na donošenje strategije diversifikacije prevođenja DNS-a. Nadalje, države članice trebale bi poticati razvoj i upotrebu javne i sigurne usluge europskih prevoditelja DNS-a.

(101) Ovom se Direktivom utvrđuje pristup izvješćivanju o značajnim incidentima u više faza kako bi se uspostavila prava ravnoteža između, s jedne strane, brzog izvješćivanja koje doprinosi ublažavanju potencijalnog širenja značajnih incidenata i omogućuje ključnim i važnim 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 subjekata i cijelih sektora. U tom pogledu ova bi Direktiva trebala uključivati i izvješćivanje o incidentima koji bi, na temelju početne procjene koju dotični subjekt provodi, mogli uzrokovati ozbiljne poremećaje u funkcioniranju usluga ili financijske gubitke za taj subjekt ili utjecati na druge fizičke ili pravne osobe uzrokovanjem znatne materijalne ili nematerijalne štete. Takvom početnom procjenom trebalo bi uzeti u obzir, između ostalog, pogođene mrežne i informacijske sustave, a posebno njihovu važnost u pružanju usluga predmetnog subjekta, ozbiljnost i tehničke značajke kiberprijetnje te sve temeljne ranjivosti koje se iskorištavaju kao i iskustvo subjekta sa sličnim incidentima. Pokazatelji kao što su mjera u kojoj je ugroženo funkcioniranje usluge, trajanje incidenta ili broj primatelja usluga na koje je incident utjecao mogli bi imati važnu ulogu u utvrđivanju toga je li poremećaj u funkcioniranju usluge ozbiljan.

(102) Kada ključni ili važni subjekti saznaju za značajan incident, trebali bi biti obvezni bez nepotrebne odgode, a u svakom slučaju u roku od 24 sata, podnijeti rano upozorenje. Nakon tog ranog upozorenja trebala bi uslijediti obavijest o incidentu. Dotični subjekti bi trebali podnijeti obavijest o incidentu bez nepotrebne odgode, a u svakom slučaju u roku od 72 sata otkad saznaju za značajan incident, u prvom redu kako bi ažurirali informacije podnesene u ranom upozorenju i naveli početnu procjenu značajnog incidenta, uključujući njegovu ozbiljnosti i učinak te, ako su dostupni, pokazatelje ugroženosti. Završno izvješće trebalo bi podnijeti najkasnije jedan mjesec nakon obavijesti o incidentu. Rano upozorenje trebalo bi sadržavati samo informacije koje su nužne kako bi CSIRT-ovi ili, ako je to primjenjivo, nadležno tijelo bili upoznati s značajnim incidentom i kako bi se dotičnom subjektu, prema potrebi, omogućilo traženje pomoći. U takvom ranom upozoravanju, ako je to primjenjivo, trebalo bi navesti postoji li sumnja da je značajan incident uzrokovan nezakonitim ili zlonamjernim djelovanjem te postoji li vjerojatnost da će imati prekogranični učinak. Države članice trebale bi osigurati da se zbog obveze podnošenja tog ranog upozorenja ili naknadne obavijesti o incidentu resursi subjekta koji obavješćuje ne preusmjeruju s aktivnosti povezanih s postupanjem sa značajnim incidentima koje bi trebale biti prioritetne kako bi se spriječilo da se zbog obveza izvješćivanja o incidentima resursi za postupanje sa značajnim incidentima preusmjere ili na drugi način ugroze aktivnosti subjekta u tom pogledu. U slučaju incidenta koji je u tijeku u trenutku podnošenja završnog izvješća države članice trebale bi osigurati da dotični subjekti dostave izvješće o napretku u tom trenutku te završno izvješće u roku od jednog mjeseca od postupanja sa značajnim incidentom.

(103) Ako je to primjenjivo, ključni i važni subjekti bi trebali bez nepotrebnog odgađanja obavijestiti svoje primatelje usluga o svim mjerama ili pravnim sredstvima koje mogu poduzeti kako bi ublažili rizike koji proizlaze iz ozbiljne kiberprijetnje. Ti subjekti bi trebali, prema potrebi, a posebno ako je vjerojatno da će se ozbiljna kiberprijetnja ostvariti, svoje primatelje usluga obavijestiti i o samoj prijetnji. Zahtjev za izvješćivanje tih primatelja usluga o ozbiljnim kiberprijetnjama trebao bi se ispuniti u najvećoj mogućoj mjeri, ali ne bi smio podrazumijevati oslobađanje tih subjekata od obveze da o vlastitom trošku poduzme odgovarajuće i hitne mjere kako bi se spriječile ili uklonile sve takve prijetnje i ponovno uspostavila normalna sigurnosna razina usluge. Pružanje takvih informacija o ozbiljnim kiberprijetnjama trebalo bi biti besplatno za primatelje usluga i sastavljeno na lako razumljivom jeziku.

(104) Pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga trebali bi provoditi tehničku i integriranu sigurnost i obavijestiti primatelje svojih usluga o ozbiljnim kiberprijetnjama te o mjerama koje mogu poduzeti kako bi očuvali sigurnost svojih uređaja i komunikacija, na primjer upotrebom posebnih vrsta softvera ili tehnologija kriptiranja.

(105) Proaktivan pristup kiberprijetnjama ključna je sastavnica upravljanja kibersigurnosnim rizikom te bi nadležnim tijelima trebao omogućiti da učinkovito spriječe da se kiberprijetnje pretvore u incidente koji mogu uzrokovati znatnu materijalnu ili nematerijalnu štetu. Zato je obavješćivanje o kiberprijetnjama od presudne važnosti i subjekte se u tu svrhu potiče da dobrovoljno izvješćuju o kiberprijetnjama.

(106) Kako bi se pojednostavnilo izvješćivanje o informacijama koje se zahtijevaju na temelju ove Direktive te usto smanjilo administrativno opterećenje za subjekte, države članice trebale bi osigurati tehnička sredstva za podnošenje relevantnih informacija o kojima se treba izvješćivati, kao što su jedinstvena ulazna točka, automatizirani sustavi, internetski obrasci, sučelja prilagođena korisnicima, predlošci, namjenske platforme koje upotrebljavaju subjekti, neovisno o tome jesu li obuhvaćeni područjem primjene ove Direktive ili su iz njega isključeni. Financiranje Unije kojim se podupire provedba ove Direktive, osobito u okviru programa Digitalna Europa, uspostavljenog Uredbom (EU) 2021/694 Europskog parlamenta i Vijeća[1], moglo bi uključivati potporu za jedinstvene ulazne točke. Nadalje, subjekti često određeni incident, zbog njegovih značajki, moraju prijaviti različitim tijelima u skladu s obvezama obavješćivanja uključenima u razne pravne instrumente. Takvi slučajevi stvaraju dodatno administrativno opterećenje te bi također mogli dovesti do nesigurnosti u pogledu oblika obavijesti i postupanja s njima. Ako je uspostavljena jedinstvena ulazna točka, države članice potiču se i na to da upotrebljavaju tu jedinstvenu ulaznu točku za obavješćivanje o sigurnosnim incidentima koje se zahtijeva u skladu s drugim pravom Unije, kao što su Uredba (EU) 2016/679 i Direktiva 2002/58/EZ. Upotreba takve jedinstvene ulazne točke za izvješćivanja o sigurnosnim incidentima u skladu s Uredbom (EU) 2016/679 i Direktivom 2002/58/EZ ne bi trebala utjecati na primjenu odredaba Uredbe (EU) 2016/679 i Direktive 2002/58/EZ, posebno onih koje se odnose na neovisnost tijela navedenih u njima. U suradnji sa skupinom za suradnju ENISA bi trebala izraditi zajedničke predloške za obavješćivanje s pomoću smjernica za pojednostavljivanje i usklađivanje informacija o kojima se treba izvješćivati koje se zahtijevaju u skladu s pravom Unije, čime bi se smanjilo administrativno opterećenje za subjekte koji obavješćuju.

[1] Uredba (EU) 2021/694 Europskog parlamenta i Vijeća od 29. travnja 2021. o uspostavi programa Digitalna Europa te stavljanju izvan snage Odluke (EU) 2015/2240 (SL L 166, 11.5.2021., str. 1.).

(107) 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 Europski centar za kiberkriminalitet (EC3) i ENISA olakšavaju koordinaciju između nadležnih tijela i tijela za izvršavanje zakonodavstva različitih država članica.

(108) 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 iz Uredbe (EU) 2016/679 i Direktive 2002/58/EZ.

(109) Vođenje točnih i potpunih baza podataka s podacima o registraciji naziva domena (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 širom Unije. U tu specifičnu svrhu od registara naziva vršnih domena i subjekata koji pružaju usluge registracije naziva domena trebalo bi zahtijevati da obrađuju određene podatke potrebne za postizanje te svrhe. Obrada koja uključuje osobne podatke trebala bi predstavljati pravnu obvezu u smislu članka 6. stavka 1. točke (c) Uredbe (EU) 2016/679. Tom se obvezom ne dovodi u pitanje mogućnost prikupljanja podataka o registraciji naziva domena u druge svrhe, na primjer na temelju ugovornih aranžmana ili pravnih zahtjeva utvrđenih u drugom pravu Unije ili nacionalnom pravu. Tom se obvezom nastoji ostvariti potpun i točan skup registracijskih podataka te ona ne bi trebala dovesti do višestrukog prikupljanja istih podataka. Registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena trebali bi međusobno surađivati kako bi se izbjeglo udvostručavanje navedene zadaće.

(110) Dostupnost i pravodobna pristupačnost podacima o registraciji naziva domena zakonitim tražiteljima pristupa ključna je za potrebe sprečavanja i borbe protiv zloupotrebe DNS-a te za sprečavanje i otkrivanje incidenta te odgovaranje na njih. Zakonitim tražiteljima pristupa smatra se svaka fizička ili pravna osoba koja podnosi zahtjev na temelju prava Unije ili nacionalnog prava. Oni mogu uključivati tijela nadležna na temelju ove Direktive i ona koja su u skladu s pravom Unije ili nacionalnim pravom nadležna za sprečavanje, istragu, otkrivanje ili progon kaznenih djela te CERT-ove ili CSIRT-ove. Od registra naziva vršnih domena i subjekata koji pružaju usluge registracije naziva domena trebalo bi zahtijevati da zakonitim tražiteljima pristupa omoguće legalan pristup podacima o registraciji određenih naziva domena, koji su nužni za potrebe zahtjeva za pristup, u skladu s pravom Unije i nacionalnim pravom. Zahtjev zakonitih tražitelja pristupa trebao bi biti popraćen obrazloženjem kojim se omogućuje procjena nužnosti pristupa podacima.

(111) Kako bi se osigurala dostupnost točnih i potpunih podataka o registraciji naziva domena, registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena trebali bi prikupljati i jamčiti cjelovitost i dostupnost podataka o registraciji naziva domena. Posebno, registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena trebali bi uspostaviti politike i postupke za prikupljanje i održavanje točnih i potpunih podataka o registraciji naziva domena te za sprečavanje i ispravljanje netočnih registracijskih podataka u skladu s pravom Unije o zaštiti podataka. Tim politikama i postupcima trebalo bi uzeti u obzir, u mjeri u kojoj je to moguće, norme koje su razvile strukture upravljanja s više dionika na međunarodnoj razini. Registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena trebali bi usvojiti i provoditi proporcionalne postupke za provjeru podataka o registraciji naziva domena. Ti bi postupci trebali odražavati najbolje prakse korištene u sektoru i, u mjeri u kojoj je to moguće, napredak postignut u području elektroničke identifikacije. Primjeri postupaka provjere mogu uključivati *ex ante* kontrole provedene u trenutku registracije i *ex post* kontrole provedene nakon registracije. Registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena trebali bi u prvom redu provjeriti barem jedan on načina za kontaktiranje korisnika domene.

(112) Od registra vršnih domena i subjekata koji pružaju usluge registracije naziva domena trebalo bi zahtijevati da javno objave podatke o registraciji naziva domena koji su izvan područja primjene pravila Unije o zaštiti podataka, kao što su podaci o pravnim osobama, u skladu s preambulom Uredbe (EU) 2016/679. Za pravne osobe registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena trebali bi javno objaviti barem ime korisnika domene i broj telefona za kontakt. Trebalo bi objaviti i e-adresu za kontakt pod uvjetom da ne sadržava osobne podatke, kao što je to slučaj sa pseudonimima za e-poštu ili funkcionalnim profilima. Registri naziva vršnih domena i subjekti koji pružaju usluge registracije 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 zahtijevati da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena bez nepotrebne odgode odgovaraju na zahtjeve za otkrivanje podataka o registraciji naziva domena koje upute zakoniti tražitelji pristupa. Registri vršnih domena i subjekti koji 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. Tim politikama i postupcima trebalo bi uzeti u obzir, u mjeri u kojoj je to moguće, sve smjernice i standarde koje su razvile upravljačke strukture s više dionika na međunarodnoj razini. Postupak pristupa mogao bi uključivati i upotrebu sučelja, portala ili drugog tehničkog alata kako bi se osigurao učinkovit sustav za podnošenje zahtjeva i pristupanje registracijskim podacima. S ciljem promicanja usklađenih praksi na unutarnjem tržištu, Komisija može, ne dovodeći u pitanje nadležnosti Europskog odbora za zaštitu podataka, pružiti smjernice u vezi s takvim postupcima, kojima se u mogućoj mjeri uzimaju u obzir standardi koje su razvile strukture upravljanja s više dionika na međunarodnoj razini. Države članice trebale bi osigurati da sve vrste pristupa osobnim i neosobnim registracijskim podacima domena budu besplatne.

(113) Za subjekte obuhvaćene područjem primjene ove Direktive trebalo bi se smatrati da su u nadležnosti države članice u kojoj imaju poslovni nastan. Ipak, trebalo bi smatrati da su pružatelji javnih elektroničkih komunikacijskih mreža ili pružatelji javno dostupnih elektroničkih komunikacijskih usluga u nadležnosti države članice u kojoj pružaju usluge. Trebalo bi smatrati da su pružatelji usluga DNS-a, registri naziva vršnih domena, subjekti koji pružaju usluge registracije naziva domena, pružatelji usluga računalstva u oblaku, pružatelji usluga podatkovnog centra, pružatelji mreža za isporuku sadržaja, pružatelji upravljanih usluga, pružatelji upravljanih sigurnosnih usluga, pružatelji internetskih tržišta, pružatelji internetskih tražilica i pružatelji platformi za usluge društvenih mreža u nadležnosti države članice u kojoj imaju glavni poslovni nastan u Uniji. Subjekti javne uprave trebali bi biti u nadležnosti države članice koja ih je osnovala. 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, uzajamno si pomagati i, prema potrebi, provoditi zajedničke nadzorne aktivnosti. Ako države članice imaju nadležnost, u skladu s načelom ne bis in idem ne bi trebale izricati mjere izvršavanja ili kazne više od jedanput za isto ponašanje.

(114) Kako bi se u obzir uzela prekogranična priroda usluga i djelatnosti pružatelja usluga DNS-a, registara naziva vršnih domena, subjekata koji pružaju usluge registracije naziva domena, pružatelja usluga računalstva u oblaku, pružatelja upravljanih usluga, pružatelja upravljanih sigurnosnih usluga, pružatelja internetskih tržišta, pružatelja internetske tražilice i pružatelja platformi za usluge društvenih mreža, 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 učinkovito obavljanje djelatnosti u okviru stabilnih aranžmana. Pravni oblik takvih aranžmana, bilo da je riječ o podružnici ili društvu kćeri 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. Trebalo bi smatrati da se glavni poslovni nastan nalazi u državi članici u kojoj se, gledano na razini Unije, pretežno donose odluke povezane s mjerama upravljanja kibersigurnosnim rizicima. To obično odgovara mjestu u Uniji na kojem se nalazi središnja uprava subjekata. Ako se takva država članica ne može utvrditi ili ako se takve odluke ne donose u Uniji, trebalo bi smatrati da se glavni poslovni nastan nalazi u državi članici u kojoj se provode kibersigurnosne operacije. Ako se takva država članica ne može utvrditi, trebalo bi smatrati da se glavni poslovni nastan nalazi u državi članici u kojoj subjekti imaju poslovnu jedinicu s najvećim brojem zaposlenika u Uniji. Ako usluge pruža grupa poduzetnika, glavni poslovni nastan vladajućeg poduzetnika trebao bi se smatrati glavnim nastanom grupe poduzetnika.

(115) Ako javno dostupnu rekurzivnu uslugu DNS-a 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.

(116) Ako pružatelj usluga DNS-a, registar naziva vršnih domena, subjekt koji pruža usluge registracije naziva domena, pružatelj usluga računalstva u oblaku, pružatelj usluga podatkovnog centra, pružatelj mreža za isporuku sadržaja, pružatelj upravljanih usluga, pružatelj upravljanih sigurnosnih usluga ili pružatelj internetskih tržišta, internetskih tražilica ili platformi za usluge društvenih mreža koji nema poslovni nastan u Uniji, a nudi usluge unutar Unije, trebao bi imenovati predstavnika u Uniji. Kako bi se utvrdilo nudi li takav subjekt usluge u Uniji, trebalo bi provjeriti planira li subjekt nuditi usluge osobama u jednoj državi članici ili više njih. Sama dostupnost u Uniji internetskih stranica subjekta ili posrednog davatelja takvih usluga ili e-adrese ili drugih podataka za kontakt ili korištenje jezikom koji je uobičajeno u upotrebi u trećoj zemlji u kojoj subjekt ima poslovni nastan, ne bi se trebala smatrati dovoljnom za utvrđivanje takve namjere. Međutim, čimbenici kao što su korištenje jezikom ili valutom koji su uobičajeno u uporabi u jednoj državi članica ili više njih, s mogućnošću naručivanja usluga na tom jeziku ili spominjanje kupaca ili korisnika koji se nalaze u Uniji, mogli bi ukazati na to da je očito da subjekt planira nuditi usluge u Uniji. Predstavnik bi trebao djelovati u ime subjekta te bi nadležna tijela ili CSIRT-ovi trebali moći obratiti se predstavniku. Subjekt bi trebao pisanim ovlaštenjem izričito imenovati predstavnika da djeluje u njegovo ime s obzirom na obveze tog subjekta utvrđenih u ovoj Direktivi, što uključuje izvješćivanja o incidentima.

(117) Kako bi se osigurao jasan pregled pružatelja usluga DNS-a, registara naziva vršnih domena, subjekata koji pružaju usluge registracije naziva domena, pružatelja usluga računalstva u oblaku, pružatelja usluga podatkovnog centra, pružatelja mreža za isporuku sadržaja, pružatelja upravljanih usluga, pružatelja upravljanih sigurnosnih usluga, pružatelja internetskih tržišta, pružatelja internetskih tražilica i pružatelja platformi za usluge društvenih mreža, koji pružaju usluge obuhvaćene područjem primjene ove Direktive širom Unije, ENISA bi trebala uspostaviti i voditi registar takvih subjekata na temelju informacija koje prime države članice, ako je to primjenjivo u okviru nacionalnih mehanizama uspostavljenih kako bi se subjekti sami registrirali. Jedinstvene kontaktne točke trebale bi ENISA-i prosljeđivati informacije i sve njihove izmjene. Kako bi se osigurala točnost i potpunost informacija koje bi trebale biti uključene u taj registar, države članice mogu ENISA-i dostavljati informacije o tim subjektima koje su dostupne u bilo kojem od nacionalnih registara. ENISA i države članice trebale bi poduzeti mjere za olakšavanje interoperabilnosti takvih registara te pritom osigurati zaštitu povjerljivih ili klasificiranih podataka. ENISA bi trebala uspostaviti odgovarajuće protokole za klasifikaciju informacija i upravljanje njima kako bi se osigurala sigurnost i povjerljivost otkrivenih informacija i ograničili pristup tim informacijama predviđenim korisnicima te njihovo skladištenje i prijenos.

(118) Ako se informacije koje su klasificirane u skladu s pravom Unije ili nacionalnim pravom razmjenjuju, dostavljaju ili na drugi način dijele u skladu s ovom Direktivom, trebalo bi primjenjivati odgovarajuća posebna pravila o postupanju s klasificiranim podacima. Usto, ENISA bi trebala uspostaviti infrastrukturu, postupke i pravila za postupanje s osjetljivim i klasificiranim podacima u skladu s primjenjivim sigurnosnim pravilima za zaštitu klasificiranih podataka EU-a.

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

(120) Stoga bi države članice trebale poticati subjekte te bi im pomagati da zajednički iskorištavaju svoja znanja i praktična iskustva na strateškoj, taktičkoj i operativnoj razini kako bi povećali svoje sposobnosti za odgovarajuće sprečavanje, otkrivanje, pružanje odgovora i oporavak kada je riječ o incidentima ili ublažavanju njihova učinka. Stoga je potrebno omogućiti razvijanje mehanizama dobrovoljne razmjene informacija na razini Unije. U tu bi svrhu države članice trebale aktivno pomagati subjektima, kao što su subjekti koji pružaju usluge i istraživanja u području kibersigurnosti, kao i subjektima koji nisu obuhvaćeni područjem primjene ove Direktive, i poticati ih na sudjelovanje u takvim mehanizmima razmjene informacija. Ti bi se mehanizmi trebali provoditi u skladu s pravilima Unije o tržišnom natjecanju te pravom Unije o zaštiti podataka.

(121) Obrada osobnih podataka u mjeri u kojoj je to potrebno i razmjerno za potrebe osiguravanja sigurnosti mrežnih i informacijskih sustava koju provode ključni i važni subjekti mogla bi se smatrati zakonitom na temelju toga što je takva obrada usklađena s pravnom obvezom kojoj podliježe voditelj obrade, a u skladu sa zahtjevima iz članka 6. stavka 1. točke (c) i članka 6. stavka 3. Uredbe (EU) 2016/679. Obrada osobnih podataka mogla bi biti potrebna i zbog legitimnih interesa ključnih i važnih subjekata kao i pružatelja sigurnosnih tehnologija i usluga koji djeluju u ime tih subjekata, u skladu s člankom 6. stavkom 1. točkom (f) Uredbe (EU) 2016/679, među ostalim ako je takva obrada nužna za potrebe mehanizama razmjene informacija o kibersigurnosti ili dobrovoljno obavješćivanje o relevantnim informacijama u skladu s ovom Direktivom. Mjere za sprečavanje, otkrivanje, identifikaciju, suzbijanje, 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, pokazatelji ugroženosti, taktike, tehnike i postupci, kibersigurnosna upozorenja i konfiguracijski alati mogli bi zahtijevati obradu određenih kategorija osobnih podataka, kao što su IP adrese, jedinstveni lokatori resursa (URL-ovi), nazivi domena, e-adrese, te vremenski žigovi ako se njima otkrivaju osobni podaci. Obrada osobnih podataka koju provode nadležna tijela, jedinstvene kontaktne točke i CSIRT-ovi mogla bi predstavljati pravnu obvezu ili se smatrati nužnom za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade podataka u skladu s člankom 6. stavkom 1. točkom (c) ili (e) te člankom 6. stavkom 3. Uredbe (EU) 2016/679 ili za ostvarivanje legitimnog interesa ključnih i važnih subjekata, kako je navedeno u članku 6. stavku 1. točki (f) te uredbe.

Nadalje, nacionalnim pravom mogla bi se utvrditi pravila kojima se nadležnim tijelima, jedinstvenim kontaktnim točkama i CSIRT-ovima, u mjeri u kojoj je to potrebno i razmjerno u svrhu jamčenja sigurnosti mrežnih i informacijskih sustava ključnih i važnih subjekata, omogućuje obrada posebnih kategorija osobnih podataka u skladu s člankom 9. Uredbe (EU) 2016/679, u prvom redu na temelju predviđanja odgovarajućih i posebnih mjera za zaštitu temeljnih prava i interesa fizičkih osoba, uključujući tehnička ograničenja ponovne uporabe takvih podataka i primjenu najsuvremenijih mjera sigurnosti i zaštite privatnosti, kao što su pseudonimizacija ili kriptiranje u slučaju da anonimizacija može znatno utjecati na svrhu koja se želi postići.

(122) Kako bi se ojačale nadzorne ovlasti i mjere koje pomažu u osiguravanju učinkovite usklađenosti, ovom bi se Direktivom trebao predvidjeti popis minimalnih nadzornih mjera i sredstava uz pomoć kojih nadležna tijela mogu nadzirati ključne i važne subjekte. Usto, Direktivom bi se trebalo utvrditi razlikovanje sustava nadzora između ključnih i važnih subjekata kako bi se osigurala pravedna ravnoteža obveza tih subjekata i nadležnih tijela. Stoga bi se na ključne subjekte trebao primjenjivati sveobuhvatni *ex ante* i *ex post* nadzorni sustav, dok bi se na važne subjekte trebao primjenjivati blagi sustav samo *ex post* nadzora. Od važnih subjekata ne bi trebalo zahtijevati da sustavno dokumentiraju usklađenost sa mjerama upravljanja 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. *Ex post* nadzor nad važnim subjektima može se pokrenuti na temelju dokaza, naznaka ili informacija o kojima su nadležna tijela obaviještena i za koje ta tijela smatraju da upućuju na moguće povrede ove Direktive. 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.

(123) Pri obavljanju nadzornih zadaća nadležna tijela ne bi trebala nepotrebno ometati poslovne aktivnosti predmetnog subjekta. Ako nadležna tijela obavljaju svoje nadzorne zadaće u vezi s ključnim subjektima, uključujući provedbu inspekcija na lokaciji i neizravnog nadzora, istragu povreda ove Direktive i provođenje revizija sigurnosti i analiza sigurnosti, ona bi na najmanju moguću mjeru trebala svesti učinak na poslovne aktivnosti predmetnog subjekta.

(124) Pri provedbi *ex ante* nadzora nadležna tijela trebala bi moći na razmjeran način odlučiti o određivanju prioriteta u pogledu primjene nadzornih mjera 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 rizika. Konkretnije, te metodologije mogle bi uključivati kriterije ili referentna mjerila za razvrstavanje ključnih subjekata u kategorije rizika i odgovarajućih nadzornih mjera i preporučenih sredstava po kategoriji rizika, kao što su upotreba, učestalost ili vrste inspekcija na lokaciji ili ciljanih revizija sigurnosti ili analiza sigurnosti, vrsta informacija koje treba zahtijevati i razina detalja tih informacija. Takve nadzorne metodologije mogle bi biti popraćene i programima rada te bi ih se moglo redovito ocjenjivati i preispitivati, među ostalim u pogledu aspekata kao što su dodjela resursa i potrebe u vezi s resursima. U odnosu na subjekte javne uprave nadzorne ovlasti trebalo bi izvršavati u skladu s nacionalnim zakonodavnim i institucionalnim okvirima.

(125) Nadležna tijela trebala bi osigurati da njihove nadzorne zadaće u odnosu na ključne i važne subjekte obavljaju osposobljeni stručnjaci, koji bi trebali posjedovati vještine potrebne za obavljanje tih zadaća, osobito u smislu provedbe inspekcija na lokaciji i neizravnog nadzora, uključujući utvrđivanje nedostataka u bazama podataka, hardveru, vatrozidovima, kriptiranju i mrežama. Ti bi se nadzori trebali provoditi na objektivan način.

(126) U propisno obrazloženim slučajevima ako je nadležno tijelo upoznato s ozbiljnom kiberprijetnjom ili neposrednim rizikom, ono bi trebalo biti u stanju donijeti hitne odluke o izvršavanju radi sprečavanja incidenta ili odgovaranja na njega.

(127) Kako bi izvršavanje bilo učinkovito, potrebno je utvrditi popis minimalnih ovlasti izvršavanja koje se mogu primijeniti za kršenje mjera upravljanja kibersigurnosnim rizicima i obveza izvješćivanja predviđenih ovom Direktivom, čime bi se uspostavio jasan i usklađen okvir za takvo izvršavanje širom Unije. Posebna bi se pozornost trebala posvetiti prirodi, ozbiljnosti i trajanju povrede ove Direktive, uzrokovanoj materijalnoj ili nematerijalnoj šteti, bez obzira na to je li povreda bila namjerna ili nehotična, mjerama poduzetima radi sprečavanja ili ublažavanja materijalne ili nematerijalne štete, stupnju odgovornosti ili svim relevantnim prethodnim povredama, stupnju suradnje s nadležnim tijelom kao i bilo kojem drugom otegotnom ili olakotnom čimbeniku. Mjere izvršavanja, uključujući upravne novčane kazne, trebale bi biti proporcionalne, a njihovo izricanje podlijegati odgovarajućim postupovnim zaštitnim mjerama u skladu s općim načelima prava Unije i Poveljom Europske unije o temeljnim pravima („Povelja“), uključujući pravo na djelotvoran pravni lijek i pošteno suđenje, pretpostavku nedužnosti i prava na obranu.

(128) Ovom se Direktivom od država članica ne zahtijeva da predvide kaznenu ili građansku odgovornost u pogledu fizičkih osoba odgovornih za osiguravanje usklađenosti subjekta s ovom Direktivom u vezi sa štetom koju su treće strane pretrpjele zbog kršenja ove Direktive.

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

(130) Kada se upravna novčana kazne izriče ključnom ili važnom subjektu koji je poduzetnik, poduzetnik bi se u te svrhe trebao smatrati poduzetnikom u skladu s člancima 101. i 102. UFEU-a. Ako se upravna novčana kazna izriče osobi koja nije poduzetnik, pri razmatranju odgovarajućeg iznosa novčane kazne nadležno 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 tijela javne vlasti. Izricanje upravne novčane kazne ne utječe na primjenu ovlasti nadležnih tijela ili drugih sankcija utvrđenih u nacionalnim pravilima kojima se prenosi ova Direktiva.

(131) Države članice trebale bi moći 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 upravnih sankcija ne bi smjelo dovesti do kršenja načela *ne bis in idem*, kako ga tumači Sud Europske unije.

(132) Ako ovom Direktivom nisu usklađene upravne sankcije ili ako je to potrebno u drugim slučajevima, na primjer u slučaju ozbiljne povrede ove Direktive, države članice trebale bi uvesti sustav kojim se predviđaju učinkovite, proporcionalne i odvraćajuće sankcije. Prirodu tih sankcija, i to jesu li kaznenog ili upravnog karaktera, trebalo bi odrediti u nacionalnom pravu.

(133) Kako bi se dodatno ojačali djelotvornost i odvraćajući učinak mjera izvršavanja koje se primjenjuju na povrede ove Direktive, nadležna tijela trebala bi biti ovlaštena privremeno suspendirati ili zahtijevati privremenu suspenziju certifikata ili ovlaštenja za dio relevantnih usluga ili sve relevantne usluge koje ključni subjekt pruža ili djelatnosti koje obavlja i zahtijevati izricanje privremene zabrane obavljanja upravljačkih dužnosti svakoj fizičkoj osobi koja upravljačke dužnosti obavlja na razini glavnog izvršnog direktora ili pravnog zastupnika. S obzirom na njihovu ozbiljnost i učinak na aktivnosti subjekata te naposljetku na njihove korisnike, takve bi privremene suspenzije ili zabrane trebalo primjenjivati samo razmjerno ozbiljnosti povrede i uzimajući u obzir posebne okolnosti svakog slučaja, uključujući namjernu ili nehotičnu prirodu povrede kao i mjere poduzete radi sprečavanja ili ublažavanja materijalne ili nematerijalne štete. Takve bi se privremene suspenzije ili zabrane trebale primjenjivati samo kao *ultima ratio*, odnosno tek nakon što se iscrpe druge odgovarajuće mjere izvršavanja utvrđene ovom Direktivom i samo dok subjekti na koje se primjenjuju ne poduzmu potrebne mjere za otklanjanje nedostataka ili dok ne ispune zahtjeve nadležnog tijela na koje se odnose takve privremene suspenzije ili zabrane. Izricanje takvih privremenih suspenzija ili zabrana treba podlijegati odgovarajućim postupovnim zaštitnim mjerama u skladu s općim načelima prava Unije i Poveljom, uključujući pravo na djelotvoran pravni lijek i pošteno suđenje, pretpostavku nedužnosti i prava na obranu.

(134) Kako bi se osiguralo da subjekti ispunjavaju svoje obveze utvrđene u ovoj Direktivi, države članice trebale bi surađivati i međusobno si pomagati u pogledu nadzornih mjera i mjera izvršavanja, posebno ako subjekt pruža usluge u više od jedne države članice ili ako se njegovi mrežni i informacijski sustavi nalaze u državi članici koja nije ona u kojoj pruža usluge. Pri pružanju pomoći nadležno tijelo primatelj zahtjeva trebalo bi poduzeti nadzorne mjere ili mjere izvršavanja u skladu s nacionalnim pravom. Kako bi se osiguralo neometano funkcioniranje uzajamne pomoći na temelju ove Direktive, nadležna tijela trebala bi se koristiti skupinom za suradnju kao forumom za raspravljanje o različitim slučajevima i konkretnim zahtjevima za pomoć.

(135) Kako bi se osigurali učinkovit nadzor i izvršavanje, posebno u situacijama s prekograničnom dimenzijom, država članica koja primi zahtjev za uzajamnu pomoć trebala bi, u okvirima tog zahtjeva, poduzeti odgovarajuće nadzorne mjere i mjere izvršavanja u odnosu na subjekt koji je predmet tog zahtjeva i koji pruža usluge ili koji ima mrežni i informacijski sustav na državnom području te države članice.

(136) Ovom bi se Direktivom trebala utvrditi pravila suradnje između nadležnih tijela i nadzornih tijela na temelju Uredbe (EU) 2016/679 radi postupanja u slučaju povreda ove Direktive povezanih s osobnim podacima.

(137) Cilj ove Direktive trebao bi biti osiguravanje visoke razine odgovornosti za mjere upravljanja kibersigurnosnim rizicima i obveze izvješćivanja na razini ključnih i važnih subjekata. Stoga bi upravljačka tijela ključnih i važnih subjekata trebala odobravati mjere upravljanja kibersigurnosnim rizicima i nadzirati njihovu provedbu.

(138) Kako bi se osigurala visoka zajednička razina kibersigurnosti širom Unije na temelju ove Direktive, Komisiji bi trebalo delegirati ovlast za donošenje akata u skladu s člankom 290. UFEU-a u vezi s dopunom ove Direktive određivanjem od kojih se kategorija ključnih i važnih subjekata treba zahtijevati korištenje određenim certificiranim IKT proizvodima, IKT uslugama i IKT procesima ili pribavljanje certifikata na temelju jednog od europskih programa kibersigurnosne certifikacije. Posebno je važno da Komisija tijekom svojeg pripremnog rada provede odgovarajuća savjetovanja, uključujući ona na razini stručnjaka, te da se ta savjetovanja provedu u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.[1]. Osobito, s ciljem osiguravanja ravnopravnog sudjelovanja u pripremi delegiranih akata, Europski parlament i Vijeće primaju sve dokumente istodobno kada i stručnjaci iz država članica te njihovi stručnjaci sustavno imaju pristup sastancima stručnih skupina Komisije koji se odnose na pripremu delegiranih akata.

[1] SL L 123, 12.5.2016., str. 1.

(139) Radi osiguranja jedinstvenih uvjeta za provedbu ove Direktive, Komisiji bi trebalo dodijeliti provedbene ovlasti za utvrđivanje postupovnih aranžmana potrebnih za funkcioniranje skupine za suradnju te tehničkih, metodoloških i sektorskih zahtjeva u pogledu mjera upravljanja kibersigurnosnim rizicima i za dodatno utvrđivanje vrste informacija, oblika i postupka obavješćivanja o incidentima, kiberprijetnjama i izbjegnutim incidentima te dodatno utvrđivanje komunikacije o ozbiljnim kiberprijetnjama kao i o slučajevima u kojima se incident treba smatrati značajnim. Te bi ovlasti trebalo izvršavati u skladu s Uredbom (EU) br. 182/2011 Europskog parlamenta i Vijeća[1].

[1] 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.).

(140) Komisija bi periodično trebala preispitivati ovu Direktivu, nakon savjetovanja s dionicima, naročito u cilju utvrđivanja je li potrebno predlagati amandmane u svjetlu promjene društvenih, političkih, tehnoloških i tržišnih uvjeta. U tim preispitivanjima Komisija bi trebala ocijeniti relevantnost veličine dotičnih subjekata, te sektora, podsektora i vrste subjekata iz prilogâ ovoj Direktivi za funkcioniranje gospodarstva i društva u pogledu kibersigurnosti. Komisija bi, između ostalog, trebala ocijeniti može li se pružatelje obuhvaćene područjem primjene ove Direktive koji su određeni kao vrlo velike internetske platforme u smislu članka 33. Uredbe (EU) 2022/2065 Europskog parlamenta i Vijeća[1] utvrditi kao ključna tijela na temelju ove Direktive.

[1] Uredba (EU) 2022/2065 Europskog parlamenta i Vijeća od 19. listopada 2022. o jedinstvenom tržištu digitalnih usluga i izmjeni Direktive 2000/31/EZ (Akt o digitalnim uslugama) (SL L 227, 27.10.2022., str. 1.).

(141) Ova Direktiva stvara nove zadaće za ENISA-u, čime se jača njezina uloga, a mogla bi također dovesti do toga da se od ENISA-e zahtijeva izvršavanje njezinih postojećih zadaća u skladu s Uredbom (EU) 2019/881 na višoj razini nego prije. Kako bi se osiguralo da ENISA raspolaže potrebnim financijskim i ljudskim resursima za obavljanje postojećih i novih zadaća kao i za ispunjavanje svih viših razina provedbe koje proizlaze iz njezine snažnije uloge, treba povećati njezin proračun. Osim toga, kako bi se osiguralo učinkovito korištenje resursima, ENISA-i treba dati veću fleksibilnost u načinu na koji ona može interno dodjeljivati resurse kako bi učinkovito izvršavala svoje zadaće i ispunila očekivanja.

(142) S obzirom na to da cilj ove Direktive, to jest postizanje visoke zajedničke razine kibersigurnosti širom Unije, 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.

(143) Ovom Direktivom poštuju se temeljna prava i načela priznata Poveljom, posebno pravo na poštovanje privatnog života i komuniciranja, zaštita osobnih podataka, sloboda poduzetništva, pravo na vlasništvo, pravo na djelotvoran pravni lijek i na pošteno suđenje, pretpostavka nedužnosti i prava na obranu. Pravo na djelotvoran pravni lijek obuhvaća i primatelje usluga koje pružaju ključni i važni subjekti. Ova Direktiva trebala bi se provoditi u skladu s tim pravima i načelima.

(144) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća[1] te je on dao mišljenje 11. ožujka 2021.[2],

DONIJELI SU OVU DIREKTIVU:

---

[1] Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39.).

[2] SL C 183, 11.5.2021., str. 3.

Poglavlje I.
Opće odredbe

Članak 1.

Predmet

1. Ovom se Direktivom utvrđuju mjere čiji je cilj postići visoku zajedničku razinu kibersigurnosti širom Unije kako bi se poboljšalo funkcioniranje unutarnjeg tržišta.

2. U tu svrhu, ovom se Direktivom utvrđuju:

   (a) obveze kojima se zahtjeva da države članice donesu nacionalne strategije za kibersigurnost i imenuju ili uspostave nadležna tijela, tijela za upravljanje kiberkrizama, jedinstvene kontaktne točke za kibersigurnost (jedinstvene kontaktne točke) i timove za odgovor na računalne sigurnosne incidente (CSIRT-ovi);

   (b) mjere upravljanja kibersigurnosnim rizicima i obveze izvješćivanja za subjekte koji pripadaju vrstama navedenim u Prilogu I. i u Prilogu II kao i za subjekte utvrđene kao kritični subjekti na temelju Direktive (EU) …/…[+];

   (c) pravila i obveze u pogledu razmjene informacija o kibersigurnosti;

   (d) obveze nadzora i izvršavanja za države članice.

[+] SL: molimo u tekst umetnuti broj direktive iz dokumenta PE-CONS 51/22 (2020/0365(COD)).

Članak 2.

Područje primjene

1. Ova se Direktiva primjenjuje na javne ili privatne subjekata koji pripadaju vrstama navedenim u Prilogu I. ili u Prilogu II. koji se smatraju srednjim poduzećima na temelju članka 2. Priloga Preporuci 2003/361/EZ, ili koji prelaze gornje granice za srednja poduzeća iz stavka 1. tog članka i pružaju svoje usluge ili obavljaju svoje djelatnosti unutar Unije.

   Članak 3. stavak 4. Priloga toj Preporuci ne primjenjuje se za potrebe ove Direktive.

2. Ova se Direktiva primjenjuje i na subjekte koji pripadaju vrstama navedenim u Prilogu I. ili u Prilogu II, neovisno o njihovoj veličini:

   (a) ako usluge pružaju:

      i. pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga;

      ii. pružatelji usluga povjerenja;

      iii. registri naziva vršnih domena i pružatelji usluga sustava naziva domena;

(b) ako je subjekt u nekoj državi članici jedini pružatelj usluge koja je ključna za održavanje ključnih društvenih ili gospodarskih djelatnosti;

(c) ako bi poremećaj u funkcioniranju usluge koju pruža subjekt mogao imati znatan učinak na javnu sigurnost, javnu zaštitu ili javno zdravlje;

(d) ako bi poremećaj u funkcioniranju usluge koju pruža subjekt mogao uzrokovati znatne sistemske rizike, posebno u sektorima u kojima bi takav poremećaj mogao imati prekogranični učinak;

(e) ako je subjekt ključan zbog svoje posebne važnosti na nacionalnoj ili regionalnoj razini za određeni sektor ili vrstu usluge ili za druge međuovisne sektore u državi članici;

(f) ako se radi o subjektu javne uprave:

i. na razini državne uprave kako ga definira država članica u skladu s nacionalnim pravom; ili

ii. na regionalnoj razini kako ga definira država članica u skladu s nacionalnim pravom koji nakon procjene utemeljene na riziku pruža usluge čiji bi poremećaj mogao imati znatan učinak na ključne društvene ili gospodarske djelatnosti.

3. Neovisno o njihovoj veličini, ova se Direktiva primjenjuje na subjekte utvrđene kao kritične subjekte na temelju Direktive (EU) …/…[+].

4. Neovisno o njihovoj veličini, ova se Direktiva primjenjuje na subjekte utvrđene kao kritične subjekte koji pružaju usluge registracije naziva domena.

5. Države članice mogu predvidjeti da se ova Direktiva primjenjuje na:

   (a) subjekte javne uprave na lokalnoj razini;

   (b) obrazovne ustanove, posebno ako provode ključne istraživačke aktivnosti.

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

7. Ova se Direktiva ne primjenjuje na subjekte javne uprave koji obavljaju svoje aktivnosti u području nacionalne sigurnosti, javne sigurnosti, obrane ili izvršavanja zakonodavstva, uključujući sprečavanje, istragu, otkrivanje i progon kaznenih djela.

[+] SL: molimo u tekst umetnuti broj direktive iz dokumenta PE-CONS 51/22 (2020/0365(COD)).

8. Države članice mogu izuzeti određene subjekte koji obavljaju aktivnosti u području nacionalne sigurnosti, javne sigurnosti, obrane ili izvršavanja zakonodavstva, uključujući sprečavanje, istragu, otkrivanje i progon kaznenih djela, ili koji pružaju usluge isključivo subjektima javne uprave iz stavka 7. ovog članka od obveza iz članka 21 ili članka 23. u pogledu tih aktivnosti ili usluga. U takvim se slučajevima nadzorne mjere i mjere izvršavanja iz poglavlja VII. ne primjenjuju na te posebne aktivnosti ili usluge.
Ako subjekti obavljaju aktivnosti ili pružaju usluge isključivo one vrste koja je navedena u ovom stavku, države članice mogu i odlučiti izuzeti te subjekte od obveza utvrđenih u člancima 3. i 27.

9. Stavci 7. i 8. ne primjenjuju se ako subjekt djeluje kao pružatelj usluga povjerenja.

10. Ova se Direktiva ne primjenjuje na subjekte koje su države članice izuzele iz područja primjene Uredbe (EU) …/…[+] u skladu s člankom 2. stavkom 4. te Uredbe.

11. Obveze utvrđene u ovoj Direktivi ne podrazumijevaju dostavu informacija čije bi otkrivanje bilo u suprotnosti s osnovnim interesima u pogledu nacionalne sigurnosti, javne sigurnosti ili obrane država članica.

[+] SL: u tekst umetnuti broj Uredbe iz dokumenta PE-CONS 41/22 (2020/0266(COD)).

12. Ova se Direktiva primjenjuje ne dovodeći u pitanje Uredbu (EU) 2016/679, Direktivu 2002/58/EZ, direktive 2011/93/EU[1] i 2013/40/EU[2] Europskog parlamenta i Vijeća te Direktivu …/…[+].

13. Ne dovodeći u pitanje članak 346. UFEU-a, informacije koje se smatraju povjerljivima u skladu s pravilima Unije ili nacionalnim pravilima, 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 predmetnih subjekata.

14. Subjekti, nadležna tijela, jedinstvene kontaktne točke i CSIRT-ovi obrađuju osobne podatke u mjeri u kojoj je to potrebno za svrhe ove Direktive i u skladu s Uredbom (EU) 2016/679, a takva obrada posebno se oslanja na njezin članak 6.

---

[1] 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.).

[2] 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.).

[+] SL: molimo u tekst umetnuti broj Direktive iz dokumenta PE-CONS 51/22 (2020/0365(COD)).

Obradu osobnih podataka na temelju ove Direktive provode pružatelji javnih elektroničkih komunikacijskih mreža ili pružatelji javno dostupnih elektroničkih komunikacijskih usluga u skladu s pravom Unije o zaštiti podataka i pravom Unije o zaštiti privatnosti, a posebno s Direktivom 2002/58/EZ.

Članak 3.

Ključni i važni subjekti

1. Za potrebe ove Direktive sljedeći subjekti smatraju se ključnim subjektima:

(a) subjekti koji pripadaju vrstama iz Priloga I. koji premašuju gornje granice za srednja poduzeća iz članka 2. stavka 1. Priloga Preporuci 2003/361/EZ;

(b) kvalificirani pružatelji usluga povjerenja i registri naziva vršnih domena te pružatelji usluga DNS-a, neovisno o njihovoj veličini;

(c) pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga koji se smatraju srednjim poduzećima na temelju članka 2. Priloga Preporuci 2003/361/EZ;

(d) subjekti javne uprave iz članka 2. stavka 2. točke (f) podtočke (i);

(e) svi drugi subjekti koji pripadaju vrstama iz priloga I. ili II. koje je država članica utvrdila kao ključne subjekte na temelju članka 2. stavka 2. točaka od (b) do (e);

(f) subjekti koji su utvrđeni kao kritični subjekti na temelju Direktive (EU) …/…[+], iz članka 2. stavka 3. ove Direktive;

(g) ako država članica tako odredi, subjekti koje je ta država članica utvrdila prije… [datum stupanja na snagu ove Direktive] kao operatore ključnih usluga u skladu s Direktivom (EU) 2016/1148 ili nacionalnim pravom.

2. Za potrebe ove Direktive, svi subjekti koji pripadaju vrstama iz priloga I. ili II. koji se ne smatraju ključnim subjektima na temelju stavka 1. ovog članka smatraju se važnim subjektima. To uključuje subjekte koje je država članica utvrdila kao važne subjekte na temelju članka 2. stavka 2. točaka od (b) do (e).

3. Do … [27 mjeseci od datuma stupanja na snagu ove Direktive] države članice utvrđuju popis ključnih i važnih subjekata te subjekata koji pružaju usluge registracije naziva domena. Države članice redovito, a najmanje svake dvije godine, preispituju taj popis te ga prema potrebi ažuriraju.

[+] SL: molimo u tekst umetnuti broj Direktive iz dokumenta PE-CONS 51/22 (2020/0365(COD)).

4. Za potrebe utvrđivanja popisa iz stavka 3. države članice zahtijevaju od subjekata iz tog stavka da nadležnim tijelima dostave barem sljedeće informacije:

(a) naziv subjekta;

(b) adresu i ažurirane podatke za kontakt, uključujući e-adrese, IP raspone i telefonske brojeve;

(c) ako je to primjenjivo, relevantni sektor i podsektor iz priloga I. ili II.; i

(d) ako je to primjenjivo, popis država članica u kojima pružaju usluge obuhvaćene područjem primjene ove Direktive.

Subjekti iz stavka 3. bez odgode, a u svakom slučaju u roku od dva tjedna od datuma promjene, obavješćuju o svim promjenama podataka koje su dostavili u skladu s prvim podstavkom ovog stavka.

Komisija uz pomoć Agencije Europske unije za kibersigurnost (ENISA) bez nepotrebne odgode pruža smjernice i predloške u vezi s obvezama utvrđenim u ovom stavku.

Države članice mogu uspostaviti nacionalne mehanizme za registraciju subjekata.

5. Do … [27 mjeseci od datuma stupanja na snagu ove Direktive] i svake dvije godine nakon toga nadležna tijela obavješćuju:

(a) Komisiju i skupinu za suradnju o broju svih ključnih i važnih subjekata navedenih u skladu sa stavkom 3. za svaki sektor i podsektor iz priloga I. ili II.; i

(b) Komisiju o relevantnim informacijama o broju ključnih i važnih subjekata utvrđenih na temelju članka 2. stavka 2. točaka od (b) do (e), sektoru i podsektoru iz priloga I. ili II. kojima pripadaju, vrsti usluge koju pružaju i odredbama iz članka 2. stavka 2. točaka od (b) do (e), na temelju kojih su utvrđeni.

6. Do … [27 mjeseci od datuma stupanja na snagu ove Direktive] i na zahtjev Komisije države članice mogu obavijestiti Komisiju o nazivima ključnih i važnih subjekata iz stavka 5. točke (b).

Članak 4.

Sektorski pravni akti Unije

1. Ako se sektorskim pravnim aktima Unije od ključnih ili važnih subjekata zahtijeva donošenje mjera upravljanja kibersigurnosnim rizicima ili obavješćivanje o značajnim incidentima i ako su ti zahtjevi po učinku barem jednakovrijedni obvezama utvrđenima u ovoj Direktivi, relevantne odredbe ove Direktive, uključujući odredbe o nadzoru i izvršavanju iz poglavlja VII., 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 pravnim aktima Unije.

2. Zahtjevi iz stavka 1. ovog članka smatraju se po učinku jednakovrijednim obvezama utvrđenima u ovoj Direktivi ako:

   (a) mjere upravljanja kibersigurnosnim rizicima po učinku su barem jednakovrijedne mjerama utvrđenima u članku 21. stavcima 1. i 2.; ili

   (b) sektorskim pravnim aktom Unije predviđa se neposredan, prema potrebi automatski i izravan, pristup obavijestima o incidentima od strane CSIRT-ova, nadležnih tijela ili jedinstvenih kontaktnih točaka na temelju ove Direktive te kada su zahtjevi za obavješćivanje o značajnim incidentima po učinku barem jednakovrijedni onima utvrđenima u članku 23. stavcima od 1. do 6. ove Direktive.

3. Komisija do … [šest mjeseci od stupanja na snagu ove Direktive] pruža smjernice kojima se pojašnjava primjena stavaka 1. i 2. Komisija redovito preispituje te smjernice. Kod pripreme tih smjernica Komisija uzima u obzir primjedbe skupine za suradnju i ENISA-e.

Članak 5.

Minimalno usklađivanje

Ovom Direktivom ne sprečava se države članice da donesu ili zadrže odredbe kojima se osigurava viša razina kibersigurnosti, pod uvjetom da su te odredbe u skladu s obvezama država članica utvrđenih pravom Unije.

Članak 6.

Definicije

Za potrebe ove Direktive primjenjuju se sljedeće definicije:

1. „mrežni i informacijski sustav” znači:

   (a) elektronička komunikacijska mreža kako je definirana u članku 2. točki 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; ili

(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, prenesenih ili obrađenih podataka ili usluga koje ti mrežni i informacijski sustavi nude ili kojima omogućuju pristup;

3. „kibersigurnost” znači kibersigurnost kako je definirana u članku 2. točki 1. Uredbe (EU) 2019/881;

4. „nacionalna strategija za kibersigurnost” znači koherentan okvir države članice kojim se predviđaju strateški ciljevi i prioriteti u području kibersigurnosti i upravljanje za njihovo postizanje u toj državi članici;

5. „izbjegnuti incident” znači svaki događaj koji je mogao ugroziti dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koje mrežni i informacijski sustavi nude ili kojima omogućuju pristup, ali je uspješno spriječen ili se nije ostvario;

6. „incident” znači 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;

7. „kibersigurnosni incident velikih razmjera” znači incident koji uzrokuje razinu poremećaja koja premašuje sposobnost države članice da na njega odgovori ili koji ima znatan učinak na najmanje dvije države članice;

8. „postupanje s incidentom” znači sve radnje i postupci čiji je cilj sprečavanje, otkrivanje, analiza, zaustavljanje incidenta ili odgovor na njega te oporavak od incidenta;

9. „rizik” znači mogućnost gubitka ili poremećaja uzrokovana incidentom i treba ga izražavati kao kombinaciju opsega takvog gubitka ili poremećaja i vjerojatnosti pojave tog incidenta;

10. „kiberprijetnja” znači kiberprijetnja kako je definirana u članku 2. točki 8. Uredbe (EU) 2019/881;

11. „ozbiljna kiberprijetnja” znači kiberprijetnja za koju se na temelju njezinih tehničkih obilježja može pretpostaviti da može imati ozbiljan učinak na mrežne i informacijske sustave nekog subjekta ili korisnike usluga subjekta uzrokovanjem znatne materijalne ili nematerijalne štete;

12. „IKT proizvod” znači IKT proizvod kako je definiran u članku 2. točki 12. Uredbe (EU) 2019/881;

13. „IKT usluga” znači IKT usluga kako je definirana u članku 2. točki 13. Uredbe (EU) 2019/881;

14. „IKT proces” znači IKT proces kako je definiran u članku 2. točki 14. Uredbe (EU) 2019/881;

15. „ranjivost” znači slabost, osjetljivost ili nedostatak IKT proizvoda ili IKT usluga koje kiberprijetnja može iskoristiti;

16. „norma” znači norma kako je definirana u članku 2. točki 1. Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća[1];

17. „tehnička specifikacija” znači tehnička specifikacija kako je definirana u članku 2. točki 4. Uredbe (EU) br. 1025/2012;

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

---

[1] 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.).

19. „sustav naziva domena” ili „(DNS)” znači hijerarhijsko raspoređeni sustav imenovanja koji omogućuje utvrđivanje internetskih usluga i resursa, čime se krajnjim korisnicima uređaja omogućuje da korištenje internetskim uslugama usmjeravanja i povezivosti za pristupanje tim uslugama i resursima;

20. „pružatelj usluga DNS-a” znači subjekt koji pruža:

    (a) javno dostupne rekurzivne usluge razlučivanja naziva domena krajnjim korisnicima interneta; ili

    (b) mjerodavne usluge razlučivanja naziva domena za upotrebu trećih strana, uz iznimku korijenskih poslužitelja naziva;

21. „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, uključujući upravljanje njezinim poslužiteljima naziva, održavanje njezinih baza podataka i distribuciju datoteka iz zone vršne domene u poslužitelje naziva, neovisno o tome obavlja li sam subjekt bilo koju od tih operacija ili njihovo obavljanje eksternalizira, ali su isključene situacije u kojima registar koristi nazive vršnih domena samo za vlastitu upotrebu;

22. „subjekt koji pruža usluge registracije naziva domena” znači registrar ili zastupnik koji djeluje u ime registrara, kao što je pružatelj ili preprodavatelj usluga zaštite privatnosti i proxy registracije;

23. „digitalna usluga” znači usluga kako je definirana u članku 1. stavku 1. točki (b) Direktive (EU) 2015/1535 Europskog parlamenta i Vijeća[1];

24. „usluga povjerenja” znači usluga povjerenja kako je definirana u članku 3. točki 16. Uredbe (EU) br. 910/2014;

25. „pružatelj usluga povjerenja” znači pružatelj usluga povjerenja kako je definiran u članku 3. točki 19. Uredbe (EU) br. 910/2014;

26. „kvalificirana usluga povjerenja” znači kvalificirana usluga povjerenja kako je definirana u članku 3. točki 17. Uredbe (EU) br. 910/2014;

27. „kvalificirani pružatelj usluga povjerenja” znači kvalificirani pružatelj usluga povjerenja kako je definiran u članku 3. točki 20. Uredbe (EU) br. 910/2014;

28. „internetsko tržište” znači internetsko tržište kako je definirano u članku 2. točki (n) Direktive 2005/29/EZ Europskog parlamenta i Vijeća[2];

---

[1] 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.).

[2] 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.).

29. „internetska tražilica” znači internetska tražilica kako je definirana u članku 2. točki 5. Uredbe (EU) 2019/1150 Europskog parlamenta i Vijeća[1];

30. „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 su takvi resursi raspoređeni na nekoliko lokacija;

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

32. „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;

33. „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, posebno preko razgovora, objava, videozapisa i preporuka;

---

[1] 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.).

34. „predstavnik” znači fizička ili pravna osoba koja ima poslovni nastan u Uniji koju su pružatelj usluga DNS-a, registar naziva vršnih domena, subjekt koji pruža usluge registracije naziva domena, pružatelj usluga računalstva u oblaku, pružatelj usluga podatkovnog centra, pružatelj mreža za isporuku sadržaja, pružatelj upravljanih usluga, pružatelj upravljanih sigurnosnih usluga, ili pružatelj internetskog tržišta, pružatelj internetske tražilice ili pružatelj platforme za usluge društvenih mreža koji nema poslovni nastan u Uniji izričito imenovali da djeluje u njihovo ime i kojoj se nadležno tijelo ili CSIRT mogu obratiti umjesto samom subjektu u pogledu obveza tog subjekta na temelju ove Direktive;

35. „subjekt javne uprave” znači subjekt koji je kao takav priznat u državi članici u skladu s nacionalnim pravom, ne uključujući sudstvo, parlamente ili središnje banke 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.

36. „javna elektronička komunikacijska mreža” znači javna elektronička komunikacijska mreža kako je definirana u članku 2. točki (8) Direktive (EU) 2018/1972;

37. „elektronička komunikacijska usluga” znači elektronička komunikacijska usluga kako je definirana u članku 2. točki (4) Direktive (EU) 2018/1972;

38. „subjekt” znači 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;

39. „pružatelj upravljanih usluga” znači subjekt koji pruža usluge povezane s instalacijom, upravljanjem, radom ili održavanjem IKT proizvoda, mreža, infrastrukture, aplikacija ili bilo kojih drugih mrežnih i informacijskih sustava, u obliku pomoći ili aktivnog upravljanja koje se provodi u prostorima klijenata ili na daljinu;

40. „pružatelj upravljanih sigurnosnih usluga” znači pružatelj upravljanih usluga koji provodi ili pruža pomoć za aktivnosti povezane s upravljanjem kibersigurnosnim rizicima;

41. „istraživačka organizacija” znači subjekt čiji je primarni cilj provođenje primijenjenog istraživanja ili eksperimentalnog razvoja radi iskorištavanja rezultata tog istraživanja u komercijalne svrhe, ali koji ne uključuje obrazovne ustanove.

Poglavlje II.
Koordinirani okviri za kibersigurnost

Članak 7.

Nacionalna strategija za kibersigurnost

1. Svaka država članica donosi nacionalnu strategiju za kibersigurnost u kojoj se utvrđuju strateški ciljevi, resursi potrebni za postizanje tih ciljeva i odgovarajuće mjere politike i regulatorne mjere radi postizanja i održavanja visoke razine kibersigurnosti.
Nacionalna strategija za kibersigurnost uključuje:

   (a) ciljeve i prioritete strategije za kibersigurnost države članice koji posebno obuhvaćaju sektore i podsektore iz priloga I. i II.;

   (b) upravljački okvir za postizanje ciljeva i prioriteta iz točke (a) ovog stavka, uključujući politike iz stavka 2. ;

   (c) upravljački okvir kojim se pojašnjavaju uloge i odgovornosti relevantnih dionika na nacionalnoj razini, kojim se podupire suradnja i koordinacija na nacionalnoj razini među nadležnim tijelima, jedinstvenim kontaktnim točkama i CSIRT-ovima na temelju ove Direktive, kao i koordinacija i suradnja između tih tijela i nadležnih tijela na temelju sektorskih pravnih akata Unije;

(d) mehanizam za utvrđivanje relevantne imovine i procjenu rizika u toj državi članici;

(e) određivanje mjera za osiguravanje pripravnosti i sposobnosti reagiranja na incidente i oporavka od incidenata, uključujući suradnju javnog i privatnog sektora;

(f) popis različitih tijela i dionika koji su uključeni u provedbu nacionalne strategije za kibersigurnost;

(g) okvir politike za bolju koordinaciju između nadležnih tijela na temelju ove Direktive i nadležnih tijela na temelju Direktive (EU) …/…[+] u svrhu razmjene informacija o rizicima, kiberprijetnjama i incidentima te o rizicima, prijetnjama i incidentima izvan kiberprostora i izvršavanja nadzornih zadaća, prema potrebi;

(h) plan, uključujući potrebne mjere, za povećanje opće razine osviještenosti o kibersigurnosti među građanima.

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

(a) za rješavanje kibersigurnosnih pitanja u lancu opskrbe za IKT proizvode i IKT usluge kojima se koriste subjekti za pružanje svojih usluga;

[+] SL: molimo u tekst umetnuti broj Direktive iz dokumenta PE-CONS 51/22 (2020/0365(COD)).

(b) za uključivanje i definiranje kibersigurnosnih zahtjeva za IKT proizvode i IKT usluge u području javne nabave, uključujući u odnosu na kibersigurnosnu certifikaciju, kriptiranje i upotrebu kibersigurnosnih proizvoda otvorenog koda;

(c) za upravljanje ranjivostima, uključujući promicanje i olakšavanje koordiniranog otkrivanja ranjivosti u skladu s člankom 12. stavkom 1.;

(d) koje se odnose na održavanje opće dostupnosti, cjelovitosti i povjerljivosti javne jezgre otvorenog interneta, uključujući, ako je to potrebno, kibersigurnost podmorskih komunikacijskih kabela;

(e) za promicanje razvoja i integracije relevantnih naprednih tehnologija radi provedbe najsuvremenijih mjera upravljanja kibersigurnosnim rizicima;

(f) za promicanje i razvoj obrazovanja i osposobljavanja u području kibersigurnosti, vještina u području kibersigurnosti, informiranja te istraživačkih i razvojnih inicijativa u području kibersigurnosti, kao i smjernica o dobroj praksi i kontrolama kiberhigijene namijenjenih građanima, dionicima i subjektima;

(g) za potporu akademskim i istraživačkim institucijama u razvoju, unapređivanju i poticanju uvođenja alata za kibersigurnost i sigurne mrežne infrastrukture;

(h) koje uključuju relevantne postupke i odgovarajuće alate za razmjenu informacija u cilju podupiranja dobrovoljne razmjene informacija o kibersigurnosti među subjektima u skladu s pravom Unije;

(i) za jačanje kiberotpornosti i osnovne razine kiberhigijene malih i srednjih poduzeća, osobito onih koji su izuzeti iz područja primjene ove Direktive, pružanjem lako dostupnih smjernica i pomoći za njihove specifične potrebe;

(j) za promicanje aktivne kiberzaštite.

3. Države članice obavješćuju Komisiju o svojim nacionalnim strategijama za kibersigurnost u roku od tri mjeseca od njihova donošenja. Države članice mogu iz takvih obavijesti izostaviti informacije koje se odnose na njihovu 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 ažuriraju. ENISA pomaže državama članicama, na njihov zahtjev u razvoju ili ažuriranju nacionalne strategije za kibersigurnost i ključnih pokazatelja uspješnosti za ocjenjivanje te strategije kako bi je uskladila sa zahtjevima i obvezama utvrđenim u ovoj Direktivi.

Članak 8.

Nadležna tijela i jedinstvene kontaktne točke

1. Svaka država članica imenuje ili uspostavlja jedno ili više nadležnih tijela odgovornih za kibersigurnost i za nadzorne zadaće iz poglavlja VII. (nadležna tijela).

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

3. Svaka država članica imenuje ili uspostavlja jedinstvenu kontaktnu točku. Ako država članica imenuje ili uspostavi samo jedno nadležno tijelo u skladu sa stavkom 1., 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, i prema potrebi s Komisijom i ENISA-om, te međusektorsku suradnju s drugim nadležnim tijelima u svojoj državi članici.

5. Države članice osiguravaju da njihova nadležna tijela i jedinstvene kontaktne točke imaju odgovarajuće resurse za učinkovitu i efikasnu provedbu zadaća koje su im dodijeljene te da time ispune ciljeve ove Direktive.

6. Svaka država članica bez nepotrebne odgode obavješćuje Komisiju o identitetu nadležnog tijela iz stavka 1. i jedinstvene kontaktne točke iz stavka 3., o zadaćama tih tijela i o svim naknadnim promjenama. Svaka država članica objavljuje identitet svojeg nadležnog tijela. Komisija javno objavljuje popis jedinstvenih kontaktnih točaka.

Članak 9.

Nacionalni okviri za upravljanje kiberkrizama

1. Svaka država članica imenuje ili uspostavlja jedno ili više nadležnih tijela odgovornih za upravljanje kibersigurnosnim incidentima velikih razmjera i krizama (tijela za upravljanje kiberkrizama). Države članice osiguravaju da ta tijela imaju odgovarajuće resurse za učinkovito i efikasno obavljanje zadaća koje su im dodijeljene. Države članice osiguravaju koherentnost s postojećim nacionalnim okvirima za opće upravljanje krizama.

2. Ako pojedina država članica imenuje ili uspostavi više od jednog tijela za upravljanje kiberkrizama u skladu sa stavkom 1., jasno navodi koje od tih tijela treba služiti kao koordinator za upravljanje kibersigurnosnim incidentima velikih razmjera i krizama.

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

4. Svaka država članica donosi nacionalni plan za odgovor na kibersigurnosne incidente velikih razmjera i krize u kojem se utvrđuju ciljevi i načini upravljanja kibersigurnosnim incidentima velikih razmjera i krizama. U tom planu se konkretno utvrđuju:

   (a) ciljevi mjera i aktivnosti za nacionalnu pripravnost;

(b) zadaće i odgovornosti tijela za upravljanje kiberkrizama;

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

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

(e) relevantni javni i privatni dionici i uključena infrastruktura;

(f) nacionalni postupci i dogovori između relevantnih nacionalnih tijela i drugih tijela kako bi se osiguralo učinkovito sudjelovanje država članica u koordiniranom upravljanju kibersigurnosnim incidentima velikih razmjera i krizama na razini Unije i njihova potpora takvom upravljanju.

5. U roku od tri mjeseca od imenovanja ili uspostave tijela za upravljanje kiberkrizama iz stavka 1. svaka država članica obavješćuje Komisiju o identitetu svojeg tijela i o svim naknadnim promjenama. Države članice dostavljaju Komisiji i Europskoj mreži organizacija za vezu za kiberkrize (mreža EU-CyCLONe) relevantne informacije u vezi sa zahtjevima iz stavka 4. o svojim nacionalnim planovima za odgovor na kibersigurnosne incidente velikih razmjera i krize u roku od tri mjeseca od donošenja tih planova. Države članice mogu izostaviti određene informacije ako je to potrebno i u mjeri u kojoj je takvo izostavljanje potrebno za nacionalnu sigurnost.

Članak 10.

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

1. Svaka država članica imenuje ili uspostavlja jedan ili više CSIRT-ova. CSIRT-ovi se mogu imenovati ili uspostaviti u okviru nadležnog tijela. CSIRT-ovi ispunjavaju zahtjeve utvrđene u članku 11. stavku 1. i obuhvaćaju barem sektore, podsektore ili vrste subjekata iz priloga I. i II. te su odgovorni za postupanje s incidentima u skladu s točno propisanim postupkom.

2. Države članice osiguravaju da svaki CSIRT ima odgovarajuće resurse za učinkovito izvršavanje zadaća utvrđenih u članku 11. stavku 3.

3. Države članice osiguravaju da svaki CSIRT raspolaže odgovarajućom, sigurnom i otpornom komunikacijskom i informacijskom infrastrukturom za razmjenu informacija s ključnim i važnim subjektima te drugim relevantnim dionicima. Države članice u tu svrhu osiguravaju da svaki CSIRT doprinosi uvođenju sigurnih alata za razmjenu informacija.

4. CSIRT-ovi surađuju i, prema potrebi, razmjenjuju relevantne informacije u skladu s člankom 29. sa sektorskim ili međusektorskim zajednicama ključnih i važnih subjekata.

5. CSIRT-ovi sudjeluju u istorazinskim ocjenjivanjima organiziranima u skladu s člankom 19.

6. Države članice osiguravaju učinkovitu, efikasnu i sigurnu suradnju svojih CSIRT-ova u mreži CSIRT-ova.

7. CSIRT-ovi mogu uspostaviti odnose suradnje s nacionalnim timovima za odgovor na računalne sigurnosne incidente iz trećih zemalja. Kao dio takvih odnosa suradnje, države članice olakšavaju učinkovitu, efikasnu i sigurnu razmjenu informacija s tim nacionalnim timovima za odgovor na računalne sigurnosne incidente iz trećih zemalja koristeći se odgovarajućim protokolima za razmjenu informacija, uključujući Protokol o semaforu. CSIRT-ovi mogu razmjenjivati relevantne informacije s nacionalnim timovima za odgovor na računalne sigurnosne incidente iz trećih zemalja, uključujući osobne podatke u skladu s pravom Unije o zaštiti podataka.

8. CSIRT-ovi mogu surađivati s nacionalnim timovima za odgovor na računalne sigurnosne incidente iz trećih zemalja ili istovjetnim tijelima iz trećih zemalja, posebno kako bi im se pružila pomoć u području kibersigurnosti.

9. Svaka država članica bez nepotrebne odgode obavješćuje Komisiju o identitetu CSIRT-a iz stavka 1. ovog članka i CSIRT-a koji je imenovan koordinatorom u skladu s člankom 12. stavkom 1., o zadaćama u odnosu na ključne i važne subjekte i o svim naknadnim promjenama.

10. Države članice mogu zatražiti podršku ENISA-e u razvijanju svojih CSIRT-ova.

Članak 11.

Zahtjevi, tehničke sposobnosti *u pogledu CSIRT-ova i njihove zadaće*

1. CSIRT-ovi moraju ispunjavati 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; oni 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 usmjeravanjem, posebno kako bi se olakšale učinkovite i efikasne primopredaje;

   (d) CSIRT-ovi osiguravaju povjerljivost i pouzdanost svojih operacija;

   (e) CSIRT-ovi imaju dovoljno osoblja kako bi se osigurala dostupnost njihovih usluga u svako doba i osiguravaju da je njihovo osoblje osposobljeno na odgovarajući način;

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

   CSIRT-ovi mogu sudjelovati u međunarodnim mrežama za suradnju.

2. Države članice osiguravaju da njihovi CSIRT-ovi zajedno imaju tehničke sposobnosti potrebne za izvršavanje zadaća iz stavka 3. Države članice osiguravaju da se njihovim CSIRT-ovima dodijele dostatni resursi za osiguravanje dovoljno osoblja kako bi se CSIRT-ovima omogućilo da razviju svoje tehničke sposobnosti.

3. CSIRT-ovi obavljaju sljedeće zadaće:

(a) praćenje i analiziranje kiberprijetnji, ranjivosti i incidenata na nacionalnoj razini i, na zahtjev, pružanje pomoći predmetnim ključnim i važnim subjektima u vezi s praćenjem njihovih mrežnih i informacijskih sustava u stvarnom ili gotovo stvarnom vremenu;

(b) pružanje ranih upozorenja i najava te informiranje predmetnih ključnih i važnih subjekata, kao i nadležnih tijela i drugih relevantnih dionika o kiberprijetnjama, ranjivostima i incidentima, ako je moguće u gotovo stvarnom vremenu;

(c) odgovaranje na incidente i, ako je to primjenjivo, pružanje pomoći predmetnim ključnim i važnim subjektima;

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

(e) osiguravanje, na zahtjev predmetnog ključnog ili važnog subjekta, proaktivnog skeniranja mrežnih i informacijskih sustava predmetnog subjekta radi otkrivanja ranjivosti s potencijalno znatnim učinkom;

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

(g) ako je to primjenjivo, djelovanje u svojstvu koordinatora za potrebe postupka koordiniranog otkrivanja ranjivosti iz članka 12. stavka 1.;

(h) doprinošenje korištenju alata za sigurnu razmjenu informacija na temelju članka 10. stavka 3.

CSIRT-ovi mogu provoditi proaktivno neintruzivno skeniranje javno dostupnih mrežnih i informacijskih sustava ključnih i važnih subjekata. Takvo skeniranje provodi se kako bi se otkrili ranjivi ili nesigurno konfigurirani mrežni i informacijski sustavi te kako bi se obavijestili dotični subjekti. Takvo skeniranje ne smije imati negativan učinak na funkcioniranje usluga subjekata.

Pri obavljanju zadaća iz prvog podstavka CSIRT-ovi mogu dati prednost određenim zadaćama na temelju pristupa utemeljenog na procjeni rizika.

4. CSIRT-ovi uspostavljaju odnose suradnje s relevantnim dionicima u privatnom sektoru radi ostvarenja ciljeva ove Direktive.

5. Kako bi olakšali suradnju iz stavka 4., CSIRT-ovi promiču donošenje i primjenu zajedničkih ili standardiziranih praksi, planova za klasifikaciju i taksonomija u odnosu na:

(a) postupke za postupanje s incidentima;

(b) upravljanje krizama; i

(c) koordinirano otkrivanje ranjivosti na temelju članka 12. stavka 1.

Članak 12.

Koordinirano otkrivanje ranjivosti i europska baza podataka o *ranjivosti*

1. Svaka država članica imenuje jednog od svojih CSIRT-ova koordinatorom za potrebe koordiniranog otkrivanja ranjivosti. CSIRT koji je imenovan koordinatorom djeluje kao pouzdani posrednik koji, prema potrebi, olakšava interakciju između fizičke ili pravne osobe koja prijavljuje ranjivost i proizvođača ili pružatelja potencijalno ranjivih IKT proizvoda ili IKT usluga, na zahtjev bilo koje strane. Zadaće CSIRT-a koji je imenovan koordinatorom uključuju:

(a) utvrđivanje predmetnih subjekata i kontaktiranje s njima;

(b) pomaganje fizičkim ili pravnim osobama koje prijavljuju ranjivost; i

(c) pregovaranje o vremenskom okviru za otkrivanje i upravljanje ranjivostima koje utječu na više subjekata.

Države članice osiguravaju da fizičke ili pravne osobe, kad to zatraže, mogu anonimno prijaviti ranjivost CSIRT-u koji je imenovan koordinatorom. CSIRT koji je imenovan koordinatorom osigurava provedbu pažljivih daljnjih mjera u pogledu prijavljene ranjivosti i osigurava anonimnost fizičke ili pravne osobe koja prijavljuje ranjivost. Ako bi prijavljena ranjivost mogla imati znatan učinak na subjekte u više od jedne države članice, CSIRT koji je imenovan koordinatorom svake dotične države članice, prema potrebi, surađuje s drugim CSIRT-ovima koji su imenovani koordinatorima u okviru mreže CSIRT-ova.

2. ENISA nakon savjetovanja sa skupinom za suradnju razvija i vodi europsku bazu podataka o ranjivosti. U tu svrhu ENISA uspostavlja i održava odgovarajuće informacijske sustave, politike i postupke te usvaja potrebne tehničke i organizacijske mjere za osiguravanje sigurnosti i cjelovitosti europske baze podataka o ranjivosti, osobito kako bi omogućila subjektima, neovisno jesu li obuhvaćeni područjem primjene ove Direktive, kao i njihovim dobavljačima mrežnih i informacijskih sustava, da, na dobrovoljnoj osnovi, otkriju i registriraju javno poznate ranjivosti u IKT proizvodima ili IKT uslugama. Svim dionicima omogućuje se pristup informacijama o ranjivostima sadržanima u europskoj bazi podataka o ranjivosti. Ta baza podataka uključuje:

(a) informacije koje opisuju ranjivost;

(b) IKT proizvode ili IKT usluge na koje ona utječe i ozbiljnost ranjivosti s obzirom na okolnosti u kojima se može iskoristiti;

(c) dostupnost odgovarajućih popravaka i ako nisu dostupni popravci, smjernice koje pružaju nadležna tijela ili CSIRT-ovi namijenjene korisnicima ranjivih IKT proizvoda i IKT usluga o načinu na koji se mogu ublažiti rizici koji proizlaze iz otkrivenih ranjivosti.

Članak 13.

Suradnja na nacionalnoj razini

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

2. Države članice osiguravaju da njihovi CSIRT-ovi ili, ako je to primjenjivo, njihova nadležna tijela, primaju obavijesti o značajnim incidentima u skladu s člankom 23. i incidentima, kiberprijetnjama i izbjegnutim incidentima u skladu s člankom 30.

3. Države članice osiguravaju da njihovi CSIRT-ovi ili, ako je to primjenjivo, njihova nadležna tijela obavješćuju njezinu jedinstvenu kontaktnu točku o obavijestima o incidentima, kiberprijetnjama i izbjegnutim incidentima koje su im dostavljene skladu s ovom Direktivom.

4. Kako bi se osiguralo učinkovito obavljanje zadaća i obveza nadležnih tijela, jedinstvenih kontaktnih točaka i CSIRT-ova, države članice, u mjeri u kojoj je to moguće, osiguravaju odgovarajuću suradnju između tih tijela i tijela za izvršavanje zakonodavstva, tijela za zaštitu podataka, nacionalnih tijela na temelju uredaba (EZ) br. 300/2008 i (EU) 2018/1139, nadzornih tijela na temelju Uredbe (EU) br. 910/2014, nadležnih tijela na temelju Uredbe (EU) …/…[+], nacionalnih regulatornih tijela na temelju Direktive (EU) 2018/1972, nadležnih tijela na temelju Direktive (EU) …/…[++], kao i nadležnih tijela na temelju drugih sektorskih pravnih akta Unije, unutar te države članice.

[+] SL: molimo u tekst umetnuti broj Uredbe iz dokumenta PE-CONS 41/22 (2020/0266(COD)).

[++] SL: molimo u tekst umetnuti broj Direktive iz dokumenta PE-CONS 51/22 (2020/0365(COD)).

5. Države članice osiguravaju da njihova nadležna tijela na temelju ove Direktive i njihova nadležna tijela na temelju Direktive (EU) …/…[+] redovito surađuju i razmjenjuju informacije u pogledu utvrđivanja kritičnih subjekata, o rizicima, kiberprijetnjama i incidentima, kao i o rizicima, prijetnjama i incidentima izvan kiberprostora koji utječu na ključne subjekte koji su utvrđeni kao kritični subjekti na temelju Direktive (EU) …/…[+], kao i o poduzetim mjerama kao odgovor na takve rizike, prijetnje i incidente. Države članice osiguravaju i da njihova nadležna tijela u skladu s ovom Direktivom i njihova nadležna tijela na temelju Uredbe (EU) br. 910/2014, Uredbe (EU) …/…[++] i Direktive (EU) 2018/1972 redovito razmjenjuju relevantne informacije, među ostalim o bitnim incidentima i kiberprijetnjama.

6. Države članice pojednostavnjuju izvješćivanje tehničkim sredstvima za obavijesti iz članaka 23. i 30.

[+] SL: molimo u tekst umetnuti broj Direktive iz dokumenta PE-CONS 51/22 (2020/0365(COD)).

[++] SL: molimo u tekst umetnuti broj Uredbe iz dokumenta PE-CONS 41/22 (2020/0266(COD)).

Poglavlje III.
Suradnja na razini Unije i međunarodnoj razini

Članak 14.

Skupina za suradnju

1. Kako bi se podupirala i olakšavala strateška suradnja i razmjena informacija među državama članicama te jačalo povjerenje, osniva se skupina za suradnju.

2. Skupina za suradnju izvršava svoje zadaće na temelju dvogodišnjih programa rada iz stavka 7.

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 na temelju Uredbe (EU) …/…[+] mogu sudjelovati u aktivnostima skupine za suradnju u skladu s člankom 47. stavkom 1. te uredbe.

[+] SL: molimo u tekst umetnuti broj Uredbe iz dokumenta PE-CONS 41/22 (2020/0266(COD)).

Skupina za suradnju može, prema potrebi, pozvati Europski parlament i 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;

(b) pružanje smjernica nadležnim tijelima u vezi s razvojem i provedbom politika o koordiniranom otkrivanju ranjivosti, kako je navedeno u članku 7. stavku 2. točki (c);

(c) 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, normi i tehničkih specifikacija te utvrđivanja ključnih i važnih subjekata na temelju članka 2. stavka 2. točaka od (b) do (e);

(d) savjetovanje i suradnja s Komisijom u pogledu novih inicijativa kibersigurnosne politike i ukupne dosljednosti sektorskih kibersigurnosnih zahtjeva;

(e) savjetovanje i suradnja s Komisijom u pogledu nacrta delegiranih ili provedbenih akata donesenih u skladu s ovom Direktivom;

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

(g) razmjena mišljenja o provedbi sektorskih pravnih akata Unije koji sadržavaju odredbe o kibersigurnosti;

(h) ako je to relevantno, rasprava o izvješćivanju o istorazinskom ocjenjivanju iz članka 19. stavka 9. te donošenje zaključaka i preporuka;

(i) provedba koordinirane procjene sigurnosnih rizika kritičnih lanaca opskrbe u skladu s člankom 22. stavkom 1.;

(j) rasprava o slučajevima uzajamne pomoći, uključujući iskustva i rezultate prekograničnih zajedničkih nadzornih aktivnosti iz članka 37.;

(k) na zahtjev jedne ili više dotičnih država članica, rasprava o posebnim zahtjevima za uzajamnu pomoć iz članka 37.;

(l) pružanje strateških smjernica mreži CSIRT-ova i mreži EU-CyCLONe o određenim novonastalim pitanjima;

(m) razmjena mišljenja o politici daljnjih mjera nakon kibersigurnosnih incidenata velikih razmjera i kriza na temelju iskustava stečenih u okviru mreže CSIRT-ova i mreže EU-CyCLONe;

(n) doprinos kibersigurnosnim kapacitetima širom Unije olakšavanjem razmjene nacionalnih službenika putem programa za izgradnju kapaciteta koji uključuje osoblje iz nadležnih tijela ili CSIRT-ova;

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

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

(q) utvrđivanje metodologije i organizacijskih aspekata istorazinskog ocjenjivanja iz članka 19. stavka 1. te utvrđivanje metodologije samoocjene za države članice u skladu s člankom 19. stavkom 5. uz pomoć Komisije i ENISA-e te, u suradnji s Komisijom i ENISA-om, izrađivanje kodeksa ponašanja na kojima se temelje metode rada imenovanih stručnjaka za kibersigurnost u skladu s člankom 19. stavkom 6.;

(r) priprema izvješća u svrhu preispitivanja iz članka 40. o iskustvu stečenom na strateškoj i operativnoj razini te iz istorazinskih ocjenjivanja;

(s) rasprava i redovita provedba procjene stanja kiberprijetnji ili kiberincidenata, kao što su ucjenjivački softveri.

Izvješća iz prvog podstavka točke (r) skupina za suradnju podnosi Komisiji, Europskom parlamentu i Vijeću.

5. Države članice osiguravaju učinkovitu, djelotvornu i sigurnu suradnju svojih predstavnika u skupini za suradnju.

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

7. Do 1. veljače 2024., a nakon toga svake dvije godine, skupina za suradnju sastavlja program rada u pogledu mjera koje treba poduzeti za provedbu svojih ciljeva i zadaća.

8. 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 39. stavka 2.

   Komisija u skladu sa stavkom 4. točkom (e) razmjenjuje savjete i surađuje sa skupinom za suradnju na nacrtima provedbenih akata iz prvog podstavka ovog stavka.

9. Skupina za suradnju sastaje se redovito, a u svakom slučaju jednom godišnje, sa skupinom za otpornost kritičnih subjekata, osnovanom na temelju Direktive (EU) …/…[+] radi promicanja i olakšavanja strateške suradnje i razmjene informacija.

[+] SL: molimo u tekst umetnuti broj Direktive iz dokumenta PE-CONS 51/22 (2020/0365(COD)).

Članak 15.

Mreža CSIRT-ova

1. Kako bi se doprinijelo razvoju povjerenja i pouzdanja te promicanja brze i učinkovite operativne suradnje među državama članicama, osniva se mreža nacionalnih CSIRT-ova.

2. Mreža CSIRT-ova sastoji se od predstavnika CSIRT-ova imenovanih ili uspostavljenih u skladu s člankom 10. i tima za hitne računalne intervencije za institucije, tijela i agencije Unije (CERT-EU). Komisija u mreži CSIRT-ova sudjeluje kao promatrač.
ENISA osigurava tajništvo i aktivno pruža pomoć za suradnju među CSIRT-ovima.

3. Zadaće su mreže CSIRT-ova:

   (a) razmjena informacija o kapacitetima CSIRT-ova;

   (b) olakšavanje dijeljenja, prijenosa i razmjene tehnologije i relevantnih mjera, politika, alata, procesa, najbolje prakse i okvira među CSIRT-ovima;

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

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

(e) osiguravanje interoperabilnosti u pogledu specifikacija i protokola za razmjenu informacija;

(f) 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;

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

(h) pružanje pomoći državama članicama u rješavanju prekograničnih incidenata u skladu s ovom Direktivom;

(i) suradnja, razmjena najbolje prakse i pružanje pomoći CSIRT-ovima koji su imenovani koordinatorima u skladu s člankom 12. stavkom 1. u pogledu upravljanja koordiniranim otkrivanjem ranjivosti koje bi mogle imati znatan učinak na subjekte u više od jedne države članice;

(j) 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 kibersigurnosne incidente velikih razmjera i krize iz članka 9. stavka 4. na zahtjev države članice;

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

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

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

(n) 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 u pogledu na incidenata i kiberprijetnji širom Unije;

(o) ako je to relevantno, rasprava o izvješćima o istorazinskom ocjenjivanju iz članka 19. stavka 9.;

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

4. U svrhu preispitivanja iz članka 40. mreža CSIRT-ova do … [24 mjeseca od datuma stupanja na snagu ove Direktive], a nakon toga svake dvije godine, ocjenjuje napredak ostvaren u operativnoj suradnji i donosi izvješće. U izvješću se posebno donose zaključci i preporuke na temelju ishoda istorazinskih ocjenjivanja iz članka 19. provedenih u pogledu nacionalnih CSIRT-ova. To se izvješće dostavlja skupini za suradnju.

5. Mreža CSIRT-ova donosi svoj poslovnik.

6. Mreža CSIRT-a i mreža EU-CyCLONe dogovaraju postupovne aranžmane na temelju kojih surađuju.

Članak 16.

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

1. Mreža EU-CyCLONe osniva se kako bi se poduprlo koordinirano upravljanje kibersigurnosnim incidentima velikih razmjera i krizama na operativnoj razini i osigurala redovita razmjena relevantnih informacija među državama članicama te institucijama, tijelima, uredima i agencijama Unije.

2. Mreža EU-CyCLONe čine predstavnici tijela država članica za upravljanje kiberkrizama te, u slučajevima kada potencijalni ili aktualni kibersigurnosni incident velikih razmjera ima ili bi mogao imati znatan učinak na usluge i djelatnosti obuhvaćene područjem primjene ove Direktive, Komisija. U drugim slučajevima Komisija u aktivnostima mreže EU-CyCLONe sudjeluje kao promatrač.

ENISA osigurava tajništvo mreže EU-CyCLONe i podupire sigurnu razmjenu informacija te osigurava potrebne alate za potporu suradnji među državama članicama osiguravajući pritom sigurnu razmjenu informacija.

Mreža EU-CyCLONe može, prema potrebi, pozvati predstavnike relevantnih dionika da u njegovu radu sudjeluju kao promatrači.

3. Mreža EU-CyCLONe ima sljedeće zadaće:

(a) povećanje razine pripravnosti za upravljanje kibersigurnosnim incidentima velikih razmjera i krizama;

(b) poboljšanje zajedničke informiranosti o kibersigurnosnim incidentima velikih razmjera i krizama;

(c) procjena posljedica i učinka relevantnih kibersigurnosnih incidenata velikih razmjera i kriza te predlaganje mogućih mjera ublažavanja;

(d) koordinacija upravljanja kibersigurnosnim incidentima velikih razmjera i krizama te pomoć pri odlučivanju na političkoj razini u pogledu takvih incidenata i kriza;

(e) rasprava, na zahtjev dotične države članice, o nacionalnim planovima za odgovor na kibersigurnosne incidente velikih razmjera i krize iz članka 9. stavka 4.

4. Mreža EU-CyCLONe donosi svoj poslovnik.

5. Mreža EU-CyCLONe redovito izvješćuje skupinu za suradnju o upravljanju kibersigurnosnim incidentima velikih razmjera i krizama te o trendovima, posvećujući posebnu pažnju njihovu učinku na ključne i važne subjekte.

6. Mreža EU-CyCLONe surađuje s mrežom CSIRT-ova na temelju dogovorenih postupovnih aranžmana iz članka 15. stavka 6.

7. Mreža EU-CyCLONe do … [18 mjeseci od datuma stupanja na snagu ove Direktive] i svakih 18 mjeseci nakon toga, Europskom parlamentu i Vijeću podnosi izvješće u kojem ocjenjuje svoj rad.

Članak 17.

Međunarodna suradnja

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

Članak 18.

Izvješće o stanju kibersigurnosti u Uniji

1. ENISA u suradnji s Komisijom i skupinom za suradnju donosi dvogodišnje izvješće o stanju kibersigurnosti u Uniji te podnosi i predstavlja to izvješće Europskom parlamentu. Izvješće se, među ostalim, čini dostupnim u strojno čitljivom formatu i obuhvaća sljedeće:

   (a) procjenu rizika u području kibersigurnosti na razini Unije, uzimajući u obzir kiberprijetnje;

   (b) ocjenu razvoja kibersigurnosnih kapaciteta u javnim i privatnim sektorima širom Unije;

(c) procjenu opće razine informiranosti o kibersigurnosti i kiberhigijeni među građanima i subjektima, uključujući mala i srednja poduzeća;

(d) skupnu ocjenu ishoda istorazinskih ocjenjivanja iz članka 19.;

(e) skupnu ocjenu razine razvijenosti kibersigurnosnih kapaciteta i resursa širom Unije, uključujući one na sektorskoj razini, te do koje su mjere usklađene nacionalne strategije država članica za kibersigurnost.

2. Izvješće sadržava posebne preporuke o politikama u cilju rješavanja nedostataka i povećanja razine kibersigurnosti širom Unije te sažetak zaključaka za određeno razdoblje iz tehničkih izvješća o stanju kibersigurnosti u EU-u koje sastavlja ENISA u skladu s člankom 7. stavkom 6. Uredbe (EU) 2019/881.

3. ENISA u suradnji Komisijom, skupinom za suradnju i mrežom CSIRT-ova razvija metodologiju, uključujući relevantne varijable, kao što su kvantitativni i kvalitativni pokazatelji, skupnih ocjena iz stavka 1. točke (e).

Članak 19.

Istorazinska ocjenjivanja

1. Skupina za suradnju, uz pomoć Komisije i ENISA-e te, ako je to relevantno, mreže CSIRT-ova, do … [24 mjeseca nakon datuma stupanja na snagu ove Direktive] utvrđuje metodologiju i organizacijske aspekte istorazinskih ocjenjivanja s ciljem učenja iz zajedničkih iskustava, jačanja uzajamnog povjerenja, postizanja visoke zajedničke razine kibersigurnosti te jačanja kibersigurnosnih kapaciteta i politika država članica potrebnih za provedbu ove Direktive. Sudjelovanje u istorazinskim ocjenjivanjima je dobrovoljno. Istorazinska ocjenjivanja provode stručnjaci za kibersigurnost. Stručnjake za kibersigurnost imenuju najmanje dvije države članice, koje nisu država članica koja se ocjenjuje.

   Istorazinska ocjenjivanja obuhvaćaju barem jedno od sljedećeg:

   (a) razinu provedbe mjera upravljanja kibersigurnosnim rizicima i obveza izvješćivanja iz članaka 21. i 23.;

   (b) razinu kapaciteta, uključujući dostupne financijske, tehničke i ljudske resurse te djelotvornost izvršavanja zadaća nadležnih tijela;

(c) operativni kapacitet CSIRT-ova;

(d) razinu provedbe uzajamne pomoći iz članka 37.;

(e) razinu provedbe mehanizama za razmjenu informacija o kibersigurnosti iz članka 29.;

(f) posebne probleme prekogranične ili međusektorske prirode.

2. Metodologija iz stavka 1. uključuje objektivne, nediskriminirajuće, pravedne i transparentne kriterije na temelju kojih države članice imenuju stručnjake za kibersigurnost koji su kvalificirani za provedbu istorazinskih ocjenjivanja. ENISA i Komisija sudjeluju u istorazinskom ocjenjivanju kao promatrači.

3. Države članice mogu identificirati posebne probleme iz stavka 1. točke (f) koje treba ocijeniti za potrebe istorazinskog ocjenjivanja.

4. Prije početka istorazinskog ocjenjivanja iz stavka 1., države članice obavješćuju države članice koje sudjeluju o opsegu takvog ocjenjivanja, među ostalim o specifičnim problemima identificiranim u skladu sa stavkom 3.

5. Prije početka istorazinskog ocjenjivanja, država članica može provesti samoocjenu aspekata koji se ocjenjuju i tu samoocjenu dostaviti imenovanim stručnjacima za kibersigurnost. Skupina za suradnju uz pomoć Komisije i ENISA-e utvrđuje metodologiju za samoocjenu koju provode države članice.

6. Istorazinska ocjenjivanja uključuju fizičke ili virtualne posjete na lokaciji i razmjene informacija izvan lokacije. U skladu s načelom dobre suradnje, država članica za koju se provodi istorazinsko ocjenjivanje dostavlja imenovanim stručnjacima za kibersigurnost informacije potrebne za ocjenu, ne dovodeći u pitanje pravo Unije ili nacionalno pravo u vezi sa zaštitom povjerljivih ili klasificiranih podataka i zaštitom ključnih državnih funkcija, kao što je nacionalna sigurnost. Skupina za suradnju, u suradnji s Komisijom i ENISA-om, razvija odgovarajuće kodekse ponašanja koji podupiru metode rada imenovanih stručnjaka za kibersigurnost. Sve informacije dobivene tijekom istorazinskog ocjenjivanja smiju se upotrebljavati isključivo u tu svrhu. Stručnjaci za kibersigurnost koji sudjeluju u istorazinskom ocjenjivanju ne smiju trećim stranama otkrivati osjetljive ili povjerljive informacije dobivene tijekom tog istorazinskog ocjenjivanja.

7. Nakon provedenog istorazinskog ocjenjivanja isti aspekti ocijenjeni u određenoj državi članici ne podvrgavaju se daljnjem istorazinskom ocjenjivanju u toj državi članici tijekom dvije godine nakon završetka tog istorazinskog ocjenjivanja, osim ako država članica to ne zatraži ili na to ne pristane nakon prijedloga skupine za suradnju.

8. Države članice osiguravaju da se druge države članice, skupina za suradnju, Komisija i ENISA-a prije početka istorazinskog ocjenjivanja budu obaviještene o svakom riziku od sukoba interesa imenovanih stručnjaka za kibersigurnost. Država članica za koju se provodi istorazinsko ocjenjivanje može se usprotiviti imenovanju pojedinih stručnjaka za kibersigurnost iz opravdanih razloga, o kojima obavještava državu članicu koja ih imenuje.

9. Stručnjaci za kibersigurnost koji sudjeluju u istorazinskim ocjenjivanjima sastavljaju izvješća o nalazima i zaključcima ocjenjivanja. Države članice za koje se provodi istorazinsko ocjenjivanje mogu dostaviti primjedbe na nacrte izvješća koja se na njih odnose, a takve se primjedbe prilažu izvješćima. Izvješća sadržavaju preporuke kako bi se omogućilo poboljšanje aspekata obuhvaćenih istorazinskim ocjenjivanjem. Izvješća se podnose skupini za suradnju i, ako je to relevantno, mreži CSIRT-ova. Država članica za koju se provodi istorazinsko ocjenjivanje može odlučiti javno objaviti svoje izvješće ili njegovu redigiranu verziju.

Poglavlje IV.

Mjere upravljanja kibersigurnosnim rizicima i obveze izvješćivanja

Članak 20.

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 21., nadgledaju njegovu provedbu i mogu se smatrati odgovornima za povrede tog članka od strane subjekata.

   Primjenom ovog stavka ne dovodi se u pitanje nacionalno pravo u pogledu pravila o odgovornosti koja se primjenjuju na javne institucije ni odgovornosti javnih službenika te izabranih ili imenovanih dužnosnika.

2. Države članice osiguravaju da članovi upravljačkih tijela ključnih i važnih subjekata moraju pohađati osposobljavanja te potiču ključne i važne subjekte da slično osposobljavanje redovito nude svojim zaposlenicima kako bi stekli dovoljno znanja i vještina za prepoznavanje i procjenu praksi upravljanja kibersigurnosnim rizicima i njihova učinka na usluge koje taj subjekt pruža.

Članak 21.

Mjere upravljanja kibersigurnosnim rizicima

1. Države članice osiguravaju da ključni i važni subjekti poduzimaju odgovarajuće i razmjerne tehničke, operativne i organizacijske mjere za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi kojima se ti subjekti služe u svom poslovanju ili u pružanju svojih usluga te za sprečavanje ili smanjivanje na najmanju moguću mjeru učinka incidenata na primatelje njihovih usluga i na druge usluge.

   Uzimajući u obzir najnovija dostignuća i, ako je to primjenjivo, relevantne europske i međunarodne norme te trošak provedbe, mjerama iz stavka prvog podstavka osigurava se razina sigurnosti mrežnih i informacijskih sustava primjerena postojećem riziku.
   Pri procjeni proporcionalnosti tih mjera u obzir se uzima stupanj izloženosti subjekta rizicima, veličina subjekta, vjerojatnost pojave incidenata i njihova ozbiljnost, uključujući njihov društveni i gospodarski učinak.

2. Mjere iz stavka 1. temelje se na pristupu kojim se uzimaju u obzir sve opasnosti i čiji je cilj zaštita mrežnih i informacijskih sustava i fizičkog okruženja tih sustava od incidenata te uključuju najmanje sljedeće:

   (a) politike analize rizika i sigurnosti informacijskih sustava;

   (b) postupanje s incidentima;

(c) kontinuitet poslovanja, kao što je upravljanje sigurnosnim kopijama i oporavak od katastrofe, te upravljanje krizama;

(d) sigurnost lanca opskrbe, uključujući sigurnosne aspekte u pogledu odnosa između svakog subjekta i njegovih izravnih dobavljača ili pružatelja 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) osnovne prakse kiberhigijene i osposobljavanje o kibersigurnosti;

(h) politike i postupke u pogledu kriptografije i, prema potrebi, kriptiranja;

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

(j) korištenje višefaktorske provjere autentičnosti ili rješenja kontinuirane provjere autentičnosti, zaštićene glasovne, video i tekstualne komunikacije te sigurnih komunikacijskih sustava u hitnim slučajevima unutar subjekta, prema potrebi.

3. Države članice osiguravaju da subjekti, kada razmatraju koje su mjere iz stavka 2. točke (d) ovog članka primjerene, 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, kada razmatraju koje su mjere iz te točke primjerene, uzmu u obzir rezultate koordiniranih procjena sigurnosnih rizika ključnih lanaca opskrbe provedenih u skladu s člankom 22. stavkom 1.

4. Države članice osiguravaju da subjekt koji utvrdi da ne poštuje mjere iz stavka 2. bez nepotrebne odgode poduzme sve potrebne, primjerene i razmjerne korektivne mjere.

5. Komisija do … [21 mjesec nakon datuma stupanja na snagu ove Direktive] donosi provedbene akte kojima se utvrđuju tehnički i metodološki zahtjevi za mjere iz stavka 2. u pogledu pružatelja usluga DNS-a, registara naziva vršnih domena, pružatelja usluga računalstva u oblaku, pružatelja usluga podatkovnog centra, pružatelja mreža za isporuku sadržaja, pružatelja upravljanih usluga, pružatelja upravljanih sigurnosnih usluga, pružatelja internetskih tržišta, pružatelja internetskih tražilica i pružatelja platformi za usluge društvenih mreža i pružatelja usluga povjerenja.

Komisija može donijeti provedbene akte kojima se utvrđuju tehnički i metodološki zahtjevi te, prema potrebi, sektorski zahtjevi za mjere iz stavka 2. i u pogledu ključnih i važnih subjekata koji nisu navedeni u prvom podstavku ovog stavka.

U pripremi provedbenih akata iz prvog i drugog podstavka ovog stavka Komisija, u mjeri u kojoj je to moguće, prati europske i međunarodne norme te relevantne tehničke specifikacije. Komisija razmjenjuje savjete i surađuje sa skupinom za suradnju i ENISA-om na nacrtima provedbenih akata u skladu s člankom 14. stavkom 4. točkom (e).

Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 39. stavka 2.

Članak 22.

Koordinirane procjene rizika ključnih lanaca opskrbe na razini Unije

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

2. Komisija, nakon savjetovanja sa skupinom za suradnju i ENISA-om i, ako je to potrebno, relevantnim dionicima, utvrđuje određene ključne IKT usluge, IKT sustave ili IKT proizvode koji mogu biti predmet koordinirane procjene sigurnosnih rizika iz stavka 1.

Članak 23.

Obveze izvješćivanja

1. Svaka država članica osigurava da ključni i važni subjekti bez nepotrebne odgode obavješćuju svoj CSIRT ili, ako je to primjenjivo, svoje nadležno tijelo u skladu sa stavkom 4. o svakom incidentu koji ima znatan učinak na pružanje njihovih usluga kako se navodi u stavku 3. (značajan incident). Prema potrebi, dotični subjekti bez nepotrebne odgode obavješćuju primatelje svojih usluga o značajnim incidentima koji bi mogli negativno utjecati na pružanje tih usluga. Svaka država članica osigurava da ti subjekti, među ostalim, izvješćuju o svim informacijama koje CSIRT-u ili, ako je to primjenjivo, nadležnom tijelu omogućuju da utvrde sve prekogranične učinke incidenta. Subjekt koji obavješćuje ne podliježe samo zbog toga povećanoj odgovornosti.

Ako dotični subjekti obavijeste nadležno tijelo o značajnom incidentu u skladu s prvim podstavkom, država članica osigurava da to nadležno tijelo obavijest po primitku proslijedi CSIRT-u.

U slučaju prekograničnog ili međusektorskog značajnog incidenta, države članice osiguravaju da njihove jedinstvene kontaktne točke pravodobno dobiju relevantne informacije podnesene u skladu sa stavkom 4.

2. Države članice, ako je to primjenjivo, osiguravaju da ključni i važni subjekti primatelje svojih usluga na koje bi mogla utjecati ozbiljna kiberprijetnja bez nepotrebne odgode obavješćuju o svim mjerama ili pravnim sredstvima koje ti primatelji mogu poduzeti kao odgovor na prijetnju. Prema potrebi, subjekti te primatelje obavješćuju i o samoj ozbiljnoj kiberprijetnji.

3. Incident se smatra značajnim:

(a) ako je uzrokovao ili može uzrokovati ozbiljne poremećaje u funkcioniranju usluga ili financijske gubitke za predmetni subjekt;

(b) ako je utjecao ili bi mogao utjecati na druge fizičke ili pravne osobe uzrokovanjem znatne materijalne ili nematerijalne štete.

4. Države članice osiguravaju da, za potrebe obavješćivanja iz stavka 1., predmetni subjekti CSIRT-u ili, ako je to primjenjivo, nadležnom tijelu podnose:

(a) bez nepotrebne odgode, a u svakom slučaju u roku od 24 sata od kad su saznali za značajan incident, rano upozorenje u kojem se, ako je to primjenjivo, navodi sumnja li se da je značajan incident uzrokovan nezakonitim ili zlonamjernim djelovanjem te bi li mogao imati prekogranični učinak;

(b) bez nepotrebne odgode, a u svakom slučaju u roku od 72 sata od kad su saznali za značajan incident, obavijest o incidentu kojom se, ako je to primjenjivo, ažuriraju informacije iz točke (a) i navodi početna procjena značajnog incidenta, uključujući njegovu ozbiljnosti i učinak te, ako su dostupni, pokazatelje ugroženosti;

(c) na zahtjev CSIRT-a ili, ako je to primjenjivo, nadležnog tijela, privremeno izvješće o relevantnim ažuriranjima statusa;

(d) završno izvješće najkasnije mjesec dana nakon podnošenja obavijesti o incidentu iz točke (b), koje uključuje sljedeće:

i. detaljan opis incidenta, uključujući njegovu ozbiljnost i učinak;

ii. vrstu prijetnje ili temeljni uzrok koji je vjerojatno uzrokovao incident;

iii. primijenjene i tekuće mjere ublažavanja;

iv. ako je to primjenjivo, prekogranični učinak incidenta;

(e) u slučaju incidenta koji je u tijeku u trenutku podnošenja završnog izvješća iz točke (d), države članice osiguravaju da dotični subjekti dostave izvješće o napretku u tom trenutku te završno izvješće u roku od mjesec dana od postupanja s incidentom.

Odstupajući od prvog podstavka točke (b), pružatelj usluga povjerenja bez nepotrebne odgode, a u svakom slučaju u roku od 24 sata od kada je saznao za značajan incident, obavješćuje CSIRT ili, ako je to primjenjivo, nadležno tijelo o značajnim incidentima koji imaju učinak na pružanje njegovih usluga povjerenja.

5. CSIRT ili nadležno tijelo bez nepotrebne odgode i ako je moguće u roku od 24 sata od primitka ranog upozorenja iz stavka 4. točke (a) dostavlja odgovor subjektu koji obavješćuje, uključujući početne povratne informacije o značajnom incidentu i, na zahtjev subjekta, smjernice ili operativne savjete o provedbi mogućih mjera ublažavanja.
Ako CSIRT nije prvi primatelj obavijesti iz stavka 1., smjernice pruža nadležno tijelo u suradnji s CSIRT-om. CSIRT pruža dodatnu tehničku potporu ako to zatraži predmetni subjekt. Ako se sumnja da je značajan incident kriminalne naravi, CSIRT ili nadležno tijelo pruža i smjernice o prijavi tog značajnog incidenta tijelima za izvršavanje zakonodavstva.

6. CSIRT, nadležno tijelo ili jedinstvena kontaktna točka o značajnom incidentu bez nepotrebne odgode obavješćuje ostale pogođene države članice i ENISA-u prema potrebi, a osobito ako se značajan incident odnosi na dvije države članice ili više njih. Takve informacije obuhvaćaju vrstu informacija primljenih u skladu sa stavkom 4. Pritom CSIRT, nadležno tijelo ili jedinstvena kontaktna točka, u skladu s pravom Unije ili nacionalnim pravom, čuvaju sigurnost i komercijalne interese subjekta te povjerljivost dostavljenih informacija.

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

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

9. Jedinstvena kontaktna točka svaka tri mjeseca podnosi ENISA-i sažeto izvješće koje uključuje anonimizirane i agregirane podatke o značajnim incidentima, incidentima, ozbiljnim kiberprijetnjama i izbjegnutim incidentima o kojima je obaviješteno u skladu sa stavkom 1. ovog članka i člankom 30. Kako bi se doprinijelo dostavljanju usporedivih podataka, ENISA može donijeti tehničke smjernice o parametrima za informacije koje su uključene u sažeto izvješće. ENISA svakih šest mjeseci obavješćuje skupinu za suradnju i mrežu CSIRT-ova o svojim zaključcima o primljenim obavijestima.

10. CSIRT-ovi ili, ako je to primjenjivo, nadležna tijela dostavljaju nadležnim tijelima na temelju Direktive (EU) …/…[+] informacije o značajnim incidentima, incidentima, kiberprijetnjama i izbjegnutim incidentima o kojima su u skladu sa stavkom 1. ovog članka i člankom 30. obavijestili subjekti koji su utvrđeni kao kritični subjekti na temelju Direktive (EU) …/…[+].

11. Komisija može donijeti provedbene akte kojima se dodatno utvrđuju vrsta informacija te oblik i postupak podnošenja obavijesti u skladu sa stavkom 1. ovog članka i člankom 30. te obavijest podnesena u skladu sa stavkom 2. ovog članka.

[+] SL: molimo u tekst umetnuti broj Direktive iz dokumenta PE-CONS 51/22 (2020/0365(COD)).

Komisija do … [21 mjesec nakon datuma stupanja na snagu ove Direktive] donosi provedbene akte u pogledu pružatelja usluga DNS-a, registara naziva vršnih domena, pružatelja usluga računalstva u oblaku, pružatelja usluga podatkovnog centra, pružatelja mreža za isporuku sadržaja, pružatelja upravljanih usluga, pružatelja upravljanih sigurnosnih usluga, pružatelja internetskih tržišta, pružatelja internetskih tražilica i pružatelja platformi za usluge društvenih mreža, kojima se dodatno utvrđuju slučajevi u kojima se incident smatra značajnim, kako je navedeno u stavku 3. Komisija takve provedbene akte može donijeti u pogledu drugih ključnih i važnih subjekata.

Komisija razmjenjuje savjete i surađuje sa skupinom za suradnju na nacrtima provedbenih akata iz prvog i drugog podstavka ovog stavka u skladu s člankom 14. stavkom 4. točkom (e).

Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 39. stavka 2.

Članak 24.

Primjena europskih programa kibersigurnosne certifikacije

1. Kako bi dokazale usklađenost s pojedinim zahtjevima iz članka 21., države članice mogu od ključnih i važnih subjekata zahtijevati korištenje određenim IKT proizvodima, IKT uslugama i IKT procesima, koje je razvio ključni ili važni subjekt ili su nabavljeni od treće strane, koji su certificirani na temelju europskih programa kibersigurnosne certifikacije donesenih u skladu s člankom 49. Uredbe (EU) 2019/881. Nadalje, države članice potiču ključne i važne subjekte da se koriste kvalificiranim uslugama povjerenja.

2. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 38. radi dopune ove Direktive, kojima se određuje od kojih se kategorija ključnih i važnih subjekata treba zahtijevati korištenje određenim certificiranim IKT proizvodima, IKT uslugama i IKT procesima ili pribavljanje certifikata na temelju europskih programa kibersigurnosne certifikacije donesenih u skladu s člankom 49. Uredbe (EU) 2019/881. Ti delegirani akti donose se ako su utvrđene nedovoljne razine kibersigurnosti te obuhvaćaju razdoblje provedbe.

   Prije donošenja takvih delegiranih akata Komisija provodi procjenu učinka i organizira savjetovanja u skladu s člankom 56. Uredbe (EU) 2019/881.

3. Ako nije dostupan odgovarajući europski program kibersigurnosne certifikacije za potrebe stavka 2. ovog članka, Komisija može, nakon savjetovanja sa skupinom za suradnju i Europskom skupinom za kibersigurnosnu certifikaciju, zatražiti od ENISA-e da izradi prijedlog programa certifikacije u skladu s člankom 48. stavkom 2. Uredbe (EU) 2019/881.

Članak 25.

Normizacija

1. Države članice, u cilju promicanja konvergentne provedbe članka 21. stavaka 1. i 2., bez nametanja ili diskriminacije u korist upotrebe određene vrste tehnologije, potiču primjenu europskih i međunarodnih normi i tehničkih specifikacija relevantnih za sigurnost mrežnih i informacijskih sustava.

2. ENISA u suradnji s državama članicama i, prema potrebi, nakon savjetovanja s relevantnim dionicima, 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, kojima bi se ta područja mogla obuhvatiti.

Poglavlje V.
Nadležnost i registracija

Članak 26.

Nadležnost i teritorijalnost

1. Smatra se da su subjekti obuhvaćeni područjem primjene ove Direktive u nadležnosti države članice u kojoj imaju poslovni nastan, osim u sljedećim slučajevima:

   (a) pružatelji javnih elektroničkih komunikacijskih mreža ili pružatelji javno dostupnih elektroničkih komunikacijskih usluga, za koje se smatra da su u nadležnosti države članice u kojoj pružaju svoje usluge;

   (b) pružatelji usluga DNS-a, registri naziva vršnih domena, subjekti koji pružaju usluge registracije naziva domena, pružatelji usluga računalstva u oblaku, pružatelji usluga podatkovnog centra, pružatelji mreža za isporuku sadržaja, pružatelji upravljanih usluga, pružatelji upravljanih sigurnosnih usluga, pružatelji internetskih tržišta, pružatelji internetskih tražilica ili pružatelji platformi za usluge društvenih mreža, za koje se smatra da su u nadležnosti države članice u kojoj imaju glavni poslovni nastan u Uniji u skladu sa stavkom 2.;

(c) subjekti javne uprave, za koja se smatra da su u nadležnosti države članice koja ih je osnovala.

2. Za potrebe ove Direktive smatra se da subjekt iz stavka 1. točke (b) ima glavni poslovni nastan u Uniji u državi članici u kojoj se pretežno donose odluke povezane s mjerama upravljanja kibersigurnosnim rizicima. Ako se takva država članica ne može utvrditi ili ako se takve odluke ne donose u Uniji, smatra se da se glavni poslovni nastan nalazi u državi članici u kojoj se provode kibersigurnosne operacije. Ako se takva država članica ne može utvrditi, smatra se da se glavni poslovni nastan nalazi u državi članici u kojoj subjekt ima poslovnu jedinicu s najvećim brojem zaposlenika u Uniji.

3. Ako subjekt iz stavka 1. točke (b) nema poslovni nastan u Uniji, ali nudi usluge unutar Unije, dužan je imenovati predstavnika u Uniji. Predstavnik mora imati poslovni nastan u jednoj od država članica u kojima se nude usluge. Smatra se da je takav subjekt u nadležnosti one države članice u kojoj njegov predstavnik ima poslovni nastan.
Ako predstavnik u Uniji nije imenovan u skladu s ovim člankom, svaka država članica u kojoj subjekt pruža usluge može poduzeti pravne mjere protiv subjekta zbog povrede ove Direktive.

4. Imenovanjem predstavnika koje obavlja subjekt iz stavka 1. točke (b) ne dovode se u pitanje pravni postupci koji bi se mogli poduzeti protiv tog subjekta.

5. Države članice koje su primile zahtjev za uzajamnu pomoć u vezi sa subjektom iz stavka 1. točke (b) mogu, u okvirima zahtjeva, poduzeti odgovarajuće nadzorne mjere i mjere izvršavanja u odnosu na dotični subjekt koji pruža usluge ili koji ima mrežni i informacijski sustav na njihovu državnom području.

Članak 27.

Registar subjekata

1. ENISA uspostavlja i vodi registar pružatelja usluga DNS-a, registra naziva vršnih domena, subjekata koji pružaju usluge registracije naziva domena, pružatelja usluga računalstva u oblaku, pružatelja usluga podatkovnog centra, pružatelja mreža za isporuku sadržaja, pružatelja upravljanih usluga, pružatelja upravljanih sigurnosnih usluga, pružatelja internetskih tržišta, pružatelja internetskih tražilica ili pružatelja platformi za usluge društvenih mreža na temelju informacija dobivenih od jedinstvene kontaktne točke u skladu sa stavkom 4. ENISA na zahtjev nadležnim tijelima dopušta pristup tom registru, osiguravajući pritom, ako je to primjenjivo, zaštitu povjerljivosti informacija.

2. Države članice do … [24 mjeseca nakon datuma stupanja na snagu ove Direktive] zahtijevaju od subjekata iz stavka 1. da nadležnim tijelima dostavljaju sljedeće informacije:

(a) naziv subjekta;

(b) ako je to primjenjivo, relevantni sektor, podsektor i vrstu subjekta iz Priloga I. ili II.;

(c) adresu glavnog poslovnog nastana subjekta i njegovih drugih zakonitih poslovnih jedinica u Uniji ili, ako nemaju poslovni nastan u Uniji, njegova predstavnika imenovanog u skladu s člankom 26. stavkom 3.;

(d) ažurirane podatke za kontakt, uključujući e-adrese i telefonske brojeve subjekta i, ako je to primjenjivo, njegova predstavnika imenovanog u skladu s člankom 26. stavkom 3.;

(e) države članice u kojima subjekt pruža usluge; i

(f) IP raspone subjekta.

3. Države članice osiguravaju da subjekti iz stavka 1. bez odgode, a u svakom slučaju u roku od tri mjeseca od datuma promjene, obavješćuju nadležno tijelo o svim promjenama informacija koje su dostavili na temelju stavka 2.

4. Po primitku informacija iz stavka 2. i stavka 3., osim informacija iz stavka 2. točke (f), jedinstvena kontaktna točka dotične države članice prosljeđuje ih bez nepotrebne odgode ENISA-i.

5. Informacije iz stavaka 2. i 3. ovog članka podnose se, ako je to primjenjivo, putem nacionalnog mehanizma iz članka 3. stavka 4. četvrtog podstavka.

Članak 28.

Baza *podataka o registraciji naziva domena*

1. Kako bi se doprinijelo sigurnosti, stabilnosti i otpornosti DNS-a, države članice zahtijevaju od registara naziva vršnih domena i subjekata koji pružaju usluge registracije naziva domena da 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 u pogledu podataka koji su osobni podaci.

2. Za potrebe stavka 1. države članice zahtijevaju da baza podataka o registraciji naziva domena sadržava informacije potrebne za identifikaciju nositelja naziva domena i kontaktnih točaka koje upravljaju nazivima domena u okviru vršnih domena te za kontakt s njima. Takve informacije uključuju:

   (a) naziv domene;

(b) datum registracije;

(c) ime korisnika domene te njegovu e-adresu i telefonski broj za kontakt;

(d) e-adresu i telefonski broj za kontakt kontaktne točke koja upravlja nazivom domene ako su različiti od podataka korisnika domene.

3. Države članice zahtijevaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena uspostave politike i postupke, uključujući postupke provjere, kojima se osigurava da baze podataka iz stavka 1. sadržavaju točne i potpune informacije. Države članice zahtijevaju da se takve politike i postupci javno objavljuju.

4. Države članice zahtijevaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena bez nepotrebne odgode nakon registracije naziva domene javno objavljuju podatke o registraciji naziva domena koji nisu osobni podaci.

5. Države članice zahtijevaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena 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 zahtijevaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena odgovore bez nepotrebne odgode, a u svakom slučaju u roku od 72 sata nakon primitka svakog zahtjeva za pristup. Države članice zahtijevaju da se politike i postupci za otkrivanje takvih podataka javno objavljuju.

6. Usklađenost s obvezama utvrđenim u stavcima od 1. do 5. ne smije dovesti do dvostrukog prikupljanja podataka o registraciji naziva domena. U tu svrhu države članice zahtijevaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena međusobno surađuju.

Poglavlje VI.
Razmjena informacija

Članak 29.

Mehanizmi za razmjenu informacija o kibersigurnosti

1. Države članice osiguravaju da subjekti obuhvaćeni područjem primjene ove Direktive i, prema potrebi, drugi subjekti koji nisu obuhvaćeni područjem primjene ove Direktive mogu međusobno dobrovoljno razmjenjivati relevantne informacije o kibersigurnosti, uključujući informacije koje se odnose na kiberprijetnje, izbjegnute incidente, ranjivosti, tehnike i postupke, pokazatelje ugroženosti, neprijateljske taktike, informacije o počinitelju prijetnje, kibersigurnosna upozorenja i preporuke o konfiguraciji kibersigurnosnih alata za otkrivanje kibernapada, ako takva razmjena informacija:

   (a) ima za cilj sprečavanje ili otkrivanje incidenata, odgovaranje na njih, oporavljanje od incidenata ili ublažavanje njihova učinka;

(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, zaustavljanja i sprečavanja prijetnji, strategijama ublažavanja ili fazama odgovora i oporavka ili promicanjem suradničkog istraživanja kiberprijetnji između javnih i privatnih subjekata.

2. Države članice osiguravaju da se razmjena informacija odvija unutar zajednica ključnih i važnih subjekata te, prema potrebi, njihovih dobavljača ili pružatelja usluga. S obzirom na potencijalno osjetljivu prirodu informacija koje se razmjenjuju, takva se razmjena provodi putem mehanizama za razmjenu informacija o kibersigurnosti.

3. Države članice olakšavaju uspostavu mehanizama za dijeljenje informacija o kibersigurnosti iz stavka 2. ovog članka. Takvim mehanizmima mogu se utvrditi operativni elementi, među ostalim upotreba namjenskih IKT platformi i alata za automatizaciju, sadržaj i uvjeti mehanizama za razmjenu informacija. Utvrđivanjem pojedinosti o sudjelovanju tijela javne vlasti u takvim mehanizmima države članice mogu odrediti uvjete za informacije koje nadležna tijela ili CSIRT-ovi stavljaju na raspolaganje. Države članice nude potporu primjeni takvih mehanizama u skladu sa svojim politikama iz članka 7. stavka 2. točke (h).

4. Države članice osiguravaju da ključni i važni subjekti obavješćuju nadležna tijela o svojem sudjelovanju u mehanizmima za razmjenu informacija o kibersigurnosti 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 pruža potporu uspostavi mehanizama za razmjenu informacija o kibersigurnosti iz stavka 2. razmjenom najboljih praksi i pružanjem smjernica.

Članak 30.

Dobrovoljno obavješćivanje o relevantnim informacijama

1. Države članice osiguravaju da, uz obvezu obavješćivanja iz članka 23., CSIRT-ovima ili, ako je to primjenjivo, nadležnim tijelima obavijesti mogu dobrovoljno podnositi:

   (a) ključni i važni subjekti u pogledu incidenata, kiberprijetnji i izbjegnutih incidenata;

   (b) subjekti koji nisu subjekti iz točke (a), neovisno o tome jesu li obuhvaćeni područjem primjene ove Direktive, u pogledu značajnih incidenata, kiberprijetnji ili izbjegnutih incidenata.

2. Države članice obrađuju obavijesti iz stavka 1. ovog članka u skladu s postupkom utvrđenim u članku 23. Države članice obradi obveznih obavijesti mogu dati prednost pred obradom obavijesti na dobrovoljnoj osnovi.

Prema potrebi, CSIRT-ovi i, ako je primjenjivo, nadležna tijela, pružaju jedinstvenim kontaktnim točkama, informacije o obavijestima primljenim na temelju ovog članka, uz istovremeno osiguravanje povjerljivosti i odgovarajuće zaštite informacija koje je dostavio subjekt koji obavješćuje. Ne dovodeći u pitanje sprečavanje, istragu, otkrivanje i progon kaznenih djela, dobrovoljno izvješćivanje ne smije dovesti do nametanja dodanih obveza subjektu koji obavješćuje kojima ne bi podlijegao da nije podnio obavijest.

Poglavlje VII.
Nadzor i izvršavanje

Članak 31.

Opći aspekti nadzora i izvršavanje

1. Države članice osiguravaju da njihova nadležna tijela djelotvorno nadziru i poduzimaju mjere potrebne za osiguravanje usklađenosti s ovom Direktivom.

2. Države članice mogu dopustiti svojim nadležnim tijelima da daju prednost nadzornim zadaćama. Takvo davanje prednosti utemeljeno je na pristupu koji se temelji na riziku. U tu svrhu, pri izvršavanju svojih nadzornih zadaća iz stavaka 32. i 33. nadležna tijela mogu uspostaviti nadzorne metodologije kojima se omogućuje određivanje tih zadaća kao prioriteta primjenom pristupa utemeljenog na procjeni rizika.

3. Nadležna tijela blisko surađuju s nadzornim tijelima na temelju Uredbe (EU) 2016/679 u rješavanju incidenata koji za posljedicu imaju povrede osobnih podataka ne dovodeći u pitanje nadležnosti i zadaće nadzornih tijela na temelju te uredbe.

4. Ne dovodeći u pitanje nacionalne zakonodavne i institucionalne okvire, države članice osiguravaju da, pri nadzoru usklađenosti subjekata javne uprave s ovom Direktivom i određivanju mjera izvršavanja u odnosu na povrede ove Direktive, nadležna tijela imaju odgovarajuće ovlasti za izvršavanje takvih zadaća uz operativnu neovisnost u odnosu na subjekte javne uprave koji se nadziru. Države članice mogu odlučiti o određivanju odgovarajućih, proporcionalnih i djelotvornih nadzornih mjera i mjera izvršavanja u odnosu na te subjekte u skladu s nacionalnim zakonodavnim i institucionalnim okvirima.

Članak 32.

Nadzorne mjere i mjere izvršavanja u odnosu na ključne subjekte

1. Države članice osiguravaju da su nadzorne mjere ili mjere izvršavanja određene ključnim subjektima u pogledu obveza utvrđenih u ovoj Direktivi učinkovite, proporcionalne 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 imaju ovlasti da te subjekte obvežu barem na sljedeće:

   (a) inspekcije na lokaciji i neizravni nadzor, uključujući nasumične provjere, koji provode osposobljeni stručnjaci;

   (b) redovite i ciljane revizije sigurnosti koje provodi neovisno tijelo ili nadležno tijelo;

   (c) ad hoc revizije, među ostalim i u slučajevima kad je to opravdano na temelju značajnog incidenta ili povrede ove Direktive od strane ključnog subjekta;

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

(e) zahtjeve za informacije potrebne za ocjenjivanje mjera upravljanja kibersigurnosnim rizicima koje je donio dotični subjekt, uključujući dokumentirane kibersigurnosne politike, te usklađenosti s obvezom podnošenja informacija nadležnim tijelima u skladu s člankom 27. ;

(f) zahtjeve za pristup podacima, dokumentima i informacijama potrebnima za izvršavanje 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.

Ciljane revizije sigurnosti iz prvog podstavka točke (b) temelje se na procjenama rizika koje provodi nadležno tijelo ili subjekt revizije, ili na drugim dostupnim informacijama u vezi s rizikom.

Rezultati svake ciljane revizije sigurnosti stavljaju se na raspolaganje nadležnom tijelu. Troškove takve ciljane revizije sigurnosti koju provodi neovisno tijelo plaća subjekt nad kojim se provodi revizija, osim u propisno opravdanim slučajevima u kojima nadležno tijelo odluči drugačije.

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

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

(a) izdavati upozorenja o povredama ove Direktive od strane dotičnih subjekata;

(b) donositi obvezujuće upute, među ostalim u vezi s mjerama potrebnim za sprečavanje ili otklanjanje incidenta, kao i rokove za provedbu takvih mjera i za izvješćivanje o njihovoj provedbi, ili nalog kojim se od dotičnih subjekata zahtijeva da uklone utvrđene nedostatke ili povrede ove Direktive;

(c) naložiti dotičnim subjektima da prestanu s postupanjem kojim se povređuje ova Direktiva i da ne ponavljaju takvo postupanje;

(d) naložiti dotičnim subjektima da osiguraju da su njihove mjere upravljanja kibersigurnosnim rizicima u skladu s obvezama iz članka 21. ili da ispune obveze izvješćivanja iz članka 23. na utvrđeni način i u utvrđenom roku;

(e) naložiti dotičnim subjektima da obavijeste fizičke ili pravne osobe u odnosu na koje pružaju usluge ili obavljaju djelatnosti 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 dotičnim subjektima da u razumnom roku provedu preporuke dane na temelju revizije sigurnosti;

(g) imenovati službenika za praćenje s precizno definiranim zadaćama na određeno razdoblje kako bi nadgledao usklađenost dotičnih subjekata s člancima 21. i 23.;

(h) naložiti dotičnim subjektima da objave aspekte povreda ove Direktive na određeni način;

(i) izreći ili zahtijevati da relevantna tijela ili sudovi u skladu s nacionalnim pravom izreknu upravnu novčanu kaznu u skladu s člankom 34. uz sve mjere iz točaka od (a) do (h) ovog stavka.

5. Ako su mjere izvršavanja donesene u skladu sa stavkom 4. točkama od (a) do (d) i točkom (f) neučinkovite, države članice osiguravaju da njihova nadležna tijela imaju ovlast utvrditi rok u kojem se od ključnog subjekta zahtijeva da poduzme mjere potrebne za ispravljanje nedostataka ili da ispuni zahtjeve tih tijela. Ako zatražena mjera nije poduzeta u zadanom roku, države članice osiguravaju da nadležna tijela imaju ovlasti:

(a) privremeno suspendirati ili zahtijevati od certifikacijskog tijela ili tijela koje izdaje ovlaštenja ili od suda, u skladu s nacionalnim pravom, da privremeno suspendira certifikat ili ovlaštenje za dio relevantnih usluga ili sve relevantne usluge koje ključni subjekt pruža ili djelatnosti koje obavlja;

(b) zahtijevati da relevantna tijela ili sudovi u skladu s nacionalnim pravom privremeno zabrane obavljanje upravljačkih dužnosti u ključnom subjektu svakoj fizičkoj osobi koja upravljačke dužnosti obavlja na razini glavnog izvršnog direktora ili pravnog zastupnika u tom ključnom subjektu.

Privremene suspenzije ili zabrane izrečene u skladu s ovim stavkom primjenjuju se samo dok dotični subjekt ne poduzme potrebne mjere za otklanjanje nedostataka ili dok ne ispuni zahtjeve nadležnog tijela za koje su takve mjere izvršavanja primijenjene. Izricanje takvih privremenih suspenzija ili zabrana podliježe odgovarajućim postupovnim zaštitnim mjerama u skladu s općim načelima prava Unije i Poveljom, uključujući pravo na djelotvoran pravni lijek i pošteno suđenje, pretpostavku nedužnosti i prava na obranu.

Mjere izvršavanja predviđene u ovom stavku ne primjenjuju se na subjekte javne uprave koji podliježu ovoj Direktivi.

6. Države članice osiguravaju da svaka fizička osoba koja je odgovorna za ključni subjekt ili djeluje kao njegov pravni predstavnik na temelju ovlasti za zastupanje, ovlasti za donošenje odluka u njegovo ime ili ovlasti za izvršavanje kontrole nad tim subjektom ima ovlast osigurati njegovu usklađenost s ovom Direktivom. Države članice osiguravaju da se takve fizičke osobe mogu smatrati odgovornima za kršenje svojih dužnosti da osiguraju usklađenost s ovom Direktivom.

U pogledu subjekata javne uprave, ovim stavkom ne dovodi se u pitanje nacionalno pravo država članica u pogledu odgovornosti javnih službenika te izabranih ili imenovanih dužnosnika.

7. Kada poduzimaju bilo koju mjeru izvršavanja iz stavka 4. ili 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, pri čemu se ozbiljnim povredama, među ostalim, smatra sljedeće:

i. opetovane povrede;

ii. neprijavljivanje ili neispravljanje značajnih incidenata;

iii. neuklanjanje nedostataka u skladu s obvezujućim uputama nadležnih tijela;

iv. ometanje revizija ili aktivnosti praćenja koje je naložilo nadležno tijelo nakon utvrđivanja povrede;

v. pružanje lažnih ili izrazito netočnih informacija povezanih s mjerama upravljanja kibersigurnosnim rizicima ili obvezama izvješćivanja utvrđenim u člancima 21. i 23.;

(b) trajanje povrede;

(c) sve relevantne prethodne povrede koje je počinio dotični subjekt;

(d) svaku materijalnu ili nematerijalnu štetu koja je uzrokovana, uključujući sve financijske ili gospodarske gubitke, učinke na druge usluge i broj pogođenih korisnika;

(e) je li počinitelj povrede djelovao s namjerom ili nepažnjom;

(f) sve mjere koje je subjekt poduzeo radi sprečavanja ili ublažavanja materijalne ili nematerijalne štete;

(g) svako poštovanje odobrenih kodeksa ponašanja ili odobrenih mehanizama certificiranja;

(h) razinu suradnje fizičkih ili pravnih osoba koje se smatraju odgovornima s nadležnim tijelima.

8. Nadležna tijela detaljno obrazlažu svoje mjere izvršavanja. Prije donošenja takvih mjera nadležna tijela obavješćuju predmetne subjekte o svojim preliminarnim nalazima. Ona tim subjektima također daju razuman rok za podnošenje primjedaba, osim u valjano obrazloženim slučajevima u kojima bi inače bile spriječene hitne mjere za sprečavanje incidenata ili odgovor na njih.

9. Države članice osiguravaju da njihova nadležna tijela na temelju ove Direktive obavješćuju relevantna nadležna tijela unutar iste države članice na temelju Direktive …/…[+] pri izvršavanju svojih nadzornih ovlasti i ovlasti izvršavanja kojima je cilj osigurati usklađenost subjekta koji je utvrđen kao kritični subjekt na temelju Direktive (EU) …/…[+] s ovom Direktivom. Prema potrebi, nadležna tijela na temelju Direktive (EU) …/…[+] mogu zatražiti od nadležnih tijela na temelju ove Direktive da izvršavaju svoje nadzorne ovlasti i ovlasti izvršavanja u vezi s subjektom koji je utvrđen kao kritičan subjekt na temelju Direktive (EU) …/…[+].

10. Države članice osiguravaju da njihova nadležna tijela na temelju ove Direktive surađuju s relevantnim nadležnim tijelima dotične države članice na temelju Uredbe (EU) …/…[++]. Posebno, države članice osiguravaju da njihova nadležna tijela na temelju ove Direktive obavješćuju Nadzorni forum osnovan na temelju članka 32. stavka 1. Uredbe (EU) …/…[++] pri izvršavanju svojih nadzornih ovlasti i ovlasti izvršavanja usmjerenih na osiguravanje usklađenosti ključnog subjekta koji je određen kao kritična treća strana pružatelj IKT usluga na temelju članka 31. (EU) …/….[++] s ovom Direktivom.

[+] SL: molimo u tekst umetnuti broj Direktive iz dokumenta PE-CONS 51/22 (2020/0365(COD)).

[++] SL: molimo u tekst umetnuti broj Uredbe iz dokumenta PE-CONS 41/22 (2020/0266(COD)).

Članak 33.

Nadzorne mjere i mjere izvršavanja u odnosu na važne subjekte

1. Kada dobiju dokaz, naznaku ili informaciju da važan subjekt navodno ne poštuje ovu Direktivu, a posebno njezine članke 21. i 23., države članice osiguravaju da nadležna tijela, ako je potrebno, poduzmu *ex post* nadzorne mjere. Države članice osiguravaju da su te mjere učinkovite, proporcionalne i odvraćajuće, uzimajući u obzir okolnosti svakog pojedinačnog slučaja.

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

   (a) inspekcije na lokaciji i neizravni *ex post* nadzor, koji provode osposobljeni stručnjaci;

   (b) ciljane revizije sigurnosti koje provodi neovisno tijelo ili nadležno tijelo;

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

(d) zahtjeve za informacije potrebne za *ex post* ocjenjivanje mjera upravljanja kibersigurnosnim rizicima koje je donio dotični subjekt, uključujući dokumentirane kibersigurnosne politike, te usklađenosti s obvezom dostavljanja informacija nadležnim tijelima u skladu s člankom 27.;

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

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

Ciljane revizije sigurnosti iz prvog podstavka točke (b) temelje se na procjenama rizika koje provodi nadležno tijelo ili subjekt revizije, ili na drugim dostupnim informacijama u vezi s rizikom.

Rezultati svake ciljane revizije sigurnosti stavljaju se na raspolaganje nadležnom tijelu. Troškove takve ciljane revizije sigurnosti koju provodi neovisno tijelo plaća subjekt nad kojim se provodi revizija, osim u propisno opravdanim slučajevima u kojima nadležno tijelo odluči drugačije.

3. Pri izvršavanju svojih ovlasti iz stavka 2. točkama (d), (e) ili (f), nadležna tijela navode svrhu zahtjeva i pobliže određuju tražene informacije.

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

(a) izdavati upozorenja o povredama ove Direktive od strane dotičnih subjekata;

(b) donositi obvezujuće upute ili nalog kojim se od dotičnih subjekata zahtijeva da uklone utvrđene nedostatke ili povredu ove Direktive;

(c) naložiti dotičnim subjektima da prestanu s postupanjem kojim se povređuje ova Direktiva i da ne ponavljaju takvo postupanje;

(d) naložiti dotičnim subjektima da osiguraju da su njihove mjere upravljanja kibersigurnosnim rizicima u skladu s obvezama iz članka 21. ili da ispune obveze izvješćivanja iz članka 23. na utvrđeni način i u utvrđenom roku;

(e) naložiti dotičnim subjektima da obavijeste fizičke ili pravne osobe u odnosu na koje pružaju usluge ili obavljaju djelatnosti 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 dotičnim subjektima da u razumnom roku provedu preporuke dane na temelju revizije sigurnosti;

(g) naložiti dotičnim subjektima da objave aspekte povrede ove Direktive na određeni način;

(h) izreći ili zahtijevati da relevantna tijela ili sudovi u skladu s nacionalnim pravom izreknu upravnu novčanu kaznu u skladu s člankom 34. uz sve mjere iz točaka od (a) do (g) ovog stavka.

5. Članak 32. stavci 6., 7. i 8. primjenjuju se *mutatis mutandis* na nadzorne mjere i mjere izvršavanja predviđene ovim člankom za važne subjekte.

6. Države članice osiguravaju da njihova nadležna tijela na temelju ove Direktive surađuju s relevantnim nadležnim tijelima dotične države članice na temelju Uredbe (EU) …/…[+]. Posebno, države članice osiguravaju da njihova nadležna tijela na temelju ove Direktive obavješćuju Nadzorni forum osnovan na temelju članka 32. stavka 1. Uredbe (EU) …/…[+] pri izvršavanju svojih nadzornih ovlasti i ovlasti izvršavanja usmjerenih na osiguravanje usklađenosti važnog subjekta koji je određen kao kritična treća strana pružatelj IKT usluga na temelju članka 31. (EU) …/….[+] s ovom Direktivom.

[+] SL: molimo u tekst umetnuti broj Uredbe iz dokumenta PE-CONS 41/22 (2020/0266(COD)).

Članak 34.

Opći uvjeti za izricanje upravnih novčanih kazni ključnim i važnim subjektima

1. Države članice osiguravaju da su upravne novčane kazne izrečene ključnim i važnim subjektima u skladu s ovim člankom u pogledu povreda ove Direktive učinkovite, proporcionalne i odvraćajuće, uzimajući u obzir okolnosti svakog pojedinog slučaja.

2. Upravne novčane kazne izriču se dodatno uz sve mjere iz članka 32. stavka 4. točaka od (a) do (h), članka 32. stavka 5. i članka 33. stavka 4. točaka od (a) do (g).

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 32. stavku 7.

4. Države članice osiguravaju da u slučaju da povrijede članak 21. ili članak 23. ključni subjekti podliježu, u skladu sa stavcima 2. i 3. ovog članka, upravnim novčanim kaznama u najvećem iznosu od najmanje 10 000 000 EUR ili u najvećem iznosu od najmanje 2 % ukupnog godišnjeg prometa na svjetskoj razini u prethodnoj financijskoj godini poduzeća kojem pripada ključni subjekt, ovisno o tome koji je iznos veći.

5. Države članice osiguravaju da u slučaju da povrijede članak 21. ili članak 23. važni subjekti podliježu, u skladu sa stavcima 2. i 3. ovog članka, upravnim novčanim kaznama u najvećem iznosu od najmanje 7 000 000 EUR ili u najvećem iznosu od najmanje 1,4 % ukupnog godišnjeg prometa na svjetskoj razini u prethodnoj financijskoj godini poduzeća kojem pripada važni subjekt, ovisno o tome koji je iznos veći.

6. Države članice mogu predvidjeti ovlast izricanja periodičnih penala kako bi se ključni ili važni subjekt prisililo da prestane s povredom ove Direktive u skladu s prethodnom odlukom nadležnog tijela.

7. Ne dovodeći u pitanje ovlasti nadležnih tijela u skladu s člancima 32. i 33., svaka država članica može utvrditi pravila o tome mogu li se i u kojoj mjeri subjektima javne uprave izreći upravne novčane kazne.

8. Ako pravnim sustavom pojedine države članice nisu predviđene upravne novčane kazne, ta država članica osigurava da se ovaj članak primjenjuje na način da novčanu kaznu pokreće nadležno tijelo, a izriču je nadležni nacionalni sudovi, osiguravajući pritom da su ta pravna sredstva djelotvorna i imaju jednakovrijedan učinak kao upravne novčane kazne koje izriču nadležna tijela. U svakom slučaju novčane kazne koje se izriču moraju biti učinkovite, proporcionalne i odvraćajuće. Država članica najkasnije do … [21 mjesec od dana stupanja na snagu ove Uredbe] obavješćuje Komisiju o svojim zakonodavnim odredbama koje donese u skladu s ovim stavkom te, bez odgode, o svim daljnjim izmjenama tih zakonodavnih odredbi ili izmjeni koja na njih utječe.

Članak 35.

Povrede koje uključuju povredu osobnih podataka

1. Ako nadležna tijela tijekom nadzora ili izvršavanja saznaju da povreda obveza utvrđenih u člancima 21. i 23. ove Direktive koju je počinio ključni ili važni subjekt može uključivati povredu osobnih podataka iz članka 4. stavka 12. Uredbe (EU) 2016/679 o kojoj se izvješćuje na temelju članka 33. te uredbe, ta nadležna tijela bez nepotrebne odgode obavješćuju nadzorna tijela iz članaka 55. i 56. te uredbe.

2. Ako nadzorna tijela kako su utvrđena u člancima 55. i 56. Uredbe (EU) 2016/679 izreknu upravnu novčanu kaznu u skladu s člankom 58. stavkom 2. točkom (i) te uredbe, nadležna tijela ne smiju izreći upravnu novčanu kaznu na temelju članka 34. ove Direktive za povredu iz stavka 1. ovog članka koja proizlazi iz istog postupanja koje je predmet upravne novčane kazne na temelju članka 58. stavka 2. točke (i) Uredbe (EU) 2016/679. Međutim, nadležna tijela mogu izreći mjere izvršavanja predviđene u članku 32. stavku 4. točkama od (a) do (h), članku 32. stavku 5. i članku 33. stavku 4. točkama od (a) do (g) ove Direktive.

3. Ako je nadzorno tijelo nadležno na temelju Uredbe (EU) 2016/679 osnovano u državi članici različitoj od one u kojoj je osnovano nadležno tijelo, nadležno tijelo obavještava nadzorno tijelo osnovano u svojoj vlastitoj državi članici o potencijalnoj povredi podataka iz stavka 1.

Članak 36.

Sankcije

Države članice utvrđuju pravila o sankcijama koje se primjenjuju na kršenja nacionalnih mjera donesenih na temelju ove Direktive i poduzimaju sve potrebne mjere radi osiguranja njihove provedbe. Predviđene sankcije moraju biti učinkovite, proporcionalne i odvraćajuće. Države članice do …[24 mjeseca nakon datuma stupanja na snagu ove Direktive] obavješćuju Komisiju o tim pravilima i tim mjerama te je bez odgode obavješćuju o svim naknadnim izmjenama koje na njih utječu.

Članak 37.

Uzajamna pomoć

1. Ako subjekt pruža usluge u više od jedne države članice ili pruža usluge u jednoj ili više država članica, a njegovi se 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 mjere ili mjere izvršavanja u državi članici preko jedinstvene kontaktne točke obavješćuju nadležna tijela u drugim dotičnim državama članicama o poduzetim nadzornim mjerama i mjerama izvršavanja te se savjetuju s njima;

(b) nadležno tijelo može zatražiti od drugog nadležnog tijela da poduzme nadzorne mjere ili mjere izvršavanja;

(c) nakon primitka potkrijepljenog zahtjeva drugog nadležnog tijela nadležno tijelo pruža tom drugom nadležnom tijelu uzajamnu pomoć razmjernu vlastitim resursima kako bi se nadzorne mjere ili mjere izvršavanja mogle provesti na djelotvoran, učinkovit i dosljedan način.

Uzajamna pomoć iz prvog podstavka točke (c) može obuhvaćati zahtjeve za informacije i nadzorne mjere, uključujući zahtjeve za provođenje inspekcija na lokaciji ili neizravnog nadzora ili ciljanih revizija sigurnosti. Nadležno tijelo kojem je upućen zahtjev za pomoć ne smije odbiti taj zahtjev osim u slučaju da se utvrdi da to tijelo nema nadležnost za pružanje zatražene pomoći, da zatražena pomoć nije razmjerna nadzornim zadaćama nadležnog tijela ili da se zahtjev odnosi na informacije ili uključuje aktivnosti koje bi, u slučaju da se otkriju ili provedu, bile suprotne osnovnim interesima nacionalne sigurnosti, javne sigurnosti ili obrane države članice. Prije odbijanja takvog zahtjeva nadležno tijelo savjetuje se s drugim dotičnim nadležnim tijelima te, na zahtjev jedne od dotičnih država članica, Komisijom i ENISA-om.

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

Poglavlje VIII.
Delegirani i provedbeni akti

Članak 38.

Izvršavanje delegiranja ovlasti

1. Ovlast za donošenje delegiranih akata dodjeljuje se Komisiji podložno uvjetima utvrđenima u ovom članku.

2. Ovlast za donošenje delegiranih akata iz članka 24. stavka 2. dodjeljuje se Komisiji na razdoblje od pet godina počevši od … [datuma stupanja na snagu ove Direktive].

3. Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 24. stavka 2. Odlukom o opozivu prekida se delegiranje ovlasti koje je u njoj navedeno. Opoziv počinje proizvoditi učinke sljedećeg dana od dana objave spomenute odluke u *Službenom listu Europske unije* ili na kasniji dan naveden u spomenutoj odluci. On ne utječe na valjanost delegiranih akata koji su već na snazi.

4. Prije donošenja delegiranog akta Komisija se savjetuje sa stručnjacima koje je imenovala svaka država članica u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.

5. Čim donese delegirani akt, Komisija ga istodobno priopćuje Europskom parlamentu i Vijeću.

6. Delegirani akt donesen na temelju članka 24. stavka 2. stupa na snagu samo ako ni Europski parlament ni Vijeće u roku od dva mjeseca od priopćenja tog akta Europskom parlamentu i Vijeću na njega ne podnesu prigovor ili ako su prije isteka tog roka i Europski parlament i Vijeće obavijestili Komisiju da neće podnijeti prigovore. Taj se rok produljuje za dva mjeseca na inicijativu Europskog parlamenta ili Vijeća.

Članak 39.

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.

Poglavlje IX.
Završne odredbe

Članak 40.

Preispitivanje

Do … [57 mjeseci od datuma stupanja na snagu ove Direktive] i svakih 36 mjeseci nakon toga, Komisija preispituje funkcioniranje ove Direktive te o tome izvješćuje Europski parlament i Vijeće. U izvješću se posebno ocjenjuje relevantnost veličine dotičnih subjekata, te sektora, podsektora i vrsta subjekata iz priloga I. i II. za funkcioniranje gospodarstva i društva u pogledu kibersigurnosti. U tu svrhu te u cilju daljnjeg unapređivanja strateške i operativne suradnje, Komisija uzima u obzir izvješća skupine za suradnju i mreže CSIRT-ova o iskustvu stečenom na strateškoj i operativnoj razini. Uz to izvješće prilaže se, prema potrebi, zakonodavni prijedlog.

Članak 41.

Prenošenje

1. Države članice do … [21 mjeseca nakon dana stupanja na snagu ove Direktive] donose i objavljuju mjere potrebne radi usklađivanja s ovom Direktivom. One o tome odmah obavješćuju Komisiju.

   One primjenjuju te mjere od … [jedan dan nakon datuma iz prvog podstavka].

2. Kada države članice donose mjere iz stavka 1, one sadržavaju upućivanje na ovu Direktivu ili se na nju upućuje prilikom njihove službene objave. Načine tog upućivanja određuju države članice.

Članak 42.

Izmjena Uredbe (EU) br. 910/2014

U Uredbi (EU) br. 910/2014 članak 19. briše se s učinkom od … [datum iz članka 41. stavka 1. drugog podstavka ove Direktive].

Članak 43.

Izmjena Direktive (EU) 2018/1972

U Direktivi (EU) 2018/1972 članci 40. i 41. brišu se s učinkom od … [datum iz članka 41. stavka 1. drugog podstavka ove Direktive].

Članak 44.

Stavljanje izvan snage

Direktiva (EU) 2016/1148 stavlja se izvan snage s učinkom od … [datum iz članka 41. stavka 1. drugog podstavka ove Direktive].

Upućivanja na direktivu stavljenu izvan snage smatraju se upućivanjima na ovu Direktivu i čitaju se u skladu s korelacijskom tablicom iz Priloga III.

Članak 45.

Stupanje na snagu

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

Članak 46.

Adresati

Ova je Direktiva upućena državama članicama.

Sastavljeno u Strasbourgu

Za Europski parlament	*Za Vijeće*
Predsjednica	*Predsjednik/Predsjednica*

PRILOG I

SEKTORI VISOKE KRITIČNOSTI

Sektor	Podsektor	Vrsta subjekta
1. Energetika	(a) električna energija	– elektroenergetska poduzeća iz članka 2. točke 57. Direktive (EU) 2019/944 Europskog parlamenta i Vijeća[1], koja obavljaju funkciju „opskrbe” iz članka 2. točke 12. te direktive
		– operatori distribucijskog sustava kako su definirani u članku 2. točki 29. Direktive (EU) 2019/944
		– operatori prijenosnog sustava kako su definirani u članku 2. točki 35. Direktive (EU) 2019/944
		– proizvođači kako su definirani u članku 2. točki 38. Direktive (EU) 2019/944
		– nominirani operatori tržišta električne energije kako su definirani u članku 2. točki 8. Uredbe (EU) 2019/943 Europskog parlamenta i Vijeća[2]

[1] 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.).

[2] Uredba (EU) 2019/943 Europskog parlamenta i Vijeća od 5. lipnja 2019. o unutarnjem tržištu električne energije (SL L 158, 14.6.2019., str. 54.).

Sektor	Podsektor	Vrsta subjekta
		– sudionici na tržištu kako su definirani u članku 2. točki 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 – operatori mjesta za punjenje koji su odgovorni za upravljanje i rad mjesta za punjenje kojim se krajnjim korisnicima pruža usluga opskrbe, među ostalim u ime i za račun pružatelja usluga mobilnosti
	(b) centralizirano grijanje i hlađenje	– operator sustava centraliziranog grijanja ili centraliziranog hlađenja kako je definirano u članku 2. točki 19. Direktive (EU) 2018/2001 Europskog parlamenta i Vijeća[1]
	(c) nafta	– operatori naftovoda
		– operatori proizvodnje nafte, rafinerija i tvornica nafte te njezina skladištenja i prijenosa
		– središnja tijela za zalihe kako su definirana u članku 2. točki (f) Direktive Vijeća 2009/119/EZ[2]

[1] 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.).

[2] 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.).

Sektor	Podsektor	Vrsta subjekta
	(d) plin	– poduzeća za opskrbu kako su definirana u članku 2. točki 8. Direktive 2009/73/EZ Europskog parlamenta i Vijeća[1]
		– operatori distribucijskog sustava kako su definirani u članku 2. točki 6. Direktive 2009/73/EZ
		– operatori transportnog sustava kako su definirani u članku 2. točki 4. Direktive 2009/73/EZ
		– operatori sustava skladišta plina kako su definirani u članku 2. točki 10. Direktive 2009/73/EZ
		– operatori terminala za UPP kako su definirani u članku 2. točki 12. Direktive 2009/73/EZ
		– poduzeća za prirodni plin kako su definirana u članku 2. točki 1. Direktive 2009/73/EZ
		– operatori postrojenja za rafiniranje i obradu prirodnog plina
	(e) vodik	– operatori proizvodnje, skladištenja i prijenosa vodika

[1] 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.).

Sektor		Podsektor		Vrsta subjekta	
2.	Promet	(a)	zračni promet	–	zračni prijevoznici kako su definirani u članku 4. točki 3. Uredbe (EZ) br. 300/2008 koji se upotrebljavaju u komercijalne svrhe
				–	upravna tijela zračne luke kako su definirana u članku 2. točki 2. Direktive 2009/12/EZ Europskog parlamenta i Vijeća[1], zračne luke kako su definirane u članku 2. točki 1. te direktive, uključujući osnovne zračne luke navedene u odjeljku 2. Priloga II. Uredbi (EU) br. 1315/2013 Europskog parlamenta i Vijeća[2] te tijela koja upravljaju pomoćnim objektima u zračnim lukama
				–	operatori kontrole upravljanja prometom koji pružaju usluge kontrole zračnog prometa (ATC) kako su definirani u članku 2. točki 1. Uredbe (EZ) br. 549/2004 Europskog parlamenta i Vijeća[3]

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

[2] Uredba (EU) 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.).

[3] 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.).

Sektor	Podsektor	Vrsta subjekta
	(b) željeznički promet	– upravitelji infrastrukture kako su definirani u članku 3. točki 2. Direktive 2012/34/EU Europskog parlamenta i Vijeća[1]
		– željeznički prijevoznici kako su definirani u članku 3. točki 1. Direktive 2012/34/EU, među ostalim i operatori uslužnih objekata kako su definirani u članku 3. točki 12. te direktive
	(c) vodeni promet	– kompanije za prijevoz putnika unutarnjim plovnim putovima, morem i duž obale kako su definirane za pomorski promet u Prilogu I. Uredbi (EZ) br. 725/2004 Europskog parlamenta i Vijeća[2], ne uključujući pojedinačna plovila kojima upravljaju te kompanije
		– upravljačka tijela luka kako su definirane u članku 3. točki 1. Direktive 2005/65/EZ Europskog parlamenta i Vijeća[3], uključujući njihove luke kako su definirane u članku 2. točki 11. Uredbe (EZ) br. 725/2004 te subjekti koji upravljaju postrojenjima i opremom u lukama
		– služba za nadzor i upravljanje pomorskim prometom (VTS) kako je definirana u članku 3. točki (o) Direktive 2002/59/EZ Europskog parlamenta i Vijeća[4]

[1] 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.).

[2] 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.).

[3] 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.).

[4] 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.).

Sektor	Podsektor	Vrsta subjekta
	(d) cestovni promet	– tijela nadležna za ceste kako su definirana u članku 2. točki 12. Delegirane uredbe Komisije (EU) 2015/962[1] odgovorna za kontrolu upravljanja prometom, osim javnih subjekata kojima upravljanje prometom ili rad inteligentnih prometnih sustava nisu ključni dio njihove opće djelatnosti
		– operatori inteligentnih prometnih sustava kako su definirani u članku 4. točki 1. Direktive 2010/40/EU Europskog parlamenta i Vijeća[2]
3. Bankarstvo		kreditne institucije kako su definirane u članku 4. točki 1. Uredbe (EU) br. 575/2013 Europskog parlamenta i Vijeća[3]
4. Infrastruktura financijskog tržišta		– operatori mjestâ trgovanja kako su definirani u članku 4. točki 24. Direktive 2014/65/EU Europskog parlamenta i Vijeća[4]
		– središnje druge ugovorne strane (CCP-i) kako su definirane u članku 2. točki 1. Uredbe (EU) br. 648/2012 Europskog parlamenta i Vijeća[5]

[1] 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.).

[2] 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.).

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

[4] 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.).

[5] 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.).

Sektor		Podsektor	Vrsta subjekta
5.	Zdravlje		– pružatelji zdravstvene zaštite kako su definirani u članku 3. točki (g) Direktive 2011/24/EU Europskog parlamenta i Vijeća[1]
			– referentni laboratoriji EU-a iz članka 15. Uredbe (EU) …/… Europskog parlamenta i Vijeća[2+]
			– subjekti koji obavljaju djelatnosti istraživanja i razvoja lijekova kako su definirani u članku 1. točki 2. Direktive 2001/83/EZ Europskog parlamenta i Vijeća[3] – 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 zdravlja”) u smislu članka 22. Uredbe (EU) 2022/123 Europskog parlamenta i Vijeća[4]

[1] 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.).

[2] Uredba EU …/… Europskog parlamenta i Vijeća od ... o ozbiljnim prekograničnim prijetnjama zdravlju i o stavljanju izvan snage Odluke br. 1082/2013/EU (SL L …, …, str. …).

[+] SL: molimo u tekst umetnuti broj uredbe iz dokumenta PE-CONS 40/22 (2020/0322(COD)), a u bilješku umetnuti broj, datum i upućivanje na SL za tu uredbu.

[3] 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.).

[4] Uredba (EU) 2022/123 Europskog parlamenta od 25. siječnja 2022. i Vijeća o pojačanoj ulozi Europske agencije za lijekove u pripravnosti za krizne situacije i upravljanju njima u području lijekova i medicinskih proizvoda (SL L 20, 31.1.2022., str. 1).

Sektor	Podsektor	Vrsta subjekta
6. Voda za piće		dobavljači i distributeri vode namijenjene za ljudsku potrošnju kako je definirana u članku 2. točki 1. podtočki (a) Direktive (EU) 2020/2184 Europskog parlamenta i Vijeća[1], isključujući distributere kojima distribucija vode za ljudsku potrošnju nije ključni dio njihove općenite djelatnosti distribucije druge robe i proizvoda
7. Otpadne vode		poduzeća koja prikupljaju, odlažu ili pročišćavaju komunalne otpadne vode, otpadne vode iz kućanstva ili industrijske otpadne vode kako su definirane u članku 2. točkama od 1., 2., i 3. Direktive Vijeća 91/271/EEZ[2], ali isključujući poduzeća kojima prikupljanje, odlaganje ili pročišćavanje komunalnih otpadnih voda, otpadnih voda iz kućanstva ili industrijskih otpadnih voda nije ključni dio njihove općenite djelatnosti

[1] Direktiva (EU) 2020/2184 Europskog parlamenta i Vijeća od 16. prosinca 2020. o kvaliteti vode namijenjene za ljudsku potrošnju (SL L 435, 23.12.2020., str. 1.).

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

Sektor		Podsektor	Vrsta subjekta
8.	Digitalna infrastruktura		– pružatelji središta za razmjenu internetskog prometa
			– pružatelji usluga DNS-a, osim operatora korijenskih poslužitelja naziva
			– registri naziva vršnih domena
			– pružatelji usluga računalstva u oblaku
			– pružatelji usluga podatkovnog centra
			– pružatelji mreže za isporuku sadržaja
			– pružatelji usluga povjerenja
			– pružatelji javnih elektroničkih komunikacijskih mreža
			– pružatelji javno dostupnih elektroničkih komunikacijskih usluga
9.	Upravljanje uslugama IKT-a (B2B)		– pružatelji upravljanih usluga – pružatelji upravljanih sigurnosnih usluga

Sektor		Podsektor	Vrsta subjekta
10.	Javna uprava		– subjekti središnje državne uprave kako ih je definirala država članica u skladu s nacionalnim pravom
			– subjekti javne uprave na regionalnoj razini kako ih je definirala država članica u skladu s nacionalnim pravom
11.	Svemir		operatori zemaljske infrastrukture, koji su u vlasništvu, kojima upravljaju i koje vode države članice ili privatne strane te koji podupiru pružanje usluga u svemiru, isključujući pružatelje javnih elektroničkih komunikacijskih mreža

PRILOG II.

Drugi kritični sektori

Sektor		Podsektor	Vrsta subjekta
1.	Poštanske i kurirske usluge		pružatelji poštanskih usluga kako su definirani u članku 2. točki 1.a Direktive 97/67/EZ, uključujući pružatelje kurirskih usluga
2.	Gospodarenje otpadom		poduzeća koja se bave gospodarenjem otpadom kako je definirano u članku 3. točki 9. Direktive 2008/98/EZ Europskog parlamenta i Vijeća[1], isključujući poduzeća kojima gospodarenje otpadom nije glavna gospodarska djelatnost
3.	Izrada, proizvodnja i distribucija kemikalija		poduzeća koja se bave izradom tvari te distribucijom tvari ili mješavina kako su definirana u članku 3. točkama 9. i 14. Uredbe (EZ) br. 1907/2006 Europskog parlamenta i Vijeća[2] i poduzeća koja se bave proizvodnjom proizvoda kako su definirana u članku 3. točki 3. te uredbe, iz tvari ili mješavina

[1] 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.).

[2] Uredba (EZ) br. 1907/2006 Europskog parlamenta i Vijeća od 18. prosinca 2006. o registraciji, evaluaciji, autorizaciji i ograničavanju kemikalija (REACH), o osnivanju Europske agencije za kemikalije i 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 te Direktiva Komisije 91/155/EEZ, 93/67/EEZ, 93/105/EZ i 2000/21/EZ (SL L 396, 30.12.2006., str. 1.).

Sektor		Podsektor		Vrsta subjekta
4.	Proizvodnja, prerada i distribucija hrane			poduzeća za poslovanje s hranom kako su definirana u članku 3. točki 2. Uredbe (EZ) br. 178/2002 Europskog parlamenta i Vijeća[1] 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 kako su definirani u članku 2. točki 1. Uredbe (EU) 2017/745 Europskog parlamenta i Vijeća[2] i subjekti koji proizvode in vitro dijagnostičke medicinske proizvode kako su definirani u članku 2. točki 2. Uredbe (EU) 2017/746 Europskog parlamenta i Vijeća[3], osim subjekata koji proizvode medicinske proizvode navedene u Prilogu I. točki 5. petoj alineji ove Direktive.
		(b)	proizvodnja računala te elektroničkih i optičkih proizvoda	poduzeća koja obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 26. NACE Rev. 2

[1] 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.).

[2] 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.).

[3] 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.).

Sektor	Podsektor	Vrsta subjekta
	(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 platforma za usluge društvenih mreža
7. Istraživanje		Istraživačke organizacije

PRILOG III.

KORELACIJSKA TABLICA

Direktiva (EU) 2016/1148	Ova Direktiva
članak 1. stavak 1.	članak 1. stavak 1.
članak 1. stavak 2.	članak 1. stavak 2.
članak 1. stavak 3.	-
članak 1. stavak 4.	članak 2. stavak 12.
članak 1. stavak 5.	članak 2. stavak 13.
članak 1. stavak 6.	članak 2. stavci 6. i 11.
članak 1. stavak 7.	članak 4.
članak 2.	članak 2. stavak 14.
članak 3.	članak 5.
članak 4.	članak 6.
članak 5.	-
članak 6.	-
članak 7. stavak 1.	članak 7. stavci 1. i 2.
članak 7. stavak 2.	članak 7. stavak 4.
članak 7. stavak 3.	članak 7. stavak 3.
članak 8. stavci od 1. do 5.	članak 8. stavci od 1. do 5.
članak 8. stavak 6.	članak 13. stavak 4.
članak 8. stavak 7.	članak 8. stavak 6.
članak 9. stavci 1., 2. i 3.	članak 10. stavci 1., 2. i 3.

Direktiva (EU) 2016/1148	Ova Direktiva
članak 9. stavak 4.	članak 10. stavak 9.
članak 9. stavak 5.	članak 10. stavak 10.
članak 10. stavak 1., stavak 2. i stavak 3. prvi podstavak	članak 13. stavci 1., 2. i 3.
članak 10. stavak 3. drugi podstavak	članak 23. stavak 9.
članak 11. stavak 1.	članak 14. stavci 1. i 2.
članak 11. stavak 2.	članak 14. stavak 3.
članak 11. stavak 3.	članak 14. stavak 4. prvi podstavak točke od (a) do (q) i točka (s) i stavak 7.
članak 11. stavak 4.	članak 14. stavak 4. prvi podstavak točka (r) i drugi podstavak
članak 11. stavak 5.	članak 14. stavak 8.
članak 12. stavci od 1. do 5.	članak 15. stavci od 1. do 5.
članak 13.	članak 17.
članak 14. stavci 1. i 2.	članak 21. stavci od 1. do 4.
članak 14. stavak 3.	članak 23. stavak 1.
članak 14. stavak 4.	članak 23. stavak 3.
članak 14. stavak 5.	članak 23. stavci 5., 6. i 8.
članak 14. stavak 6.	članak 23. stavak 7.
članak 14. stavak 7.	članak 23. stavak 11.
članak 15. stavak 1.	članak 31. stavak 1.
članak 15. stavak 2. prvi podstavak točka (a)	članak 32. stavak 2. točka (e)
članak 15. stavak 2. prvi podstavak točka (b)	članak 32. stavak 2. točka (g)
članak 15. stavak 2. drugi podstavak	članak 32. stavak 3.
članak 15. stavak 3.	članak 32. stavak 4. točka (b)

Direktiva (EU) 2016/1148	Ova Direktiva
članak 15. stavak 4.	članak 31. stavak 3.
članak 16. stavci 1. i 2.	članak 21. stavci od 1. do 4.
članak 16. stavak 3.	članak 23. stavak 1.
članak 16. stavak 4.	članak 23. stavak 3.
članak 16. stavak 5.	-
članak 16. stavak 6.	članak 23. stavak 6.
članak 16. stavak 7.	članak 23. stavak 7.
članak 16. stavci 8. i 9.	članak 21. stavak 5. i članak 23. stavak 11.
članak 16. stavak 10.	-
članak 16. stavak 11.	članak 2. stavci 1., 2. i 3.
članak 17. stavak 1.	članak 33. stavak 1.
članak 17. stavak 2. točka (a)	članak 32. stavak 2. točka (e)
članak 17. stavak 2. točka (b)	članak 32. stavak 4. točka (b)
članak 17. stavak 3.	članak 37. stavak 1. točke (a) i (b)
članak 18. stavak 1.	članak 26. stavak 1. točka (b) i stavak 2.
članak 18. stavak 2.	članak 26. stavak 3.
članak 18. stavak 3.	članak 26. stavak 4.
članak 19.	članak 25.
članak 20.	članak 30.
članak 21.	članak 36.
članak 22.	članak 39.
članak 23.	članak 40.
članak 24.	-

Direktiva (EU) 2016/1148	Ova Direktiva
članak 25.	članak 41.
članak 26.	članak 45.
članak 27.	članak 46.
Prilog I. točka 1.	članak 11. stavak 1.
Prilog I. točka 2. podtočka (a) podtočke od i. do iv.	članak 11. stavak 2. točke od (a) do (d)
Prilog I. točka 2. podtočka (a) podtočka v.	članak 11. stavak 2. točka (f)
Prilog I. točka 2. podtočka (b)	članak 11. stavak 4.
Prilog I. točka 2. podtočka (c) podtočke i. i ii.	članak 11. stavak 5. točka (a)
Prilog II.	Prilog I.
Prilog III. točke 1. i 2.	Prilog II. točka 6.
Prilog III. točka 3.	Prilog I. točka 8.