



Odbor za unutarnje tržište i zaštitu potrošača

2020/0359(COD)

14.7.2021

MIŠLJENJE

Odbora za unutarnje tržište i zaštitu potrošača

upućeno Odboru za industriju, istraživanje i energetiku

o Prijedlogu direktive Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Izvjestitelj za mišljenje: Morten Løkkegaard

PA_Legam

KRATKO OBRAZLOŽENJE

Izvjestitelj općenito pozdravlja zakonodavni prijedlog Direktive o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije (NIS 2). Izvjestitelj smatra da je u svijetu koji se sve više digitalizira sigurnost na internetu ključna za jamčenje sigurnog digitalnog okruženja i funkciranja jedinstvenog tržišta na kojem potrošači i gospodarski subjekti mogu slobodno djelovati.

Prijedlog NIS 2 znatno je unapređenje u odnosu na Direktivu (EU) 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (NIS 1). U njemu se navode ključni nedostaci Direktive NIS 1, kao što su niska razina kiberotpornosti poduzeća i sektora, kao i neujednačena otpornost te niska razina zajedničke informiranosti o stanju i odgovora na krizu u državama članicama i među njima. Izvjestitelj pozdravlja ambicije da se to ispravi s pomoću Direktive NIS 2.

Područje primjene

Izvjestitelj pozdravlja prošireno područje primjene Prijedloga NIS 2, a posebno uključivanje novih sektora, kao što je javna uprava. Izravan popis uključenih sektora i usluga zasigurno će smanjiti diskrecijsko pravo država članica u definiranju konkretnih subjekata koji podliježu Direktivi te će se time smanjiti rascjepkanost na jedinstvenom tržištu.

Za obuhvaćene sektore i usluge Komisija je predložila pravilo o veličini kao jedinstveni kriterij za određivanje subjekata koji bi bili obuhvaćeni područjem primjene Direktive. Taj kriterij nedvojbeno ima prednost osiguravanja pravne sigurnosti, uz istodobno smanjenje divergencija među državama članicama.

Međutim, iako pozdravlja prošireno sektorsko područje primjene, izvjestitelj smatra da bi taj opći kriterij trebalo kombinirati s procjenom kritičnosti subjekata u svakom sektoru. Time bi se omogućilo da srednji i veliki subjekti za koje se nakon procjene rizika utvrdi da imaju nisku razinu kritičnosti i ovisnosti o inače kritičnim subjektima ne budu obuhvaćeni područjem primjene Direktive.

Izvjestitelj naglašava da se to ne bi smjelo smatrati prostorom za različita tumačenja među državama članicama. Kako bi se osiguralo da se time ne poveća fragmentirana provedba među državama članicama, Komisiju se potiče da o navedenom aspektu izda jasne smjernice.

Naposljetku, iako pozdravlja isključivanje mikropoduzeća i malih poduzeća iz područja primjene, izvjestitelj smatra da postoji potreba za poticanjem njihova dobrovoljnog uključivanja jer su mikrosubjekti i mali subjekti isto izloženi kibernapadima i njihove su žrtve.

Koordinirani regulatorni okviri za kibersigurnost

Izvjestitelj pozdravlja poglavje u kojem se definiraju različiti elementi nacionalnih strategija za kibersigurnost i njihovih alata za upravljanje krizama. Predlaže se da države članice u okviru svoje nacionalne strategije za kibersigurnost donesu politiku kojom se promiče uporaba kriptografije i šifriranja, posebno kada je riječ o MSP-ovima.

Izvjestitelj pozdravlja činjenicu da je ENISA razvila europski registar ranjivosti, no smatra da

je važno da se pri registraciji poštuju povjerljivost poslovnih podataka i poslovne tajne te da se ne stvara nepotrebno opterećenje za subjekte.

Suradnja među državama članicama

Posebno je dobrodošla strukturiranija suradnja među državama članicama u okviru skupine za suradnju, mreže CSIRT-ova i novoosnovane skupine za incidente velikih razmjera u okviru Direktive NIS 2. Međutim, potrebno je osigurati veću razinu povjerenja i spremnosti na razmjenu informacija među državama članicama jer učinkovitost te suradnje ima ključnu ulogu u osiguravanju visoke razine kibersigurnosti u EU-u.

Imajući na umu navedeno stajalište, sastavljen je niz izmjena kako bi se ojačala uloga mreža. Konkretno, izvjestitelj smatra da je istorazinsko ocjenjivanje koristan način za povećanje zajedničkog povjerenja država članica te se slaže da bi ono trebalo imati ključnu ulogu u ocjenjivanju učinkovitosti politika kibersigurnosti pojedinačnih država članica.

Upravljanje kibersigurnosnim rizicima

Pozdravlja se proširenje procjene rizika na cijeli lanac opskrbe (članci 18. i 19.), no izvjestitelj naglašava da su potrebna pojašnjenja kako bi se dale jasne smjernice subjektima koji podliježu tom zahtjevu te državama članicama pri provedbi koordinirane procjene sigurnosnog rizika posebno kritičnih sektora ili lanaca opskrbe.

Obveze izvješćivanja

Izvjestitelj smatra da bi trebalo osigurati veću jasnoću određenih točaka revidirane Direktive, uglavnom u pogledu nekih obveza nametnutih poduzećima u okviru Direktive NIS 2. Izvjestitelj je nastojao smanjiti birokraciju i poduzećima olakšati usklajivanje s novim pravilima, imajući na umu konačni cilj, koji se odnosi na učinkovitost provedbe Direktive.

Izvjestitelj predlaže da se predloženi rok od 24 sata u kontekstu obveze izvješćivanja za prve obavijesti produži na 72 sata kako bi se poduzećima omogućilo da prije izvješćivanja efektivno odgovore na kibernapad koji je u tijeku. Nadalje, predlaže se brisanje svih upućivanja na obvezno obavješćivanje o takozvanim „potencijalnim incidentima”.

AMANDMANI

Odbor za unutarnje tržište i zaštitu potrošača poziva Odbor za industriju, istraživanje i energetiku da kao nadležni odbor uzme u obzir sljedeće amandmane:

Amandman 1
Prijedlog direktive
Uvodna izjava 5.

Tekst koji je predložila Komisija

(5) Sve one dovode do rascjepkanosti unutarnjeg tržišta i mogu štetno utjecati na njegovo funkcioniranje, posebno na prekogranično pružanje usluga i razinu otpornosti u području kibersigurnosti zbog primjene različitih normi. 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 lijekova i sankcija ključnih za učinkovito izvršavanje tih obveza. Stoga bi Direktivu (EU) 2016/1148 trebalo staviti izvan snage i zamijeniti ovom Direktivom.

Amandman 2 Prijedlog direktive Uvodna izjava 6.a (nova)

Tekst koji je predložila Komisija

Amandman 3 Prijedlog direktive Uvodna izjava 9.

Tekst koji je predložila Komisija

(9) Međutim, ovom Direktivom trebali bi biti obuhvaćeni i mali subjekti ili mikrosubjekti koji ispunjavaju određene kriterije koji upućuju na ključnu ulogu za gospodarstva ili društva država članica ili za određene sektore ili vrste usluga. Države

Izmjena

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

Izmjena

(6.a) Ovom Direktivom ne dovode se u pitanje pravila utvrđena pravom Unije o zaštiti osobnih podataka.

članice trebale bi biti odgovorne za sastavljanje popisa takvih subjekata i dostaviti ga Komisiji.

članice trebale bi biti odgovorne za sastavljanje popisa takvih subjekata i dostaviti ga Komisiji. *Komisija bi trebala pružiti jasne smjernice o kriterijima kojima se utvrđuje koji bi mali ili mikro subjekti bili kritični ili važni, posebno kada pružaju usluge u više država članica.*

Amandman 4
Prijedlog direktive
Uvodna izjava 10.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 5
Prijedlog direktive
Uvodna izjava 12.a (nova)

Tekst koji je predložila Komisija

Izmjena

(12.a) Proširenje područja primjene ove Direktive podrazumijeva uključivanje subjekata koji podliježu sektorskim propisima. Kako bi se izbjeglo svako regulatorno udvostručavanje ili opterećenje, Komisija bi trebala osigurati da su sektorski akti kojima se od ključnih ili važnih subjekata zahtijeva donošenje mjera za upravljanje kibersigurnosnim rizicima ili obavješćivanje o incidentima ili znatnim kiberprijetnjama u skladu s ovom Direktivom.

Amandman 6
Prijedlog direktive
Uvodna izjava 12.b (nova)

Tekst koji je predložila Komisija

Izmjena

(12.b) Komisija bi trebala objaviti jasne

smjernice uz ovu Direktivu kako bi pridonijela osiguravanju usklađenosti provedbe u državama članicama i izbjegavanju rascjepkanosti.

Amandman 7
Prijedlog direktive
Uvodna izjava 12.c (nova)

Tekst koji je predložila Komisija

Izmjena

(12.c) Komisija bi također trebala izdati smjernice za potporu državama članicama u pravilnoj provedbi odredaba o području primjene i za ocjenu proporcionalnosti obveza utvrđenih ovom Direktivom s obzirom na kritičnost subjekata obuhvaćenih područjem primjene, posebno kada se primjenjuju na subjekte sa složenim poslovnim modelima ili operativnim okruženjem, pri čemu subjekt može istodobno ispunjavati kriterije dodijeljene i ključnim i važnim subjektima, ili istodobno obavljati djelatnosti koje su dio područja primjene ove Direktive ili neke izvan područja primjene ove Direktive. U slučajevima kada subjekti svoju glavnu djelatnost obavljaju izvan područja primjene ove Direktive, ali neke druge sekundarne djelatnosti unutar područja primjene, odredbe bi se trebale primjenjivati samo na funkciju ili razinu jedinice unutar subjekta, koja je obuhvaćena područjem primjene ove Direktive.

Amandman 8
Prijedlog direktive
Uvodna izjava 14.

Tekst koji je predložila Komisija

Izmjena

(14) S obzirom na međupovezanost kibersigurnosti i fizičke sigurnosti subjekata, trebalo bi osigurati usklađen pristup između Direktive (EU) XXX/XXX

(14) S obzirom na međupovezanost kibersigurnosti i fizičke sigurnosti subjekata, trebalo bi osigurati usklađen pristup između Direktive (EU) XXX/XXX

Europskog parlamenta i Vijeća¹⁷ i ove Direktive. Kako bi se to postiglo, države članice trebale bi osigurati da se kritični i ekvivalentni subjekti iz Direktive (EU) XXX/XXX smatraju ključnim subjektima na temelju ove Direktive. Države članice trebale bi osigurati i da se njihovim strategijama za kibersigurnost osigurava okvir politike za bolju koordinaciju između nadležnog tijela na temelju ove Direktive i nadležnog tijela na temelju Direktive (EU) XXX/XXX u kontekstu razmjene informacija o incidentima i kiberprijetnjama te izvršavanja nadzornih zadaća. Tijela na temelju obiju direktiva trebala bi surađivati i razmjenjivati informacije, posebno u pogledu utvrđivanja kritičnih subjekata, kiberprijetnji, kibersigurnosnih rizika, incidenata koji utječu na kritične subjekte te kibersigurnosnih mjera koje ti subjekti poduzimaju. Na zahtjev nadležnih tijela iz Direktive (EU) XXX/XXX, nadležnim tijelima iz ove Direktive trebalo bi omogućiti izvršavanje nadzornih i provedbenih ovlasti nad ključnim subjektom koji je utvrđen kao kritičan. Oba tijela trebala bi surađivati i razmjenjivati informacije u tu svrhu.

¹⁷ [Upisati puni naslov i upućivanje na objavu u SL-u kada budu poznati.]

Amandman 9 Prijedlog direktive Uvodna izjava 15.

Tekst koji je predložila Komisija

(15) Vođenje i održavanje pouzdanog, otpornog i sigurnog sustava naziva domena (DNS) ključni su za očuvanje cjelovitosti interneta te njegov kontinuiran i stabilan rad, o kojem ovise digitalno gospodarstvo i društvo. Stoga bi se ova Direktiva trebala primjenjivati na sve pružatelje DNS usluga

Europskog parlamenta i Vijeća¹⁷ i ove Direktive. Kako bi se to postiglo, države članice trebale bi osigurati da se kritični i ekvivalentni subjekti iz Direktive (EU) XXX/XXX smatraju ključnim subjektima na temelju ove Direktive. Države članice trebale bi osigurati i da se njihovim **nacionalnim** strategijama za kibersigurnost osigurava okvir politike za bolju koordinaciju između nadležnog tijela na temelju ove Direktive i nadležnog tijela na temelju Direktive (EU) XXX/XXX u kontekstu **izješćivanja o incidentima**, razmjene informacija o **incidentima**, **izbjegnutim** incidentima i kiberprijetnjama te izvršavanja nadzornih zadaća. Tijela na temelju obiju direktiva trebala bi surađivati i razmjenjivati informacije, posebno u pogledu utvrđivanja kritičnih subjekata, kiberprijetnji, kibersigurnosnih rizika, incidenata koji utječu na kritične subjekte te kibersigurnosnih mjera koje ti subjekti poduzimaju. Na zahtjev nadležnih tijela iz Direktive (EU) XXX/XXX, nadležnim tijelima iz ove Direktive trebalo bi omogućiti izvršavanje nadzornih i provedbenih ovlasti nad ključnim subjektom koji je utvrđen kao kritičan. Oba tijela trebala bi surađivati i razmjenjivati informacije u tu svrhu.

¹⁷ [Upisati puni naslov i upućivanje na objavu u SL-u kada budu poznati.]

Izmjena

(15) Vođenje i održavanje pouzdanog, otpornog i sigurnog sustava naziva domena (DNS) ključni su za očuvanje cjelovitosti interneta te njegov kontinuiran i stabilan rad, o kojem ovise digitalno gospodarstvo, **unutarnje tržište** i društvo. Stoga bi se ova Direktiva trebala primjenjivati na sve

u lancu DNS prevođenja, uključujući operatore korijenskih poslužitelja naziva, poslužitelja naziva vršnih domena, mjerodavnih poslužitelja naziva za nazive domena i rekurzivnih prevoditelja.

pružatelje DNS usluga u lancu DNS prevođenja, uključujući operatore korijenskih poslužitelja naziva, poslužitelja naziva vršnih domena, mjerodavnih poslužitelja naziva za nazive domena i rekurzivnih prevoditelja, *te pružatelje usluga zaštite privatnosti i registracije proxy poslužitelja i brokere ili preprodavatelje domena te sve druge usluge koje su povezane s registracijom naziva domena.*

Amandman 10
Prijedlog direktive
Uvodna izjava 20.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 11
Prijedlog direkture
Uvodna izjava 23.

Tekst koji je predložila Komisija

(23) Nadležna tijela ili CSIRT-ovi trebali bi od subjekata primati obavijesti o incidentima na djelotvoran i učinkovit način. Zadaća jedinstvenih kontaktnih točaka trebala bi biti proslijedivanje obavijesti o incidentima jedinstvenim kontaktnim točkama drugih pogodjenih država članica. Kako bi se osigurala jedinstvena ulazna točka u svakoj državi članici, jedinstvene kontaktne točke **na razini tijela država članica** trebale bi primati relevantne informacije o incidentima koji se odnose na subjekte finansijskog sektora od nadležnih tijela iz Uredbe XXXX/XXXX koje bi, prema potrebi, trebale moći proslijediti relevantnim nacionalnim nadležnim tijelima ili CSIRT-ovima iz ove Direktive.

Amandman 12
Prijedlog direkture
Uvodna izjava 25.

Tekst koji je predložila Komisija

(25) **Kad** je riječ o osobnim podacima, CSIRT-ovi bi, u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća¹⁹ o osobnim podacima, u ime subjekta iz ove Direktive i na njegov zahtjev, trebali moći osigurati proaktivno pregledavanje mrežnih i informacijskih sustava koji se upotrebljavaju za pružanje njihovih usluga. Države članice trebale bi nastojati osigurati jednaku razinu tehničkih sposobnosti za sve sektorske CSIRT-ove. Države članice mogu zatražiti pomoć Agencije Europske unije za kibersigurnost (ENISA) u razvoju nacionalnih CSIRT-ova.

Izmjena

(23) Nadležna tijela ili CSIRT-ovi trebali bi od subjekata primati obavijesti o incidentima na **standardiziran**, djelotvoran i učinkovit način. Zadaća jedinstvenih kontaktnih točaka trebala bi biti proslijedivanje obavijesti o incidentima jedinstvenim kontaktnim točkama drugih pogodjenih država članica. Kako bi se osigurala jedinstvena ulazna točka u svakoj državi članici, jedinstvene kontaktne točke trebale bi primati relevantne informacije o incidentima koji se odnose na subjekte finansijskog sektora od nadležnih tijela iz Uredbe XXXX/XXXX koje bi, prema potrebi, trebale moći proslijediti relevantnim nacionalnim nadležnim tijelima ili CSIRT-ovima iz ove Direktive.

ova.

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

Amandman 13
Prijedlog direktive
Uvodna izjava 26.a (nova)

Tekst koji je predložila Komisija

Izmjena

(26.a) U okviru svojih nacionalnih strategija za kibersigurnost države članice trebale bi donositi politike o promicanju i integraciji inteligentnih sustava u sprečavanju i otkrivanju kibersigurnosnih incidenta i prijetnji. Države članice trebale bi, u skladu sa svojim nacionalnim strategijama za kibersigurnost, uspostaviti politike usmjerene na svijest o kibersigurnosti i kiberpismenost, s ciljem zaštite potrošača. Pri donošenju nacionalnih strategija kibersigurnosti države članice trebale bi osigurati okvire politika za rješavanje pitanja zakonitog pristupa informacijama.

Amandman 14
Prijedlog direktive
Uvodna izjava 27.

Tekst koji je predložila Komisija

Izmjena

(27) U skladu s Prilogom Preporuci Komisije (EU) 2017/1548 o koordiniranom odgovoru na kiberincidente i kiberkriže velikih razmjera („plan”)²⁰, incident velikih razmjera trebao bi značiti incident sa znatnim utjecajem na najmanje dvije države članice ili incident čiji učinci

(27) U skladu s Prilogom Preporuci Komisije (EU) 2017/1548 o koordiniranom odgovoru na kiberincidente i kiberkriže velikih razmjera („plan”)²⁰, incident velikih razmjera trebao bi značiti incident sa znatnim utjecajem na najmanje dvije države članice ili incident čiji učinci

premašuju sposobnost države članice da na njega odgovori. Ovisno o svojem uzroku i utjecaju, incidenti velikih razmjera mogu se proširiti i pretvoriti u prave krize koje onemogućavaju pravilno funkcioniranje unutarnjeg tržišta. S obzirom na širok opseg i, u većini slučajeva, prekograničnu prirodu takvih incidenata, države članice i relevantne institucije, tijela i agencije Unije trebali bi surađivati na tehničkoj, operativnoj i političkoj razini kako bi pravilno koordinirali odgovor u cijeloj Uniji.

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

Amandman 15 Prijedlog direktive Uvodna izjava 28.

Tekst koji je predložila Komisija

(28) Budući da iskorištavanje ranjivosti u mrežnim i informacijskim sustavima može uzrokovati zнатне poremećaje i štetu, brzo prepoznavanje i otklanjanje tih ranjivosti važan je čimbenik u smanjenju kibersigurnosnog rizika. Subjekti koji razvijaju takve sustave trebali bi stoga uspostaviti odgovarajuće postupke za otklanjanje ranjivosti kada ih se otkrije. Budući da ranjivosti često prepoznaju i prijavljuju (otkrivaju) treće strane (subjekti koji podliježu obvezi obavljanja), proizvođač ili pružatelj IKT proizvoda ili usluga trebao bi uspostaviti i postupke potrebne za primanje informacija o ranjivosti od trećih strana. U tom pogledu međunarodne norme ISO/IEC 30111 i ISO/IEC 29417 pružaju smjernice o postupanju s ranjivostima i njihovu otkrivanju. Kad je riječ o otkrivanju ranjivosti, posebno je važna koordinacija

premašuju sposobnost države članice da na njega odgovori, **čime se ugrožava unutarnje tržište**. Ovisno o svojem uzroku i utjecaju, incidenti velikih razmjera mogu se proširiti i pretvoriti u prave krize koje onemogućavaju pravilno funkcioniranje unutarnjeg tržišta. S obzirom na širok opseg i, u većini slučajeva, prekograničnu prirodu takvih incidenata, države članice i relevantne institucije, tijela i agencije Unije trebali bi surađivati na tehničkoj, operativnoj i političkoj razini kako bi pravilno koordinirali odgovor u cijeloj Uniji.

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

Izmjena

(28) Budući da iskorištavanje ranjivosti u mrežnim i informacijskim sustavima može uzrokovati zнатне poremećaje i štetu **poduzećima i potrošačima**, brzo prepoznavanje i otklanjanje tih ranjivosti važan je čimbenik u smanjenju kibersigurnosnog rizika. Subjekti koji razvijaju takve sustave trebali bi stoga uspostaviti odgovarajuće postupke za otklanjanje ranjivosti kada ih se otkrije. Budući da ranjivosti često prepoznaju i prijavljuju (otkrivaju) treće strane (subjekti koji podliježu obvezi obavljanja), proizvođač ili pružatelj IKT proizvoda ili usluga trebao bi uspostaviti i postupke potrebne za primanje informacija o ranjivosti od trećih strana. U tom pogledu međunarodne norme ISO/IEC 30111 i ISO/IEC 29417 pružaju smjernice o postupanju s ranjivostima i njihovu otkrivanju. Kad je riječ o otkrivanju

između subjekata koji podliježu obvezi obavlješčivanja i proizvođača ili pružatelja IKT proizvoda ili usluga. Koordinirano otkrivanje ranjivosti odvija se strukturiranim postupkom u okviru kojeg se ranjivosti prijavljuju organizacijama na način kojim se organizaciji omogućuje dijagnosticiranje i otklanjanje ranjivosti prije nego što se detaljne informacije o ranjivosti otkriju trećim stranama ili javnosti. Koordinirano otkrivanje ranjivosti trebalo bi obuhvaćati i koordinaciju između subjekta koji obavlješće i organizacije u pogledu vremena otklanjanja i objave ranjivosti.

ranjivosti, posebno je važna koordinacija između subjekata koji podliježu obvezi obavlješčivanja i proizvođača ili pružatelja IKT proizvoda ili usluga. Koordinirano otkrivanje ranjivosti odvija se strukturiranim postupkom u okviru kojeg se ranjivosti prijavljuju organizacijama na način kojim se organizaciji omogućuje dijagnosticiranje i otklanjanje ranjivosti prije nego što se detaljne informacije o ranjivosti otkriju trećim stranama ili javnosti. Koordinirano otkrivanje ranjivosti trebalo bi obuhvaćati i koordinaciju između subjekta koji obavlješće i organizacije u pogledu vremena otklanjanja i objave ranjivosti.

Amandman 16
Prijedlog direktive
Uvodna izjava 28.a (nova)

Tekst koji je predložila Komisija

Izmjena

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

Amandman 17
Prijedlog direktive
Uvodna izjava 30.

Tekst koji je predložila Komisija

Izmjena

(30) Pristup točnim i pravodobnim informacijama o ranjivostima koje utječu na IKT proizvode i usluge pridonosi boljem upravljanju kibersigurnosnim rizicima. U tom su pogledu izvori javno dostupnih informacija o ranjivostima važan alat za subjekte i njihove korisnike, ali i za nacionalna nadležna tijela i CSIRT-ove.

(30) Pristup točnim i pravodobnim informacijama o ranjivostima koje utječu na IKT proizvode i usluge pridonosi boljem upravljanju kibersigurnosnim rizicima. U tom su pogledu izvori javno dostupnih informacija o ranjivostima važan alat za subjekte i njihove korisnike, ali i za nacionalna nadležna tijela i CSIRT-ove.

Zbog toga bi ENISA trebala uspostaviti **registar ranjivosti** u **kojem** ključni i važni subjekti i njihovi dobavljači te subjekti koji nisu obuhvaćeni područjem primjene ove Direktive mogu dobrovoljno otkriti ranjivosti i pružiti informacije o ranjivostima koje korisnicima omogućuju poduzimanje odgovarajućih mjera ublažavanja.

Amandman 18
Prijedlog direktive
Uvodna izjava 31.

Tekst koji je predložila Komisija

(31) Iako slični registri ili baze podataka o ranjivosti postoje, na poslužitelju ih smještaju i vode subjekti koji nemaju poslovni nastan u Uniji. **Europski register ranjivosti** koji bi vodila ENISA omogućio bi veću transparentnost u pogledu postupka objavljivanja prije službenog otkrivanja ranjivosti i otpornost u slučajevima poremećaja ili prekida u pružanju sličnih usluga. Kako bi se izbjeglo udvostručavanje aktivnosti i postigla komplementarnost u mjeri u kojoj je to moguće, ENISA bi trebala istražiti mogućnost sklapanja sporazuma o strukturiranoj suradnji *sa sličnim* registrima **u nadležnosti trećih zemalja**.

Amandman 19
Prijedlog direktive
Uvodna izjava 32.

Tekst koji je predložila Komisija

(32) Skupina za suradnju trebala bi svake dvije godine uspostaviti program rada, uključujući mjere koje skupina mora poduzeti radi provedbe svojih ciljeva i zadaća. Vremenski okvir prvog programa

Zbog toga bi ENISA trebala uspostaviti **bazu podataka o ranjivostima u kojoj** ključni i važni subjekti i njihovi dobavljači te subjekti koji nisu obuhvaćeni područjem primjene ove Direktive mogu dobrovoljno otkriti ranjivosti i pružiti informacije o ranjivostima koje korisnicima omogućuju poduzimanje odgovarajućih mjera ublažavanja.

Izmjena

(31) 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** koji bi vodila ENISA omogućio bi veću transparentnost u pogledu postupka objavljivanja prije službenog otkrivanja ranjivosti i otpornost u slučajevima poremećaja ili prekida u pružanju sličnih usluga. Kako bi se izbjeglo udvostručavanje aktivnosti i postigla komplementarnost u mjeri u kojoj je to moguće, ENISA bi trebala istražiti mogućnost sklapanja sporazuma o strukturiranoj suradnji *s bazama podataka o ranjivosti ili* registrima *pod uvjetom da se takvim radnjama ne ugrožava zaštita povjerljivosti i poslovnih tajni*.

donesenog na temelju ove Direktive trebalo bi uskladiti s vremenskim okvirom posljednjeg programa donesenog na temelju Direktive (EU) 2016/1148 kako bi se izbjegli mogući poremećaji u radu skupine.

koje skupina mora poduzeti radi provedbe svojih ciljeva i zadaća. Vremenski okvir prvog programa donesenog na temelju ove Direktive trebalo bi uskladiti s vremenskim okvirom posljednjeg programa donesenog na temelju Direktive (EU) 2016/1148 kako bi se izbjegli mogući poremećaji u radu skupine.

Amandman 20
Prijedlog direktive
Uvodna izjava 32.a (nova)

Tekst koji je predložila Komisija

Izmjena

(32.a) Skupina za suradnju trebala bi se sastojati od predstavnika država članica, Komisije i ENISA-e.

Amandman 21
Prijedlog direktive
Uvodna izjava 34.

Tekst koji je predložila Komisija

Izmjena

(34) 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. Trebala bi organizirati redovite zajedničke sastanke s relevantnim privatnim dionicima iz cijele Unije na kojima bi se raspravljalo o aktivnostima skupine i prikupljale informacije o novim političkim izazovima. Kako bi se poboljšala suradnja na razini Unije, skupina bi trebala razmotriti mogućnost pozivanja tijela i agencija Unije uključenih u politiku kibersigurnosti, kao što su Europski centar za kiberkriminalitet (EC3), Agencija Europske unije za sigurnost zračnog prometa (EASA) i Agencija Europske unije za svemirski program (EUSPA), da sudjeluju u njezinu radu.

(34) 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. Trebala bi organizirati redovite zajedničke sastanke s relevantnim privatnim dionicima iz cijele Unije na kojima bi se raspravljalo o aktivnostima skupine i prikupljale informacije o novim političkim izazovima. Kako bi se poboljšala suradnja na razini Unije, skupina bi trebala razmotriti mogućnost pozivanja tijela i agencija Unije uključenih u politiku kibersigurnosti, kao što su Europski centar za kiberkriminalitet (EC3), Agencija Europske unije za sigurnost zračnog prometa (EASA) i Agencija Europske unije za svemirski program (EUSPA), da sudjeluju u njezinu radu, *kao i drugih relevantnih tijela i agencija Unije*.

Amandman 22
Prijedlog direktive
Uvodna izjava 35.

Tekst koji je predložila Komisija

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

Izmjena

(35) Nadležna tijela i CSIRT-ove trebalo bi poticati na sudjelovanje u programima razmjene *i zajedničkim programima osposobljavanja* za službenike iz drugih država članica 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*.

Amandman 23
Prijedlog direktive
Uvodna izjava 39.

Tekst koji je predložila Komisija

(39) Za potrebe ove Direktive pojam „izbjegnuti incident“ trebao bi se odnositi na događaj koji je potencijalno mogao prouzročiti štetu, ali je njegovo nastajanje uspješno spriječeno.

Izmjena

Briše se.

Amandman 24
Prijedlog direktive
Uvodna izjava 45.a (nova)

Tekst koji je predložila Komisija

Izmjena

(45.a) Uz to, subjekti bi trebali osigurati i odgovarajuću edukaciju i osposobljavanje svojeg osoblja o kibersigurnosti na svim razinama organizacije.

Amandman 25
Prijedlog direktive
Uvodna izjava 46.

Tekst koji je predložila Komisija

(46) Kako bi se dodatno suzbili ključni rizici u lancu opskrbe i pomoglo subjektima koji djeluju u sektorima obuhvaćenima ovom Direktivom da na odgovarajući način upravljaju kibersigurnosnim rizicima u lancu opskrbe i kibersigurnosnim rizicima povezanim s dobavljačima, skupina za suradnju koja uključuje relevantna nacionalna tijela, u suradnji s Komisijom i ENISA-om, trebala bi provoditi koordinirane procjene rizika u lancu opskrbe pojedinog sektora, kao što je već učinjeno za 5G mreže u skladu s Preporukom (EU) 2019/534 o kibersigurnosti 5G mreža²¹, u cilju utvrđivanja ključnih IKT usluga, sustava ili proizvoda, relevantnih prijetnji i ranjivosti **za pojedini sektor.**

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

Amandman 26
Prijedlog direktive
Uvodna izjava 47.

Tekst koji je predložila Komisija

(47) U procjenama rizika u lancu opskrbe, s obzirom na značajke predmetnog sektora, trebalo bi uzeti u obzir tehničke i, prema potrebi, netehničke čimbenike, uključujući one definirane u Preporuci (EU) 2019/534, u usklađenoj procjeni rizika sigurnosti 5G mreža na razini EU-a i u paketu instrumenata EU-a za kibersigurnost 5G tehnologije oko kojih se suglasila skupina za suradnju. Pri utvrđivanju lanaca opskrbe koji bi trebali biti podložni koordiniranoj procjeni rizika,

Izmjena

(46) Kako bi se dodatno suzbili ključni rizici u lancu opskrbe i pomoglo subjektima koji djeluju u sektorima obuhvaćenima ovom Direktivom da na odgovarajući način upravljaju kibersigurnosnim rizicima u lancu opskrbe i kibersigurnosnim rizicima povezanim s dobavljačima, skupina za suradnju koja uključuje relevantna nacionalna tijela, u suradnji s Komisijom i ENISA-om, trebala bi provoditi koordinirane procjene rizika u lancu opskrbe pojedinog sektora, kao što je već učinjeno za 5G mreže u skladu s Preporukom (EU) 2019/534 o kibersigurnosti 5G mreža²¹, u cilju utvrđivanja ključnih IKT usluga, sustava ili proizvoda, relevantnih prijetnji i ranjivosti **u svakom sektoru.**

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

u obzir bi trebalo uzeti sljedeće kriterije: i. i. mjera u kojoj se ključni i važni subjekti koriste određenim ključnim IKT uslugama, sustavima ili proizvodima i oslanjaju na njih; ii važnost specifičnih ključnih IKT usluga, sustava ili proizvoda u obavljanju ključnih ili osjetljivih funkcija, uključujući obradu osobnih podataka; iii dostupnost alternativnih IKT usluga, sustava ili proizvoda; iv. otpornost cjelokupnog lanca opskrbe IKT uslugama, sustavima ili proizvodima na ometajuće događaje i v. potencijalna buduća važnost novih IKT usluga, sustava ili proizvoda za aktivnosti subjekata.

procjeni rizika, u obzir bi trebalo uzeti sljedeće kriterije: i. i. mjera u kojoj se ključni i važni subjekti koriste određenim ključnim IKT uslugama, sustavima ili proizvodima i oslanjaju na njih; ii važnost specifičnih ključnih IKT usluga, sustava ili proizvoda u obavljanju ključnih ili osjetljivih funkcija, uključujući obradu osobnih podataka; iii dostupnost alternativnih IKT usluga, sustava ili proizvoda; iv. otpornost cjelokupnog lanca opskrbe IKT uslugama, sustavima ili proizvodima na ometajuće događaje i v. potencijalna buduća važnost novih IKT usluga, sustava ili proizvoda za aktivnosti subjekata.

Amandman 27 Prijedlog direktive Uvodna izjava 51.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 28 Prijedlog direktive Uvodna izjava 52.

Tekst koji je predložila Komisija

(52) **Prema potrebi, subjekti** bi trebali obavijestiti svoje primatelje usluga o

Izmjena

(52) **Subjekti** bi trebali **nastojati** obavijestiti svoje primatelje usluga o

posebnim i ozbiljnim prijetnjama te o mjerama koje mogu poduzeti kako bi ublažili nastali rizik. **Zahtjev obavlješćivanja primatelja usluga o takvim prijetnjama** ne bi **smio** podrazumijevati oslobađanje pružatelja od obveze da o vlastitom trošku poduzme odgovarajuće i hitne mjere kako bi se spriječile ili uklonile sve kibernetičke i ponovno uspostavila normalna sigurnosna razina usluge. Pružanje takvih informacija o sigurnosnim prijetnjama trebalo bi biti besplatno za primatelje usluga.

posebnim i ozbiljnim prijetnjama te o mjerama koje mogu poduzeti kako bi ublažili nastali rizik, **posebno kada se takvim mjerama može povećati zaštita potrošača. To ne bi smjelo** podrazumijevati oslobađanje pružatelja od obveze da o vlastitom trošku poduzme odgovarajuće i hitne mjere kako bi se spriječile ili uklonile sve kibernetičke i ponovno uspostavila normalna sigurnosna razina usluge. Pružanje takvih informacija o sigurnosnim prijetnjama trebalo bi biti besplatno za primatelje usluga **i na lako razumljivom jeziku.**

Amandman 29 Prijedlog direktive Uvodna izjava 53.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 30 Prijedlog direktive Uvodna izjava 54.

Tekst koji je predložila Komisija

(54) Kako bi se zaštitila sigurnost elektroničkih komunikacijskih mreža i usluga, trebalo bi promicati upotrebu šifriranja, posebice šifriranja s kraja na kraj, koja bi, prema potrebi, trebala biti obvezna za pružatelje takvih usluga i mreža u skladu s načelima zadane i integrirane sigurnosti i privatnosti u **smislu**

Izmjena

(54) Kako bi se zaštitila sigurnost elektroničkih komunikacijskih mreža i usluga, trebalo bi promicati upotrebu šifriranja, posebice šifriranja s kraja na kraj, koja bi, prema potrebi, trebala biti obvezna za pružatelje takvih usluga i mreža u skladu s načelima zadane i integrirane sigurnosti i privatnosti u **svrhu**

članka 18. Upotrebu šifriranja s kraja na kraj **trebalo bi uskladiti s ovlastima** država članica da osiguraju zaštitu svojih ključnih sigurnosnih interesa i javne sigurnosti te da dopuste istragu, otkrivanje i progona kaznenih djela u skladu s pravom Unije. Rješenjima za zakonit pristup informacijama u komunikacijama šifriranima s kraja na kraj trebala bi se očuvati učinkovitost šifriranja u zaštiti privatnosti i sigurnosti komunikacija te bi se istodobno trebao osigurati učinkovit odgovor na kriminal.

mjera upravljanja kibersigurnosnim rizicima. **Upotrebom** šifriranja s kraja na kraj **ne dovode se u pitanje ovlasti** država članica, **politike i procedure** da osiguraju zaštitu svojih ključnih sigurnosnih interesa i javne sigurnosti te da dopuste istragu, otkrivanje i progona kaznenih djela u skladu s pravom Unije. Rješenjima za zakonit pristup informacijama u komunikacijama šifriranima s kraja na kraj trebala bi se očuvati učinkovitost šifriranja u zaštiti privatnosti i sigurnosti komunikacija te bi se istodobno trebao osigurati učinkovit odgovor na kriminal. **Sve poduzete mjere moraju strogo poštovati načela proporcionalnosti i subsidijarnosti.**

Amandman 31 Prijedlog direktive Uvodna izjava 55.

Tekst koji je predložila Komisija

(55) Ovom se Direktivom utvrđuje pristup izvješćivanju o incidentima **u dvije faze** kako bi se uspostavila prava ravnoteža između, s jedne strane, brzog izvješćivanja koje pridonosi ublažavanju potencijalnog širenja incidenata i omogućuje subjektima da traže podršku te, s druge strane, detaljnog izvješćivanja kojim se iz pojedinačnih incidenata izvlače vrijedne pouke i s vremenom poboljšava otpornost na kiberprijetnje pojedinačnih poduzeća i cijelih sektora. Kada subjekti dobiju informaciju o incidentu, trebali bi biti dužni u roku od **24** sata dostaviti prvu obavijest, nakon čega u roku od mjesec dana moraju **dostaviti završno izvješće**. Prva obavijest trebala bi sadržavati samo informacije koje su nužne kako bi nadležna tijela bila upoznata s incidentom i kako bi se subjektu omogućilo traženje pomoći, ako je to potrebno. U takvoj bi obavijesti, ako je to moguće, trebalo navesti pretpostavlja li se da je incident uzrokovani nezakonitim ili zlonamjernim djelovanjem. Države članice trebale bi osigurati da se

Izmjena

(55) Ovom se Direktivom utvrđuje pristup izvješćivanju o incidentima **korak po korak** kako bi se uspostavila prava ravnoteža između, s jedne strane, brzog izvješćivanja koje pridonosi ublažavanju potencijalnog širenja incidenata i omogućuje subjektima da traže podršku te, s druge strane, detaljnog izvješćivanja kojim se iz pojedinačnih incidenata izvlače vrijedne pouke i s vremenom poboljšava otpornost na kiberprijetnje pojedinačnih poduzeća i cijelih sektora. Kada subjekti dobiju informaciju o incidentu **ili izbjegnutom incidentu**, trebali bi biti dužni u roku od **72** sata dostaviti prvu obavijest, nakon čega **moraju dostaviti sveobuhvatno izvješće najkasnije tri mjeseca nakon podnošenja prve obavijesti te završno izvješće** u roku od mjesec dana moraju **nakon ublažavanja incidenta**. Prva obavijest trebala bi sadržavati samo informacije koje su nužne kako bi nadležna tijela bila upoznata s incidentom i kako bi se subjektu omogućilo traženje pomoći, ako je to potrebno. U takvoj bi obavijesti,

zahtjevom za podnošenje te prve obavijesti resursi subjekta koji obavješćuje ne preusmjeravaju s aktivnosti povezanih s rješavanjem incidenata koje bi trebale biti prioritetne. Kako bi se dodatno spriječilo da se zbog obveza izvješćivanja o incidentima oduzimaju resursi za rješavanje incidenata ili na drugi način ugrožavaju aktivnosti subjekata u tom pogledu, države članice trebale bi, u opravdanim slučajevima i u dogovoru s nadležnim tijelima ili CSIRT-om, predmetnom subjektu omogućiti odstupanje od *roka od 24 sata za prvu obavijest i roka od mjesec dana za završno izvješće*.

ako je to moguće, trebalo navesti pretpostavlja li se da je incident uzrokovan nezakonitim ili zlonamjernim djelovanjem. Države članice trebale bi osigurati da se zahtjevom za podnošenje te prve obavijesti resursi subjekta koji obavješćuje ne preusmjeravaju s aktivnosti povezanih s rješavanjem incidenata koje bi trebale biti prioritetne. *Prvoj obavijesti trebalo bi prethoditi rano upozorenje o incidentu u prvih 24 sata bez obveze objavljivanja dodatnih informacija. To bi rano upozorenje trebalo dostaviti što je prije moguće, čime se subjektima omogućuje da brzo zatraže potporu nadležnih tijela ili CSIRT-ova i nadležnim tijelima ili CSIRT-ovima da ublaže potencijalno širenje prijavljenog incidenta, a služi i kao alat za informiranost o stanju za CSIRT-ove.* Kako bi se dodatno spriječilo da se zbog obveza izvješćivanja o incidentima oduzimaju resursi za rješavanje incidenata ili na drugi način ugrožavaju aktivnosti subjekata u tom pogledu, države članice trebale bi, u opravdanim slučajevima i u dogovoru s nadležnim tijelima ili CSIRT-om, predmetnom subjektu omogućiti odstupanje od *predvidenih rokova*.

Amandman 32 Prijedlog direktive Uvodna izjava 56.

Tekst koji je predložila Komisija

(56) Ključni i važni subjekti često određeni incident, zbog njegovih značajki, moraju prijaviti različitim tijelima u skladu s obvezama obavješćivanja uključenima u razne pravne instrumente. Takvi slučajevi stvaraju dodatna opterećenja i mogu dovesti do nesigurnosti u pogledu oblika obavijesti i postupanja s njima. S obzirom na to i u svrhu pojednostavljenja izvješćivanja o sigurnosnim incidentima, države članice trebale bi uspostaviti jedinstvenu ulaznu točku za sve obavijesti koje se zahtijevaju ovom Direktivom i

Izmjena

(56) Ključni i važni subjekti često određeni incident, zbog njegovih značajki, moraju prijaviti različitim tijelima u skladu s obvezama obavješćivanja uključenima u razne pravne instrumente. Takvi slučajevi stvaraju dodatna opterećenja i mogu dovesti do nesigurnosti u pogledu oblika obavijesti i postupanja s njima. S obzirom na to i u svrhu pojednostavljenja izvješćivanja o sigurnosnim incidentima *i održavanja načela „samo jednom”*, države članice trebale bi uspostaviti jedinstvenu ulaznu točku za sve obavijesti koje se

drugim pravom Unije, kao što su Uredba (EU) 2016/679 i Direktiva 2002/58/EZ. ENISA bi sa skupinom za suradnju trebala izraditi zajedničke predloške za obavlješćivanje s pomoću smjernica kojima bi se pojednostavnile i uskladile izvještajne informacije koje se zahtijevaju pravom Unije, čime bi se smanjilo opterećenje za poduzeća.

zahtijevaju ovom Direktivom i drugim pravom Unije, kao što su Uredba (EU) 2016/679 i Direktiva 2002/58/EZ. ENISA bi sa skupinom za suradnju trebala izraditi zajedničke predloške za obavlješćivanje s pomoću smjernica kojima bi se pojednostavnile i uskladile izvještajne informacije koje se zahtijevaju pravom Unije, čime bi se smanjilo opterećenje za poduzeća.

Amandman 33 Prijedlog direktive Uvodna izjava 59.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 34 Prijedlog direktive Uvodna izjava 61.

Tekst koji je predložila Komisija

(61) Kako bi se osigurala dostupnost točnih i potpunih podataka o registraciji naziva domena, registri vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu (**tzv. registrari**) trebali bi prikupljati i jamčiti cjelovitost i dostupnost podataka o registraciji naziva domena. U konkretnom slučaju, registri vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu trebali bi

Izmjena

(61) Kako bi se osigurala dostupnost točnih i potpunih podataka o registraciji naziva domena, registri vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu (**uključujući usluge koje pružaju registri i registrari naziva domena, pružatelji usluga zaštite privatnosti ili registracije proxy poslužitelja i brokeri ili preprodavatelji domena te sve druge usluge povezane s registracijom naziva domena**) trebali bi

uspovjetiti politike i postupke za prikupljanje i održavanje točnih i potpunih registracijskih podataka te za sprečavanje i ispravljanje netočnih registracijskih podataka u skladu s pravilima Unije o zaštiti podataka.

prikupljati i jamčiti cjelovitost i dostupnost podataka o registraciji naziva domena. U konkretnom slučaju, registri vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu trebali bi uspostaviti politike i postupke za prikupljanje i održavanje točnih i potpunih registracijskih podataka te za sprečavanje i ispravljanje netočnih registracijskih podataka u skladu s pravilima Unije o zaštiti podataka.

Amandman 35
Prijedlog direktive
Uvodna izjava 68.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 36
Prijedlog direktive
Uvodna izjava 69.

Tekst koji je predložila Komisija

(69) Obrada osobnih podataka **u mjeri koja je nužna i proporcionalna** za potrebe osiguravanja mrežne i informacijske

Izmjena

(69) Obrada osobnih podataka **koja bi trebala biti ograničena na ono što je nužno i proporcionalno** za potrebe

sigurnosti, koju provode subjekti, javna tijela, CERT-ovi, CSIRT-ovi i pružatelji sigurnosnih tehnologija i usluga, trebala bi se smatrati legitimnim interesom predmetnog voditelja obrade podataka u skladu s Uredbom (EU) 2016/679. To bi trebalo uključivati mjere za sprečavanje, otkrivanje, analizu i odgovor na incidente, mjere za informiranje o određenim kiberprijetnjama, razmjenu informacija u kontekstu uklanjanja i koordiniranog otkrivanja ranjivosti, kao i dobrovoljnu razmjenu informacija o tim incidentima, kiberprijetnjama i ranjivostima, pokazatelje ugroženosti, taktike, tehnike i postupke, kbersigurnosna upozorenja i konfiguracijske alate. Takve mjere mogu zahtijevati obradu sljedećih vrsta osobnih podataka: IP adresa, jedinstvenih lokatora resursa (URL-ova), naziva domena i adresa elektroničke pošte.

osiguravanja mrežne i informacijske sigurnosti **i zaštite potrošača**, koju provode subjekti, javna tijela, CERT-ovi, CSIRT-ovi i pružatelji sigurnosnih tehnologija i usluga, trebala bi se smatrati legitimnim interesom predmetnog voditelja obrade podataka u skladu s Uredbom (EU) 2016/679. To bi trebalo uključivati mjere za sprečavanje, otkrivanje, analizu i odgovor na incidente, mjere za informiranje o određenim kiberprijetnjama, razmjenu informacija u kontekstu uklanjanja i koordiniranog otkrivanja ranjivosti, kao i dobrovoljnu razmjenu informacija o tim incidentima, kiberprijetnjama i ranjivostima, pokazatelje ugroženosti, taktike, tehnike i postupke, kbersigurnosna upozorenja i konfiguracijske alate. Takve mjere mogu zahtijevati obradu sljedećih vrsta osobnih podataka: IP adresa, jedinstvenih lokatora resursa (URL-ova), naziva domena i adresa elektroničke pošte.

Amandman 37 Prijedlog direktive Uvodna izjava 70.

Tekst koji je predložila Komisija

(70) 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 putem 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 subjekata i nadležnih tijela. Stoga bi se na ključne subjekte trebao primjenjivati sveobuhvatni nadzorni sustav (ex ante i ex post), dok bi se na važne subjekte trebao primjenjivati blagi sustav nadzora, i to samo ex post. U potonjem slučaju to znači da važni subjekti ne bi trebali sustavno dokumentirati usklađenost

Izmjena

(70) Kako bi se ojačale nadzorne ovlasti i mjere koje pomažu u osiguravanju učinkovite usklađenosti **te postigla zajednička visoka razina sigurnosti diljem digitalnog sektora, uključujući sprečavanjem rizika za korisnike ili druge mreže, informacijske sustave i usluge**, ovom bi se Direktivom trebao predvidjeti popis minimalnih nadzornih mjera i sredstava putem 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 subjekata i nadležnih tijela. Stoga bi se na ključne subjekte trebao primjenjivati sveobuhvatni nadzorni sustav (ex ante i ex

sa zahtjevima za upravljanje kibersigurnosnim rizicima, dok bi nadležna tijela trebala primjenjivati reaktivni ex post pristup nadzoru te stoga ne bi trebala imati opću obvezu nadzora tih subjekata.

post), dok bi se na važne subjekte trebao primjenjivati blagi sustav nadzora, i to samo ex post, *uzimajući u obzir pristup koji se temelji na riziku*. U potonjem slučaju to znači da važni subjekti ne bi trebali sustavno dokumentirati usklađenost sa zahtjevima za upravljanje kibersigurnosnim rizicima, dok bi nadležna tijela trebala primjenjivati reaktivni ex post pristup nadzoru te stoga ne bi trebala imati opću obvezu nadzora tih subjekata, *osim u slučaju očitog kršenja obveza*.

Amandman 38 Prijedlog direktive Uvodna izjava 76.

Tekst koji je predložila Komisija

(76) Kako bi se dodatno ojačali učinkovitost i odvraćajući učinak sankcija koje se primjenjuju na povrede obveza utvrđenih u skladu s ovom Direktivom, nadležna tijela trebala bi biti ovlaštena za primjenu sankcija koje se sastoje od suspenzije certifikata ili ovlaštenja za *dio usluga ili sve usluge* koje pruža ključni subjekt *i izricanja privremene zabrane fizičkoj osobi da obavlja rukovoditeljske dužnosti*. S obzirom na njihovu ozbiljnost i učinak na aktivnosti subjekata te napisljeku na njihove potrošače, takve bi se sankcije trebale primjenjivati samo razmjerno ozbiljnosti povrede i uzimajući u obzir posebne okolnosti svakog slučaja, uključujući namjerna ili nehotična obilježja povrede, kao i mjere poduzete radi sprečavanja ili ublažavanja pretrpljene štete i/ili gubitaka. Takve bi se sankcije trebale primjenjivati samo kao ultima ratio, što znači tek nakon što se iscrpe druge odgovarajuće provedbene mjere 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 te sankcije. Izricanje takvih sankcija podliježe odgovarajućim

Izmjena

(76) Kako bi se dodatno ojačali učinkovitost i odvraćajući učinak sankcija koje se primjenjuju na povrede obveza utvrđenih u skladu s ovom Direktivom, nadležna tijela trebala bi biti ovlaštena za primjenu sankcija koje se sastoje od suspenzije certifikata ili ovlaštenja za *relevantne usluge* koje pruža ključni subjekt. S obzirom na njihovu ozbiljnost i učinak na aktivnosti subjekata te napisljeku na njihove potrošače, takve bi se sankcije trebale primjenjivati samo razmjerno ozbiljnosti povrede i uzimajući u obzir posebne okolnosti svakog slučaja, uključujući namjerna ili nehotična obilježja povrede, kao i mjere poduzete radi sprečavanja ili ublažavanja pretrpljene štete i/ili gubitaka. Takve bi se sankcije trebale primjenjivati samo kao ultima ratio, što znači tek nakon što se iscrpe druge odgovarajuće provedbene mjere 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 te sankcije. Izricanje takvih sankcija podliježe odgovarajućim postupovnim zaštitnim mjerama u skladu s općim načelima prava Unije i Poveljom

postupovnim zaštitnim mjerama u skladu s općim načelima prava Unije i Poveljom Europske unije o temeljnim pravima, uključujući djelotvornu sudsku zaštitu, zakonito postupanje, prepostavku nedužnosti i pravo na obranu.

Europske unije o temeljnim pravima, uključujući djelotvornu sudsku zaštitu, zakonito postupanje, prepostavku nedužnosti i pravo na obranu.

Amandman 39
Prijedlog direktive
Uvodna izjava 79.

Tekst koji je predložila Komisija

(79) Trebalo bi uvesti mehanizam istorazinskog ocjenjivanja kojim bi se stručnjacima koje su imenovale države članice omogućila procjena provedbe kibersigurnosnih politika, uključujući razinu sposobnosti i dostupnih resursa država članica.

Izmjena

(79) Trebalo bi uvesti mehanizam istorazinskog ocjenjivanja kojim bi se stručnjacima koje su imenovale države članice *i ENISA* omogućila procjena provedbe kibersigurnosnih politika, uključujući razinu sposobnosti i dostupnih resursa država članica, *te razmjena najboljih praksi povezanih*.

Amandman 40
Prijedlog direktive
Uvodna izjava 80.

Tekst koji je predložila Komisija

(80) Kako bi se uzeli u obzir nove kiberprijetnje, tehnološki razvoj ili sektorske posebnosti, Komisiji bi trebalo delegirati ovlast za donošenje akata u skladu s člankom 290. UFEU-a u pogledu elemenata povezanih s mjerama upravljanja rizicima propisanima ovom Direktivom. Komisija bi *isto tako* trebala biti ovlaštena **donositi delegirane akte** kojima se *utvrđuje* koje **kategorije ključnih subjekata moraju pribaviti certifikat i na temelju kojih posebnih 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

Izmjena

(80) Kako bi se uzeli u obzir nove kiberprijetnje, tehnološki razvoj ili sektorske posebnosti, Komisiji bi trebalo delegirati ovlast za donošenje akata u skladu s člankom 290. UFEU-a u pogledu elemenata povezanih s mjerama upravljanja rizicima propisanima ovom Direktivom. Komisija bi *također* trebala biti ovlaštena **za donošenje delegiranih akata** kojima se *utvrđuju tehnički elementi povezani s mjerama upravljanja rizicima*. Komisija bi također trebala biti ovlaštena **za donošenje delegiranih akata određivanjem vrste informacija** koje podnose **ključni i važni subjekti za svaki incident koji ima znatan učinak na pružanje njihovih usluga ili bilo kakav izbjegnuti incident te utvrđivanjem**

načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva²⁶ od 13. travnja 2016. 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.

slučajeva u kojima bi se incident trebao smatrati značajnim. 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 zakonodavstva²⁶ od 13. travnja 2016. 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.

²⁶ SL L 123, 12.5.2016., str. 1.

²⁶ SL L 123, 12.5.2016., str. 1.

Amandman 41 Prijedlog direktive Uvodna izjava 81.

Tekst koji je predložila Komisija

(81) Kako bi se osigurali jedinstveni uvjeti za provedbu relevantnih odredaba ove Direktive koje se odnose na postupovne aranžmane potrebne za funkcioniranje skupine za suradnju, *tehničke elemente povezane s mjerama upravljanja rizicima ili vrstu informacija*, oblik i postupak obavješćivanja o incidentima, provedbene ovlasti trebalo bi dodijeliti Komisiji. Te bi ovlasti trebalo izvršavati u skladu s Uredbom (EU) br. 182/2011 Europskog parlamenta i Vijeća²⁷.

²⁷ 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

Izmjena

(81) Kako bi se osigurali jedinstveni uvjeti za provedbu relevantnih odredaba ove Direktive koje se odnose na postupovne aranžmane potrebne za funkcioniranje skupine za suradnju, oblik i postupak obavješćivanja o incidentima, provedbene ovlasti trebalo bi dodijeliti Komisiji. Te bi ovlasti trebalo izvršavati u skladu s Uredbom (EU) br. 182/2011 Europskog parlamenta i Vijeća²⁷.

²⁷ 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.).

(SL L 55, 28.2.2011., str. 13.).

Amandman 42

Prijedlog direktive

Članak 1. – stavak 1.

Tekst koji je predložila Komisija

1. Ovom se Direktivom utvrđuju mjere kojima se osigurava visoka zajednička razina kibersigurnosti unutar Unije.

Izmjena

1. Ovom se Direktivom utvrđuju mjere kojima se osigurava visoka zajednička razina kibersigurnosti unutar Unije *kako bi se ostvarilo pouzdano digitalno okruženje za potrošače i gospodarske subjekte te kako bi se poboljšalo funkcioniranje unutarnjeg tržišta i uklonile prepreke za njegovo funkcioniranje.*

Amandman 43

Prijedlog direktive

Članak 2. – stavak 2. – podstavak 1. – uvodni dio

Tekst koji je predložila Komisija

2. Međutim, Direktiva se primjenjuje i na subjekte iz priloga I. i II. neovisno o njihovoj veličini:

Izmjena

2. Međutim, Direktiva se primjenjuje i na subjekte *određenog tipa* iz priloga I. i II. neovisno o njihovoj veličini:

Amandman 44

Prijedlog direktive

Članak 2. – stavak 2. – podstavak 2.a (novi)

Tekst koji je predložila Komisija

Izmjena

Komisija izdaje smjernice kako bi podržala države članice u ispravnoj provedbi odredaba o području primjene, kao i radi odobravanja mogućih odstupanja za određene važne subjekte iz područja primjene Direktive ili od nekih njezinih odredaba, uzimajući u obzir njihovu nisku razinu kritičnosti u njihovom specifičnom sektoru i/ili njihovu nisku razinu ovisnosti o drugim sektorima ili vrstama usluga. Države članice,

uzimajući u potpunosti u obzir smjernice Komisije, obavješćuju Komisiju o svojim obrazloženim odlukama u tom pogledu.

Amandman 45

Prijedlog direktive

Članak 4. – stavak 1. – točka 4.

Tekst koji je predložila Komisija

(4) „nacionalna strategija za kibersigurnost” znači usklađen okvir države članice kojim se predviđaju strateški ciljevi i prioriteti za sigurnost mrežnih i informacijskih sustava u toj državi članici;

Izmjena

(4) „nacionalna strategija za kibersigurnost” znači usklađen okvir države članice kojim se predviđaju strateški ciljevi i prioriteti za sigurnost mrežnih i informacijskih sustava u toj državi članici, *kao i politike potrebne za njihovo postizanje*;

Amandman 46

Prijedlog direktive

Članak 4. – stavak 1. – točka 5.a (nova)

Tekst koji je predložila Komisija

Izmjena

(5.a) „prekogranični incident” znači svaki incident koji utječe na operatere pod nadzorom nacionalnih nadležnih tijela iz najmanje dviju različitih država članica;

Amandman 47

Prijedlog direktive

Članak 4. – stavak 1. – točka 6.a (nova)

Tekst koji je predložila Komisija

Izmjena

(6.a) „izbjegnuti incident” znači događaj koji je mogao prouzročiti štetu, ali je njegovo nastajanje uspješno spriječeno;

Amandman 48

Prijedlog direktive

Članak 4. – stavak 1. – točka 15.a (nova)

Tekst koji je predložila Komisija

Izmjena

(15.a) „*usluge registracije naziva domena*” znači usluge koje pružaju registri i registrari naziva domena, pružatelji usluga privatnosti ili proxy registracije te brokeri ili preprodavatelji domena i sve druge usluge povezane s registracijom naziva domena;

Amandman 49

Prijedlog direktive

Članak 5. – stavak 1. – uvodni dio

Tekst koji je predložila Komisija

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

Izmjena

1. Svaka država članica donosi nacionalnu strategiju za kibersigurnost kojom se utvrđuju strateški ciljevi i odgovarajuće mjere politike i regulatorne mjere, *što uključuje adekvatne ljudske i finansijske resurse*, radi postizanja i održavanja visoke razine kibersigurnosti. Nacionalna strategija za kibersigurnost posebno uključuje sljedeće:

Amandman 50

Prijedlog direktive

Članak 5. – stavak 1. – točka b

Tekst koji je predložila Komisija

(b) upravljački okvir za postizanje tih ciljeva i prioriteta, uključujući politike iz stavka 2. te uloge i odgovornosti javnih tijela i subjekata kao i drugih relevantnih aktera;

Izmjena

(b) upravljački okvir za postizanje tih ciljeva i prioriteta, uključujući politike iz stavka 2. te uloge i odgovornosti javnih tijela i subjekata kao i drugih relevantnih aktera, *uključujući one koji su odgovorni za saznanja o kiberprijetnjama i kiberobranu*;

Amandman 51

Prijedlog direktive

Članak 5. – stavak 1. – točka c

Tekst koji je predložila Komisija

(c) procjenu radi utvrđivanja relevantne imovine i kibersigurnosnih rizika u toj državi članici;

Izmjena

(c) procjenu radi utvrđivanja relevantne imovine i kibersigurnosnih rizika u toj državi članici, ***uključujući potencijalne nedostatke koji mogu negativno utjecati na jedinstveno tržište.***

Amandman 52

Prijedlog direktive

Članak 5. – stavak 1. – točka e

Tekst koji je predložila Komisija

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

Izmjena

(e) popis različitih tijela i aktera koji su uključeni u provedbu nacionalne strategije za kibersigurnost, ***uključujući jedinstvenu kontaktnu točku za MSP-ove;***

Amandman 53

Prijedlog direktive

Članak 5. – stavak 2. – točka b

Tekst koji je predložila Komisija

(b) smjernice za uključivanje i definiranje kibersigurnosnih zahtjeva za IKT proizvode i usluge u području javne nabave;

Izmjena

(b) smjernice za uključivanje i definiranje kibersigurnosnih zahtjeva za IKT proizvode i usluge u području javne nabave, ***uključujući upotrebu kibersigurnosnih proizvoda otvorenog koda;***

Amandman 54

Prijedlog direktive

Članak 5. – stavak 2. – točka c

Tekst koji je predložila Komisija

(c) politiku za promicanje i olakšavanje koordiniranog otkrivanja ranjivosti u smislu članka 6.;

Izmjena

(c) politiku za promicanje i olakšavanje koordiniranog otkrivanja ranjivosti u smislu članka 6., ***uključujući utvrđivanjem smjernica i najboljih praksi koje se temelje na već uspostavljenim međunarodno priznatim normama za***

rješavanje i otkrivanje ranjivosti;

Amandman 55
Prijedlog direktive
Članak 5. – stavak 2. – točka e

Tekst koji je predložila Komisija

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

Izmjena

(e) politiku promicanja *kibersigurnosti za potrošače, senzibilizacije o kiberprijetnjama, povećanja kiberpismenosti, jačanja povjerenja korisnika, tehnološki neutralnih* vještina *i obrazovanja* u području kibersigurnosti *te promicanja* istraživačkih i razvojnih inicijativa *i kibersigurnosti povezanih proizvoda;*

Amandman 56
Prijedlog direktive
Članak 5. – stavak 2. – točka ea (nova)

Tekst koji je predložila Komisija

Izmjena

(ea) politiku kojom se promiče uporaba kriptografije i šifriranja, posebno od strane MSP-ova;

Amandman 57
Prijedlog direktive
Članak 5. – stavak 2. – točka h

Tekst koji je predložila Komisija

Izmjena

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

(h) politiku za *promicanje kibersigurnosti i rješavanje posebnih potreba MSP-ova u pogledu ispunjavanja obveza utvrđenih ovom Direktivom, kao i posebnih potreba MSP-ova koji su izuzeti* iz područja primjene ove Direktive, u pogledu smjernica i potpore za poboljšanje njihove otpornosti na kiberprijetnje, *uključujući, npr., financiranje i obrazovanje za poticanje donošenja kibersigurnosnih mjera.*

Amandman 58
Prijedlog direktive
Članak 5. – stavak 2. – točka ha (nova)

Tekst koji je predložila Komisija

Izmjena

(ha) ta politika uključuje uspostavu nacionalne jedinstvene kontaktne točke za MSP-ove i okvira za najučinkovitiju upotrebu digitalno-inovacijskih centara i dostupnih sredstava za postizanje ciljeva politike;

Amandman 59
Prijedlog direktive
Članak 5. – stavak 2. – točka hb (nova)

Tekst koji je predložila Komisija

Izmjena

(hb) politiku kojom se promiče dosljedna i sinergijska upotreba dostupnih sredstava;

Amandman 60
Prijedlog direktive
Članak 5. – stavak 4.

Tekst koji je predložila Komisija

Izmjena

4. Države članice ocjenjuju svoje nacionalne strategije za kibersigurnost najmanje svake četiri godine na temelju ključnih pokazatelja uspješnosti te ih prema potrebi izmjenjuju. Agencija Europske unije za kibersigurnost (ENISA) pomaže državama članicama, na njihov zahtjev, u razvoju nacionalne strategije i ključnih pokazatelja uspješnosti za ocjenjivanje strategije.

4. Države članice ocjenjuju svoje nacionalne strategije za kibersigurnost najmanje svake četiri godine na temelju ključnih pokazatelja uspješnosti te ih prema potrebi izmjenjuju. Agencija Europske unije za kibersigurnost (ENISA) pomaže državama članicama, na njihov zahtjev, u razvoju nacionalne strategije i ključnih pokazatelja uspješnosti za ocjenjivanje strategije. *ENISA državama članicama upućuje i preporuke o razvoju ključnih pokazatelja uspješnosti za procjenu nacionalne strategije, usporedive na razini Unije.*

Amandman 61
Prijedlog direktive
Članak 6. – naslov

Tekst koji je predložila Komisija

Koordinirano otkrivanje ranjivosti i
europski registar ranjivosti

Izmjena

Koordinirano otkrivanje ranjivosti i
europска база података о ranjivosti

Amandman 62
Prijedlog direktive
Članak 6. – stavak 2.

Tekst koji je predložila Komisija

2. ENISA razvija i vodi **europski registar** ranjivosti. U tu svrhu ENISA uspostavlja i održava odgovarajuće informacijske sustave, politike i postupke osobito kako bi omogućila važnim i ključnim subjektima, kao i njihovim dobavljačima mrežnih i informacijskih sustava da otkriju i registriraju ranjivosti prisutne u IKT proizvodima ili IKT uslugama te da svim zainteresiranim stranama omoguće pristup informacijama o ranjivostima sadržanima u registru.

Registar konkretno uključuje informacije o ranjivosti, IKT proizvodu ili IKT uslugama na koje ona utječe i ozbiljnosti ranjivosti s obzirom na okolnosti u kojima se može iskoristiti, dostupnosti odgovarajućih popravaka i, ako nisu dostupni, smjernica namijenjenih korisnicima ranjivih proizvoda i usluga o načinu na koji se mogu ublažiti rizici koji proizlaze iz otkrivenih ranjivosti.

Izmjena

2. ENISA razvija i vodi **europskuazu podataku o** ranjivosti. U tu svrhu ENISA uspostavlja i održava odgovarajuće informacijske sustave, politike i postupke, **kao i odgovarajuće politike objavljivanja**, osobito kako bi omogućila važnim i ključnim subjektima, kao i njihovim dobavljačima mrežnih i informacijskih sustava da otkriju i **lako** registriraju ranjivosti prisutne u IKT proizvodima ili IKT uslugama te da svim zainteresiranim stranama omoguće pristup **relevantnim** informacijama o ranjivostima sadržanima u registru, **pod uvjetom da se takvim postupcima ne ugrožava zaštita povjerljivosti i poslovnih tajni. Baza podataka o ranjivosti** konkretno uključuje informacije o ranjivosti, IKT proizvodu ili IKT uslugama na koje ona utječe i ozbiljnosti ranjivosti s obzirom na okolnosti u kojima se može iskoristiti, dostupnosti odgovarajućih popravaka i, ako nisu dostupni, smjernica namijenjenih korisnicima ranjivih proizvoda i usluga o načinu na koji se mogu ublažiti rizici koji proizlaze iz otkrivenih ranjivosti. **Kako bi se izbjeglo udvostručavanje napora, ENISA sklapa sporazum o razmjeni informacija i strukturirani sporazum o suradnji s registrom zajedničkih ranjivosti i izloženosti (CVE) i, prema potrebi, s drugim bazama podataka koje na globalnoj razini razvijaju i održavaju**

pouzdani partneri.

Amandman 63

Prijedlog direktive

Članak 7. – stavak 1.a (novi)

Tekst koji je predložila Komisija

Izmjena

1.a Ako država članica imenuje više od jednog nadležnog tijela iz stavka 1., trebala bi jasno naznačiti koje će od tih nadležnih tijela služiti kao glavna kontaktna točka tijekom incidenta ili krize velikih razmjera.

Amandman 64

Prijedlog direktive

Članak 7. – stavak 3. – točka f

Tekst koji je predložila Komisija

Izmjena

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

(f) nacionalni postupci i **koordinacija** između relevantnih nacionalnih vlasti i tijela, **uključujući ona odgovorna za saznanja o kiberprijetnjama i kiberobranu**, kako bi se osiguralo učinkovito sudjelovanje država članica u koordiniranom upravljanju kiberincidentima i kiberkrizama velikih razmjera na razini Unije i njihova potpora takvom upravljanju.

Amandman 65

Prijedlog direktive

Članak 10. – stavak 2. – točka d

Tekst koji je predložila Komisija

Izmjena

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

(d) osiguravanje dinamičke analize rizika i incidenata te informiranosti o stanju u pogledu kibersigurnosti, **uključujući putem analize ranih upozorenja i obavijesti kako je utvrđeno u članku 20.;**

Amandman 66
Prijedlog direktive
Članak 10. – stavak 2. – točka e

Tekst koji je predložila Komisija

(e) osiguravanje, na zahtjev subjekta, **proaktivnog** pregledavanja mrežnih i informacijskih sustava koji se upotrebljavaju za pružanje njihovih usluga;

Izmjena

(e) osiguravanje, na zahtjev subjekta, pregledavanja mrežnih i informacijskih sustava koji se upotrebljavaju za pružanje njihovih usluga **kako bi se konkretne prijetnje utvrdile, ublažile ili spriječe**;

Amandman 67
Prijedlog direktive
Članak 10. – stavak 2. – točka f

Tekst koji je predložila Komisija

(f) **sudjelovanje** u mreži CSIRT-ova i pružanje uzajamne pomoći drugim članovima mreže na njihov zahtjev.

Izmjena

(f) **aktivno sudjelovanje** u mreži CSIRT-ova i pružanje uzajamne pomoći drugim članovima mreže na njihov zahtjev.

Amandman 68
Prijedlog direktive
Članak 10. – stavak 2. – točka fa (nova)

Tekst koji je predložila Komisija

Izmjena

(fa) pružanje operativne pomoći i smjernica subjektima iz priloga I. i II., a posebno MSP-ovima;

Amandman 69
Prijedlog direktive
Članak 10. – stavak 2. – točka fb (nova)

Tekst koji je predložila Komisija

Izmjena

(fb) sudjelovanje u zajedničkim vježbama u području kibersigurnosti na razini Unije;

Amandman 70
Prijedlog direktive
Članak 11. – stavak 2.

Tekst koji je predložila Komisija

2. Države članice osiguravaju da njihova nadležna tijela ili njihovi CSIRT-ovi primaju obavijesti o incidentima, kao i ozbiljnim kiberprijetnjama i izbjegnutim incidentima, podnesene u skladu s ovom Direktivom. Ako država članica odluči da njezini CSIRT-ovi ne primaju te obavijesti, CSIRT-ovima se, u onoj mjeri u kojoj je to potrebno za izvršavanje njihovih zadaća, omogućuje pristup podacima o incidentima o kojima su obavijestili ključni ili važni subjekti u skladu s člankom 20.

Izmjena

2. Države članice osiguravaju da njihova nadležna tijela ili njihovi CSIRT-ovi primaju obavijesti o incidentima, kao i ozbiljnim kiberprijetnjama i izbjegnutim incidentima, podnesene u skladu s ovom Direktivom. Ako država članica odluči da njezini CSIRT-ovi ne primaju te obavijesti, CSIRT-ovima se, u onoj mjeri u kojoj je to potrebno za ***učinkovito*** izvršavanje njihovih zadaća, omogućuje ***odgovarajući*** pristup podacima o incidentima o kojima su obavijestili ključni ili važni subjekti u skladu s člankom 20.

Amandman 71
Prijedlog direktive
Članak 11. – stavak 4.

Tekst koji je predložila Komisija

4. U mjeri u kojoj je to potrebno za učinkovito izvršavanje zadaća i obveza utvrđenih u ovoj Direktivi, države članice osiguravaju odgovarajuću suradnju između nadležnih tijela i jedinstvenih kontaktnih točaka i tijela za izvršavanje zakonodavstva, tijela za zaštitu podataka i tijela odgovornih za kritičnu infrastrukturu u skladu s Direktivom (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] i nacionalnih finansijskih tijela imenovanih u skladu s Uredbom (EU) XXXX/XXXX Europskog parlamenta i Vijeća³⁹ [Uredba DORA] unutar te države članice.

Izmjena

4. U mjeri u kojoj je to potrebno za učinkovito izvršavanje zadaća i obveza utvrđenih u ovoj Direktivi, države članice osiguravaju odgovarajuću suradnju između nadležnih tijela i jedinstvenih kontaktnih točaka i tijela za izvršavanje zakonodavstva, tijela za zaštitu podataka i tijela odgovornih za kritičnu infrastrukturu u skladu s Direktivom (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] i nacionalnih finansijskih tijela imenovanih u skladu s Uredbom (EU) XXXX/XXXX Europskog parlamenta i Vijeća 39 [Uredba DORA] unutar te države članice, ***kao i s tijelima za kiberobranu i saznanja o kiberprijetnjama.***

³⁹ [Upisati puni naslov i upućivanje na objavu u SL-u kada budu poznati.]

³⁹ [Upisati puni naslov i upućivanje na objavu u SL-u kada budu poznati.]

Amandman 72
Prijedlog direktive
Članak 12. – stavak 2.

Tekst koji je predložila Komisija

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

Izmjena

2. Skupina za suradnju **redovito se sastaje i** izvršava svoje zadaće na temelju dvogodišnjih programa rada iz stavka 6.

Amandman 73
Prijedlog direktive
Članak 12. – stavak 3. – podstavak 2.

Tekst koji je predložila Komisija

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

Izmjena

Skupina za suradnju može, prema potrebi, pozvati predstavnike relevantnih **tijela i agencija Unije te** dionika, da sudjeluju u njezinu radu.

Amandman 74
Prijedlog direktive
Članak 12. – stavak 4. – točka a

Tekst koji je predložila Komisija

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

Izmjena

(a) pružanje smjernica nadležnim tijelima za prenošenje i provedbu ove Direktive **te promicanje njezine ujednačene provedbe u državama članicama;**

Amandman 75
Prijedlog direktive
Članak 12. – stavak 4. – točka aa (nova)

Tekst koji je predložila Komisija

Izmjena

(aa) razmjenjivanje informacija o političkim prioritetima i ključnim izazovima u području kibersigurnosti te definiranje glavnih ciljeva kibersigurnosti;

Amandman 76

Prijedlog direktive

Članak 12. – stavak 4. – točka ab (nova)

Tekst koji je predložila Komisija

Izmjena

(ab) raspravljanje o nacionalnim strategijama država članica i njihovoj pripravnosti;

Amandman 77

Prijedlog direktive

Članak 12. – stavak 4. – točka c

Tekst koji je predložila Komisija

Izmjena

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

(c) savjetovanje i suradnja s Komisijom u pogledu novih inicijativa kibersigurnosne politike te s Europskom službom za vanjsko djelovanje u pogledu geopolitičkih aspekata kibersigurnosti u Uniji;

Amandman 78

Prijedlog direktive

Članak 12. – stavak 4. – točka f

Tekst koji je predložila Komisija

Izmjena

(f) rasprava o izvješćivanju o istorazinskom ocjenjivanju iz članka 16. stavka 7.;

*(f) rasprava o izvješćivanju o istorazinskom ocjenjivanju iz članka 16. stavka 7., **ocjena njegova djelovanja te donošenje zaključaka i preporuka;***

Amandman 79

Prijedlog direktive

Članak 12. – stavak 4. – točka ka (nova)

Tekst koji je predložila Komisija

Izmjena

(ka) podupiranje ENISA-e u organiziranju zajedničkog osposobljavanja nacionalnih nadležnih tijela na razini EU-a.

Amandman 80
Prijedlog direktive
Članak 12. – stavak 6.

Tekst koji je predložila Komisija

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

Izmjena

6. Do ... **12 mjeseci** od datuma stupanja na snagu ove Direktive, a nakon toga svake dvije godine, skupina za suradnju sastavlja program rada u pogledu mjera koje poduzima za provedbu svojih ciljeva i zadaća. Vremenski okvir prvog programa donesenog na temelju ove Direktive uskladuje se s vremenskim okvirom zadnjeg programa donesenog na temelju Direktive (EU) 2016/1148.

Amandman 81
Prijedlog direktive
Članak 12. – stavak 8.a (novi)

Tekst koji je predložila Komisija

Izmjena

8.a Skupina za suradnju redovito objavljuje sažeto izvješće o svojim aktivnostima, ne dovodeći u pitanje povjerljivost informacija koje razmjenjuje tijekom sastanaka.

Amandman 82
Prijedlog direktive
Članak 13. – stavak 3. – točka a

Tekst koji je predložila Komisija

Izmjena

(a) razmjena informacija o kapacitetima CSIRT-ova;

(a) razmjena informacija o kapacitetima *i pripravnosti* CSIRT-ova;

Amandman 83
Prijedlog direktive
Članak 13. – stavak 3. – točka b

Tekst koji je predložila Komisija

Izmjena

(b) razmjena relevantnih informacija o

(b) razmjena relevantnih informacija o

incidentima, izbjegnutim incidentima, kiberprijetnjama, rizicima i ranjivostima;

incidentima, izbjegnutim incidentima, kiberprijetnjama, rizicima i ranjivostima **te podupiranje operativnih kapaciteta država članica**;

Amandman 84

Prijedlog direktive

Članak 13. – stavak 3. – točka da (nova)

Tekst koji je predložila Komisija

Izmjena

(da) razmjena informacija u vezi s prekograničnim incidentima i raspravljanje o njima;

Amandman 85

Prijedlog direktive

Članak 13. – stavak 3. – točka g – podtočka ia (nova)

Tekst koji je predložila Komisija

Izmjena

(ia) razmjena informacija;

Amandman 86

Prijedlog direktive

Članak 13. – stavak 3. – točka j

Tekst koji je predložila Komisija

Izmjena

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

(j) rasprava o kapacitetima i pripravnosti CSIRT-ova;

Amandman 87

Prijedlog direktive

Članak 13. – stavak 4.

Tekst koji je predložila Komisija

Izmjena

4. Za potrebe preispitivanja iz članka 35. i do □24 mjeseca od datuma stupanja na snagu ove Direktive□, a nakon toga svake **dvije** godine, mreža CSIRT-ova ocjenjuje napredak ostvaren u operativnoj

4. Za potrebe preispitivanja iz članka 35. i do □24 mjeseca od datuma stupanja na snagu ove Direktive□, a nakon toga svake godine, mreža CSIRT-ova ocjenjuje napredak ostvaren u operativnoj

suradnji i priprema izvješće. U izvješću se posebno donose zaključci o ishodima istorazinskih ocjenjivanja iz članka 16. provedenih u pogledu nacionalnih CSIRT-ova, uključujući zaključke i preporuke na temelju tog članka. To se izvješće dostavlja i skupini za suradnju.

Amandman 88

Prijedlog direktive

Članak 14. – stavak 3. – točka a

Tekst koji je predložila Komisija

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

suradnji i priprema izvješće. U izvješću se posebno donose zaključci o ishodima istorazinskih ocjenjivanja iz članka 16. provedenih u pogledu nacionalnih CSIRT-ova, uključujući zaključke i preporuke na temelju tog članka. To se izvješće dostavlja i skupini za suradnju.

Izmjena

(a) povećanje razine pripravnosti za upravljanje incidentima i krizama velikih razmjera, *uključujući prekogranične kiberprijetnje*;

Amandman 89

Prijedlog direktive

Članak 14. – stavak 5.

Tekst koji je predložila Komisija

5. EU-CyCLONe redovito izvješće skupinu za suradnju o kiberprijetnjama, kiberincidentima i kibertrendovima, posvećujući posebnu pažnju njihovu utjecaju na ključne i važne subjekte.

Izmjena

5. EU-CyCLONe redovito izvješće skupinu za suradnju o kiberprijetnjama, kiberincidentima i kibertrendovima, posvećujući posebnu pažnju njihovu utjecaju na ključne i važne subjekte *i njihovu otpornost*.

Amandman 90

Prijedlog direktive

Članak 14. – stavak 6.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 91**Prijedlog direktive****Članak 15. – stavak 1. – uvodni dio***Tekst koji je predložila Komisija*

1. ENISA u suradnji s Komisijom izdaje ***dvogodišnje*** izvješće o stanju kibersigurnosti u Uniji. Izvješćem je posebno obuhvaćena ocjena sljedećeg:

Izmjena

1. ENISA u suradnji s Komisijom izdaje ***godišnje*** izvješće o stanju kibersigurnosti u Uniji ***te ga predstavlja Europskom parlamentu.*** Izvješćem je posebno obuhvaćena ocjena sljedećeg:

Amandman 92**Prijedlog direktive****Članak 15. – stavak 1. – točka a***Tekst koji je predložila Komisija*

(a) razvoja kibersigurnosnih kapaciteta širom Unije;

Izmjena

(a) razvoja kibersigurnosnih kapaciteta širom Unije, ***uključujući opću razinu vještina i kompetencija u kibersigurnosti, ukupnog stupnja otpornosti unutarnjeg tržišta na kiberprijetnje i razine provedbe Direktive u svim državama članicama;***

Amandman 93**Prijedlog direktive****Članak 15. – stavak 1. – točka c***Tekst koji je predložila Komisija*

(c) indeksa kibersigurnosti kojim se omogućuje skupna ocjena razine razvijenosti kibersigurnosnih kapaciteta.

Izmjena

(c) indeksa kibersigurnosti kojim se omogućuje skupna ocjena razine razvijenosti kibersigurnosnih kapaciteta, ***uključujući opću ocjenu kibersigurnosti za potrošače;***

Amandman 94**Prijedlog direktive****Članak 15. – stavak 1. – točka ca (nova)***Tekst koji je predložila Komisija**Izmjena*

(ca) geopolitičkih aspekata koji izravno ili neizravno utječu na kibersigurnost u

Uniji.

Amandman 95

Prijedlog direkture

Članak 16. – stavak 1. – uvodni dio

Tekst koji je predložila Komisija

1. Nakon savjetovanja sa skupinom za suradnju i ENISA-om, a najkasnije **18** mjeseci nakon stupanja na snagu ove Direktive, Komisija utvrđuje metodologiju i sadržaj sustava istorazinskog ocjenjivanja za procjenu učinkovitosti kbersigurnosnih politika država članica. Ocjenjivanja provode tehnički stručnjaci za kbersigurnost iz **država članica različitih** od onih koje se ocjenjuju i obuhvaćaju najmanje sljedeće:

Izmjena

1. Nakon savjetovanja sa skupinom za suradnju i ENISA-om, a najkasnije **12** mjeseci nakon stupanja na snagu ove Direktive, Komisija utvrđuje metodologiju i sadržaj sustava istorazinskog ocjenjivanja za procjenu učinkovitosti kbersigurnosnih politika država članica. Ocjenjivanja provode tehnički stručnjaci za kbersigurnost iz **najmanje dvije države članice i ENISA-e, različite** od onih koje se ocjenjuju, i obuhvaćaju najmanje sljedeće:

Amandman 96

Prijedlog direkture

Članak 16. – stavak 2.

Tekst koji je predložila Komisija

2. Metodologija uključuje objektivne, nediskriminirajuće, pravedne i transparentne kriterije na temelju kojih države članice imenuju stručnjake koji su kvalificirani za provedbu istorazinskih ocjenjivanja. ENISA i Komisija imenuju stručnjake koji kao promatrači sudjeluju u istorazinskom ocjenjivanju. Komisija, uz potporu ENISA-e, u okviru metodologije iz stavka 1. uspostavlja objektivan, nediskriminirajući, pravedan i transparentan sustav za odabir i nasumično raspoređivanje stručnjaka za svako istorazinsko ocjenjivanje.

Izmjena

2. Metodologija uključuje objektivne, nediskriminirajuće, **tehnički neutralne**, pravedne i transparentne kriterije na temelju kojih države članice imenuju stručnjake koji su kvalificirani za provedbu istorazinskih ocjenjivanja. ENISA i Komisija imenuju stručnjake koji kao promatrači sudjeluju u istorazinskom ocjenjivanju. Komisija, uz potporu ENISA-e, u okviru metodologije iz stavka 1. uspostavlja objektivan, nediskriminirajući, pravedan i transparentan sustav za odabir i nasumično raspoređivanje stručnjaka za svako istorazinsko ocjenjivanje.

Amandman 97

Prijedlog direkture

Članak 18. – stavak 1.

Tekst koji je predložila Komisija

1. Države članice osiguravaju da ključni i važni subjekti poduzimaju ***odgovarajuće i razmjerne*** tehničke i organizacijske mjere upravljanja rizicima kojima su izloženi mrežni i informacijski sustavi kojima se ti subjekti služe u pružanju svojih usluga. Uzimajući u obzir najnovija dostignuća, tim se mjerama osigurava razina sigurnosti mrežnih i informacijskih sustava koja odgovara postojećem riziku.

Izmjena

1. Države članice osiguravaju da ključni i važni subjekti poduzimaju tehničke i organizacijske mjere upravljanja rizicima kojima su izloženi mrežni i informacijski sustavi kojima se ti subjekti služe u pružanju svojih usluga. ***Te mjere moraju biti primjerene i razmjerne stupnju kritičnosti sektora ili vrste usluge, kao i stupnju ovisnosti subjekta o drugim sektorima ili vrstama usluga, te se donose nakon procjene temeljene na riziku.*** Uzimajući u obzir najnovija dostignuća, tim se mjerama osigurava razina sigurnosti mrežnih i informacijskih sustava koja odgovara postojećem riziku. ***Konkretno, poduzimaju se mjere za sprečavanje i smanjivanje učinka sigurnosnih incidenata na primatelje njihovih usluga.***

Amandman 98

Prijedlog direkutive

Članak 18. – stavak 2. – točka d

Tekst koji je predložila Komisija

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

Izmjena

(d) ***mjere za procjenu rizika za sigurnost*** lanca opskrbe, uključujući s ***obzirom na*** sigurnosne aspekte u pogledu odnosa između svakog subjekta i njegovih dobavljača ili pružatelja usluga kao što su pružatelji usluga pohrane i obrade podataka ili upravljanju sigurnosnih usluga;

Amandman 99

Prijedlog direkitive

Članak 18. – stavak 2. – točka f

Tekst koji je predložila Komisija

(f) politike i postupke (testiranje i revizija) za procjenu učinkovitosti mjeri upravljanja kibersigurnosnim rizicima;

Izmjena

(f) politike i postupke (testiranje i revizija) ***te redovite vježbe u području kibersigurnosti*** za procjenu učinkovitosti mjeri upravljanja kibersigurnosnim

rizicima;

Amandman 100

Prijedlog direktive

Članak 18. – stavak 2. – točka g

Tekst koji je predložila Komisija

(g) primjenu kriptografije **i** šifriranja.

Izmjena

(g) primjenu kriptografije, **šifriranja, a posebno** šifriranja s kraja na kraj;

Amandman 101

Prijedlog direktive

Članak 18. – stavak 2. – točka ga (nova)

Tekst koji je predložila Komisija

Izmjena

(ga) politike kojima se osigurava odgovarajuće osposobljavanje i senzibilizacija u području kibersigurnosti;

Amandman 102

Prijedlog direktive

Članak 18. – stavak 3.

Tekst koji je predložila Komisija

3. Države članice osiguravaju da subjekti pri razmatranju odgovarajućih mjera iz stavka 2. točke (d) uzimaju u obzir ranjivosti specifične za svakog dobavljača i pružatelja usluge te opću kvalitetu proizvoda i kibersigurnosnu praksu svojih dobavljača i pružatelja usluga, uključujući njihove sigurne razvojne postupke.

Izmjena

3. Države članice osiguravaju da subjekti, **ako imaju pristup relevantnim informacijama**, pri razmatranju odgovarajućih mjera iz stavka 2. točke (d) uzimaju u obzir ranjivosti specifične za svakog dobavljača i pružatelja usluge te opću kvalitetu proizvoda i kibersigurnosnu praksu svojih dobavljača i pružatelja usluga, uključujući njihove sigurne razvojne postupke.

Amandman 103

Prijedlog direktive

Članak 18. – stavak 5.

Tekst koji je predložila Komisija

5. Komisija **može donijeti provedbene akte** kako bi utvrdila tehničke i metodološke specifikacije elemenata iz stavka 2. ***U pripremi tih akata Komisija djeluje u skladu s postupkom ispitivanja iz članka 37. stavka 2.*** i slijedi, u što većoj mjeri, međunarodne i europske norme, kao i relevantne tehničke specifikacije.

Amandman 104
Prijedlog direktive
Članak 18. – stavak 6.

Tekst koji je predložila Komisija

6. Komisija **je ovlaštena donijeti delegirane akte u skladu s člankom 36. radi dopune elemenata utvrđenih u stavku 2.** kako bi se u obzir uzele nove kibernetički razvoj ili sektorske posebnosti.

Amandman 105
Prijedlog direktive
Članak 19. – stavak 1.

Tekst koji je predložila Komisija

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

Amandman 106
Prijedlog direktive
Članak 20. – stavak 1.

Izmjena

5. Komisija **je ovlaštena donositi delegirane** akte kako bi utvrdila tehničke i metodološke specifikacije elemenata iz stavka 2., te slijedi, u što većoj mjeri, međunarodne i europske norme, kao i relevantne tehničke specifikacije. ***U razvoju delegiranih akata Komisija se savjetuje i sa svim relevantnim dionicicima.***

Izmjena

6. Komisija **u suradnji sa skupinom za suradnju i ENISA-om pruža smjernice i najbolje prakse u pogledu razmjerne usklađenosti subjekata sa zahtjevima, koji su utvrđeni u stavku 2., a posebno sa zahtjevom iz točke (d) tog stavka.**

Izmjena

1. **Kako bi se povećala ukupna razina kibersigurnosti, skupina** za suradnju, zajedno s Komisijom i ENISA-om, može provoditi koordinirane procjene sigurnosnih rizika za određene ključne lance opskrbe IKT uslugama, sustavima ili proizvodima, uzimajući u obzir tehničke i, prema potrebi, netehničke čimbenike rizika, **kao što su geopolitički rizici.**

Tekst koji je predložila Komisija

1. Države članice osiguravaju da ključni i važni subjekti bez nepotrebne odgode obavješćuju nadležna tijela ili CSIRT u skladu sa stavcima 3. i 4. o svakom incidentu koji ima znatan učinak na pružanje njihovih usluga. Prema potrebi, ti subjekti bez nepotrebne odgode obavješćuju primatelje svojih usluga o incidentima koji bi mogli negativno utjecati na pružanje tih usluga. Države članice osiguravaju da ti subjekti, među ostalim, prijavljuju sve informacije koje nadležnim tijelima ili CSIRT-ovima omogućuju da utvrde sve prekogranične učinke incidenta.

Izmjena

1. Države članice osiguravaju da ključni i važni subjekti bez nepotrebne odgode obavješćuju nadležna tijela ili CSIRT u skladu sa stavcima 3. i 4. o svakom incidentu koji ima znatan učinak na pružanje njihovih usluga **ili o svakom izbjegnutom incidentu**. Prema potrebi, ti subjekti bez nepotrebne odgode obavješćuju primatelje svojih usluga o incidentima koji bi mogli negativno utjecati na pružanje tih usluga. Države članice osiguravaju da ti subjekti, među ostalim, prijavljuju sve informacije koje nadležnim tijelima ili CSIRT-ovima omogućuju da utvrde sve prekogranične učinke **incidenta ili izbjegnutog** incidenta.

Amandman 107

Prijedlog direktive

Članak 20. – stavak 1.a (novi)

Tekst koji je predložila Komisija

Izmjena

1.a U svrhu pojednostavljenja obveza izvješćivanja, države članice uspostavljaju jedinstvenu ulaznu točku za sve obavijesti koje se zahtijevaju ovom Direktivom i drugim pravom Unije, kao što su Uredba (EU) 2016/679 i Direktiva 2002/58/EZ.

Amandman 108

Prijedlog direktive

Članak 20. – stavak 1.b (novi)

Tekst koji je predložila Komisija

Izmjena

1.b U suradnji sa skupinom za suradnju ENISA izrađuje zajedničke predloške za obavješćivanje pomoći smjernica kojima bi se pojednostavnile i uskladile izvještajne informacije koje se zahtijevaju pravom Unije, čime bi se smanjilo opterećenje za poduzeća.

Amandman 109
Prijedlog direktive
Članak 20. – stavak 2. – podstavak 1.

Tekst koji je predložila Komisija

Izmjena

2. *Države članice osiguravaju da ključni i važni subjekti bez nepotrebne odgode obavješćuju nadležna tijela ili CSIRT o svim ozbiljnim kiberprijetnjama za koje ti subjekti utvrde da bi mogle dovesti do ozbiljnog incidenta.*

Briše se.

Amandman 110
Prijedlog direktive
Članak 20. – stavak 2. – podstavak 2.

Tekst koji je predložila Komisija

Izmjena

Ako je primjenjivo, ti subjekti bez nepotrebne odgode obavješćuju primatelje svojih usluga na koje bi mogla utjecati ozbiljna kiberprijetnja o svim mjerama ili pravnim lijekovima koje ti primatelji mogu poduzeti kao odgovor na tu prijetnju. Prema potrebi, subjekti isto tako obavješćuju te primatelje o samoj prijetnji. Subjekt koji šalje obavijest ne podliježe zbog toga povećanoj odgovornosti.

Briše se.

Amandman 111
Prijedlog direktive
Članak 20. – stavak 3. – točka a

Tekst koji je predložila Komisija

Izmjena

(a) ako je uzrokovao *ili može uzrokovati* znatne poremećaje u radu ili finansijske gubitke za predmetni subjekt;

(a) ako je uzrokovao znatne poremećaje u radu ili finansijske gubitke za predmetni subjekt;

Amandman 112**Prijedlog direktive****Članak 20. – stavak 3. – točka b***Tekst koji je predložila Komisija*

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

Izmjena

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

Amandman 113**Prijedlog direktive****Članak 20. – stavak 3.a (novi)***Tekst koji je predložila Komisija**Izmjena*

3.a Komisija je ovlaštena donijeti delegirane akte u skladu s člankom 36. radi dopune ove Uredbe određivanjem vrste informacija koje se dostavljaju u skladu sa stavkom 1. ovog članka i dalnjim određivanjem slučajeva u kojima se incident smatra ozbiljnim kako je navedeno u stavku 3. ovog članka.

Amandman 114**Prijedlog direktive****Članak 20. – stavak 4. – točka -a (nova)***Tekst koji je predložila Komisija**Izmjena*

(-a) rano upozorenje u roku od 24 sata nakon dobivanja informacija o incidentu, bez ikakve obveze subjekta u pogledu otkrivanja dodatnih informacija o incidentu;

Amandman 115**Prijedlog direktive****Članak 20. – stavak 4. – točka a***Tekst koji je predložila Komisija**Izmjena*

(a) bez nepotrebne odgode, a u svakom

(a) bez nepotrebne odgode, a u svakom

slučaju u roku od **24** sata od primitka informacije o incidentu, prvu obavijest u kojoj se, prema potrebi, navodi pretpostavlja li se da je incident uzrokovani nezakonitim ili zlonamjernim djelovanjem;

slučaju u roku od **72** sata od primitka informacije o incidentu, prvu obavijest u kojoj se, prema potrebi, navodi pretpostavlja li se da je incident uzrokovani nezakonitim ili zlonamjernim djelovanjem;

Amandman 116

Prijedlog direktive

Članak 20. – stavak 4. – točka c – uvodni dio

Tekst koji je predložila Komisija

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

Izmjena

(c) ***sveobuhvatno*** izvješće najkasnije ***tri mjeseca*** nakon podnošenja obavijesti iz točke (a), koje uključuje najmanje sljedeće:

Amandman 117

Prijedlog direktive

Članak 20. – stavak 4. – točka c – podtočka i

Tekst koji je predložila Komisija

i. ***detaljni*** opis incidenta, njegovu ozbiljinost i učinak;

Izmjena

i. ***detaljniji*** opis incidenta, njegovu ozbiljinost i učinak;

Amandman 118

Prijedlog direktive

Članak 20. – stavak 4. – točka ca (nova)

Tekst koji je predložila Komisija

Izmjena

(ca) u slučaju incidenta koji traje u trenutku podnošenja sveobuhvatnog izvješća u skladu s točkom (c), završno izvješće dostavlja se jedan mjesec nakon što je incident ublažen;

Amandman 119

Prijedlog direktive

Članak 20. – stavak 7.

Tekst koji je predložila Komisija

Izmjena

7. Ako je za sprečavanje incidenta ili

7. Ako je za sprečavanje incidenta ili

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

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

Amandman 120
Prijedlog direktive
Članak 20. – stavak 8.

Tekst koji je predložila Komisija

8. Na zahtjev nadležnog tijela ili CSIRT-a jedinstvena kontaktna točka prosljeđuje obavijesti primljene na temelju **stavaka 1. i 2.** jedinstvenim kontaktnim točkama drugih pogodjenih država članica.

Izmjena

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

Amandman 121
Prijedlog direktive
Članak 20. – stavak 9.

Tekst koji je predložila Komisija

9. Jedinstvena kontaktna točka jedanput mjesečno podnosi ENISA-i sažeto izvješće koje uključuje anonimizirane i agregirane podatke o incidentima, ozbiljnim kiberprijetnjama i izbjegnutim incidentima prijavljenima u skladu sa **stavcima 1. i 2.** te u skladu s člankom 27. Kako bi se doprinijelo tome da dostavljeni podaci budu usporedivi, ENISA može izdati tehničke smjernice o parametrima za informacije uključene u sažeto izvješće.

Izmjena

9. Jedinstvena kontaktna točka jedanput mjesečno podnosi ENISA-i sažeto izvješće koje uključuje anonimizirane i agregirane podatke o incidentima, ozbiljnim kiberprijetnjama i izbjegnutim incidentima prijavljenima u skladu sa **stavkom 1.** te u skladu s člankom 27. Kako bi se doprinijelo tome da dostavljeni podaci budu usporedivi, ENISA može izdati tehničke smjernice o parametrima za informacije uključene u sažeto izvješće.

Amandman 122
Prijedlog direktive
Članak 20. – stavak 10.

Tekst koji je predložila Komisija

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

Amandman 123
Prijedlog direkutive
Članak 20. – stavak 11.

Tekst koji je predložila Komisija

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

Amandman 124
Prijedlog direkutive
Članak 21. – stavak 1.

Tekst koji je predložila Komisija

1. Kako bi dokazale usklađenost s određenim zahtjevima iz članka 18., države članice **mogu zahtijevati da ključni i važni subjekti** certificiraju određene IKT proizvode, IKT usluge i IKT procese u okviru posebnih europskih programa

Izmjena

10. Nadležna tijela dostavljaju nadležnim tijelima imenovanima u skladu s Direktivom (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] informacije o incidentima i kibernetičkim događajima koje su u skladu sa stavkom 1. prijavili ključni subjekti koji su identificirani kao kritični subjekti ili kao subjekti istovjetni kritičnim subjektima, u skladu s Direktivom (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata].

Izmjena

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

Izmjena

1. Kako bi dokazale usklađenost s određenim zahtjevima iz članka 18. *i povećale razinu kibersigurnosti*, države članice, **nakon savjetovanja sa skupinom za suradnju i ENISA-om, potiču ključne i važne subjekte da** certificiraju određene

kibersigurnosne certifikacije donesenih u skladu s člankom 49. Uredbe (EU) 2019/881. *Proizvode, usluge i procese koji podliježu certifikaciji mogu razviti ključni ili važni subjekti ili se mogu nabaviti od trećih strana.*

IKT proizvode, IKT usluge i IKT procese, *bez obzira na to je li ih razvio ključni ili važan subjekt ili su nabavljeni od treće strane*, u okviru posebnih europskih programa kibersigurnosne certifikacije donesenih u skladu s člankom 49. Uredbe (EU) 2019/881 *ili u okviru sličnih međunarodno priznatih programa certifikacije. Kad god je to moguće, države članice potiču primjenu donesenih certifikacijskih programa na usklađen način.*

**Amandman 125
Prijedlog direktive
Članak 21. – stavak 2.**

Tekst koji je predložila Komisija

2. Komisija je ovlaštena donositi delegirane akte kojima se određuje koje kategorije ključnih subjekata ***moraju pribaviti certifikat*** i na temelju kojih posebnih europskih programa kibersigurnosne certifikacije u skladu sa stavkom 1. ***Delegirani akti donose se u skladu s člankom 36.***

Izmjena

2. Komisija redovito procjenjuje učinkovitost i upotrebu donesenih europskih programa kibersigurnosne certifikacije iz članka 49. Uredbe (EU) 2019/881 i utvrđuju koje se kategorije ključnih subjekata ***potiču da pribave certifikat*** i na temelju kojih posebnih europskih programa kibersigurnosne certifikacije u skladu sa stavkom 1.

**Amandman 126
Prijedlog direktive
Članak 22. – stavak -1. (novi)**

Tekst koji je predložila Komisija

Izmjena

-1. Komisija u suradnji s ENISA-om podupire i promiče razvoj i provedbu normi koje utvrđuju relevantna normizacijska tijela Unije i međunarodna normizacijska tijela za konvergentnu provedbu članka 18. stavaka 1. i 2. Komisija podupire ažuriranje normi s obzirom na tehnološki razvoj.

Amandman 127
Prijedlog direktive
Članak 22. – stavak 1.

Tekst koji je predložila Komisija

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

Izmjena

1. Države članice, u cilju promicanja konvergentne provedbe članka 18. stavaka 1. i 2., bez nametanja ili diskriminacije određene vrste tehnologije, *i u skladu sa smjernicama ENISA-e i skupine za suradnju* potiču primjenu europskih ili međunarodno priznatih normi i specifikacija relevantnih za sigurnost mrežnih i informacijskih sustava.

Amandman 128
Prijedlog direktive
Članak 23. – naslov

Tekst koji je predložila Komisija

Baze podataka s nazivima domena i registracijskim podacima

Izmjena

Infrastruktura baze podataka s nazivima domena i registracijskim podacima

Amandman 129
Prijedlog direktive
Članak 23. – stavak 1.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 130
Prijedlog direktive
Članak 23. – stavak 2.

Tekst koji je predložila Komisija

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

Izmjena

2. Države članice osiguravaju da *infrastruktura* baze podataka o registraciji naziva domena iz stavka 1. *sadržava* relevantne informacije, *koje uključuju barem ime korisnika domene, njegovu fizičku adresu i adresu elektroničke pošte te telefonski broj, koji su potrebni* za identifikaciju i kontakt nositelja naziva domena te kontaktnih točaka koje upravljaju nazivima domena u okviru vršnih domena, *što uključuje barem ime korisnika domene, fizičku adresu, adresu elektroničke pošte i telefonski broj.*

Amandman 131
Prijedlog direktive
Članak 23. – stavak 3.

Tekst koji je predložila Komisija

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

Izmjena

3. Države članice osiguravaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu uspostave politike i postupke kojima se osigurava da *infrastruktura* baze podataka *sadržava točne, provjerene* i potpune informacije *te da bi netočne ili nepotpune podatke korisnik domene trebao bez odgode ispraviti ili izbrisati.* Države članice osiguravaju da su takve politike i postupci javno dostupni.

Amandman 132
Prijedlog direktive
Članak 23. – stavak 4.

Tekst koji je predložila Komisija

4. Države članice osiguravaju da

Izmjena

4. Države članice osiguravaju da

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

registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena **bez nepotrebne odgode, a u svakom slučaju unutar 24 sata od** registracije naziva domene objave **svepodatke** o registraciji domene **pravnih osoba kao korisnika domene.**

Amandman 133
Prijedlog direktive
Članak 23. – stavak 5.

Tekst koji je predložila Komisija

5. Države članice osiguravaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena **za vršnu domenu omoguće** pristup određenim podacima o registraciji naziva domena **na temelju zakonitih i opravdanih zahtjeva legitimnih tražitelja pristupa, u skladu s pravom Unije o zaštiti podataka.** Države članice osiguravaju da registri **naziva** vršnih domena i subjekti koji pružaju usluge registracije naziva domena **za vršnu domenu bez nepotrebne odgode** odgovaraju na sve zahtjeve za pristup. Države članice osiguravaju javnu dostupnost politika i postupaka za objavljivanje takvih podataka. Odjeljak II. Nadležnost i registracija Članak 24. Nadležnost i teritorijalnost

Izmjena

5. Države članice osiguravaju da **su** registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena **obvezni omogućiti** pristup određenim podacima o registraciji naziva domena, **uključujući osobne podatke, na temelju** opravdanih zahtjeva legitimnih tražitelja pristupa, u skladu s pravom Unije o zaštiti podataka. Države članice osiguravaju da registri vršnih domena i subjekti koji pružaju usluge registracije naziva domena **bez nepotrebne odgode, a u svakom slučaju u roku od 72 sata** odgovaraju na sve **zakonite i opravdane** zahtjeve za pristup. Države članice osiguravaju javnu dostupnost politika i postupaka za objavljivanje takvih podataka. Odjeljak II. Nadležnost i registracija Članak 24. Nadležnost i teritorijalnost

Amandman 134
Prijedlog direktive
Članak 24. – stavak 2.

Tekst koji je predložila Komisija

2. Za potrebe ove Direktive smatra se da subjekti iz stavka 1. imaju glavni poslovni nastan u Uniji u državi članici u kojoj se donose odluke povezane s mjerama upravljanja kibersigurnosnim

Izmjena

2. Za potrebe ove Direktive smatra se da subjekti iz stavka 1. imaju glavni poslovni nastan u Uniji u državi članici u kojoj se donose odluke povezane s mjerama upravljanja kibersigurnosnim

rizicima. Ako se takve odluke ne donose ni u jednoj poslovnoj jedinici u Uniji, smatra se da se glavni poslovni nastan nalazi u državi članici u kojoj subjekti imaju poslovnu jedinicu s najvećim brojem zaposlenika u Uniji.

rizicima. Ako se takve odluke ne donose ni u jednoj poslovnoj jedinici u Uniji, smatra se da se glavni poslovni nastan nalazi u državi članici u kojoj subjekti imaju poslovnu jedinicu s najvećim brojem zaposlenika u Uniji. **To se provodi na način kojim se osigurava da regulatorno tijelo jedne države članice ne preuzme nerazmjerne opterećenje.**

Amandman 135

Prijedlog direktive

Članak 25. – stavak 1. – uvodni dio

Tekst koji je predložila Komisija

1. ENISA uspostavlja i vodi registar za ključne i važne subjekte iz članka 24. stavka 1. Najkasnije do [12 mjeseci nakon stupanja na snagu ove Direktive] subjekti dostavljaju ENISA-i sljedeće informacije:

Izmjena

1. ENISA uspostavlja i vodi registar za ključne i važne subjekte iz članka 24. stavka 1. **Za te potrebe**, najkasnije do [12 mjeseci nakon stupanja na snagu ove Direktive] subjekti dostavljaju ENISA-i sljedeće informacije:

Amandman 136

Prijedlog direktive

Članak 26. – stavak 1. – točka b

Tekst koji je predložila Komisija

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

Izmjena

(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 *i sprečavanja* prijetnji, strategijama ublažavanja ili fazama odgovora i oporavka.

Amandman 137

Prijedlog direktive

Članak 26. – stavak 3.

Tekst koji je predložila Komisija

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

Izmjena

3. Države članice utvrđuju **smjernice** kojima se određuju postupak, operativni elementi (uključujući upotrebu namjenskih IKT platformi), sadržaj i uvjeti mehanizama za razmjenu informacija iz stavka 2. **Takve smjernice uključuju** i pojedinosti o sudjelovanju, **prema potrebi**, javnih tijela i **neovisnih stručnjaka** u takvim mehanizmima, kao i operativni elementi, uključujući upotrebu namjenskih informatičkih platformi. Države članice nude potporu primjeni takvih mehanizama u skladu sa svojim politikama iz članka 5. stavka 2. točke (g).

Amandman 138
Prijedlog direktive
Članak 26. – stavak 5.

Tekst koji je predložila Komisija

5. U skladu s pravom Unije, ENISA podupire uspostavu mehanizama za razmjenu informacija o kibersigurnosti iz stavka 2. pružanjem primjera najbolje prakse i smjernica.

Izmjena

5. U skladu s pravom Unije, ENISA podupire uspostavu mehanizama za razmjenu informacija o kibersigurnosti iz stavka 2. pružanjem primjera najbolje prakse i smjernica **te olakšavanjem razmjene informacija na razini Unije, uz istodobnu zaštitu poslovno osjetljivih informacija. Skupina za suradnju poziva se da, na zahtjev ključnih i važnih subjekata, stavi na raspolaganje najbolje prakse i smjernice.**

Amandman 139
Prijedlog direktive
Članak 27. – stavak -1. (novi)

Tekst koji je predložila Komisija

Izmjena

-1. Države članice jamče da ključni i važni subjekti mogu na dobrovoljnoj osnovi podnosići obavijesti o kiberprijetnjama za koje ti subjekti utvrde

da su potencijalno mogle dovesti do ozbiljnog incidenta. Države članice jamče da, za potrebe tih obavijesti, subjekti djeluju u skladu s postupkom utvrđenim u članku 20. Dobrovoljno obavješćivanje ne smije dovesti do nametanja dodatnih obveza subjektu koji je podnio obavijest.

Amandman 140
Prijedlog direktive
Članak 27. – stavak 1.

Tekst koji je predložila Komisija

Ne dovodeći u pitanje članak 3., države članice osiguravaju da subjekti koji nisu obuhvaćeni područjem primjene ove Direktive mogu dobrovoljno podnosi obavijesti o ozbiljnim incidentima, kiberprijetnjama ili izbjegnutim incidentima. Pri obradi obavijesti države članice djeluju u skladu s postupkom utvrđenim u članku 20. Države članice obradi obveznih obavijesti **mogu dati** prednost pred obradom obavijesti na dobrovoljnoj osnovi. Subjektu koji je obavijest podnio dobrovoljno ne smiju se zbog tog obavješćivanja nametati dodatne obveze kojima ne bi podlijegao da nije podnio tu obavijest.

Izmjena

I. *Ne* dovodeći u pitanje članak 3., države članice osiguravaju da subjekti koji nisu obuhvaćeni područjem primjene ove Direktive mogu dobrovoljno podnosi obavijesti o ozbiljnim incidentima, kiberprijetnjama ili izbjegnutim incidentima. Pri obradi obavijesti države članice djeluju u skladu s postupkom utvrđenim u članku 20. Države članice obradi obveznih obavijesti **daju** prednost pred obradom obavijesti na dobrovoljnoj osnovi. Subjektu koji je obavijest podnio dobrovoljno ne smiju se zbog tog obavješćivanja nametati dodatne obveze kojima ne bi podlijegao da nije podnio tu obavijest, **ali država članica može mu odobriti pomoć CSIRT-ova.**

Amandman 141
Prijedlog direktive
Članak 28. – stavak 1.

Tekst koji je predložila Komisija

1. Države članice osiguravaju da nadležna tijela djelotvorno prate i poduzimaju mjere potrebne za osiguravanje usklađenosti s ovom Direktivom, posebno s obvezama utvrđenima u člancima 18. i 20.

Izmjena

1. Države članice osiguravaju da nadležna tijela djelotvorno prate i poduzimaju mjere potrebne za osiguravanje usklađenosti s ovom Direktivom, posebno s obvezama utvrđenima u člancima 18. i 20., **te da su im pružena odgovarajuća sredstva za izvršavanje njihove funkcije.**

Amandman 142
Prijedlog direktive
Članak 28. – stavak 2.

Tekst koji je predložila Komisija

2. Nadležna tijela blisko surađuju s tijelima za zaštitu podataka u rješavanju incidenata koji za posljedicu imaju povrede osobnih podataka.

Izmjena

2. Nadležna tijela blisko surađuju s tijelima za zaštitu podataka u rješavanju incidenata koji za posljedicu imaju povrede osobnih podataka, *uključujući, prema potrebi, tijela za zaštitu podataka iz drugih država članica.*

Amandman 143
Prijedlog direktive
Članak 29. – stavak 2. – točka c

Tekst koji je predložila Komisija

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

Izmjena

(c) ciljane revizije sigurnosti na temelju procjena rizika ili dostupnih informacija povezanih s rizikom *koje provodi kvalificirano neovisno tijelo ili nadležno tijelo;*

Amandman 144
Prijedlog direktive
Članak 29. – stavak 2. – točka f

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 145
Prijedlog direktive
Članak 29. – stavak 3.

Tekst koji je predložila Komisija

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

Izmjena

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

određuju tražene informacije.

određuju tražene informacije *i ograničavaju svoje zahtjeve na opseg incidenta ili problema koji izaziva zabrinutost.*

Amandman 146

Prijedlog direktive

Članak 29. – stavak 5. – podstavak 1. – točka a

Tekst koji je predložila Komisija

(a) obustaviti ili zatražiti od certifikacijskog ili tijela koje izdaje ovlaštenja da obustavi certificiranje ili izdavanje ovlaštenja povezanih s *dijelom ili svim* uslugama koje ključni subjekt pruža ili s djelatnostima koje obavlja;

Izmjena

(a) obustaviti ili zatražiti od certifikacijskog ili tijela koje izdaje ovlaštenja da obustavi certificiranje ili izdavanje ovlaštenja povezanih s *relevantnim* uslugama koje ključni subjekt pruža ili s djelatnostima koje obavlja;

Amandman 147

Prijedlog direktive

Članak 29. – stavak 5. – podstavak 1. – točka b

Tekst koji je predložila Komisija

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

Izmjena

Briše se.

Amandman 148

Prijedlog direktive

Članak 30. – stavak 1.

Tekst koji je predložila Komisija

1. Kada dobiju dokaz ili naznaku da važan subjekt ne ispunjava obveze utvrđene u ovoj Direktivi, a posebno u člancima 18. i 20., države članice

Izmjena

1. Kada dobiju dokaz ili naznaku da važan subjekt ne ispunjava obveze utvrđene u ovoj Direktivi, a posebno u člancima 18. i 20., države članice

osiguravaju da nadležna tijela, ako je potrebno, poduzmu ex post nadzorne mјere.

osiguravaju da nadležna tijela, ako je potrebno, ***te uzimajući u obzor pristup temeljen na riziku***, poduzmu ex post nadzorne mјere.

Amandman 149

Prijedlog direktive

Članak 30. – stavak 2. – točka b

Tekst koji je predložila Komisija

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

Izmjena

(b) ciljane revizije sigurnosti na temelju procjena rizika ili dostupnih informacija povezanih s rizikom ***koje provodi kvalificirano neovisno tijelo ili nadležno tijelo;***

Amandman 150

Prijedlog direktive

Članak 30. – stavak 3.

Tekst koji je predložila Komisija

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

Izmjena

3. Pri izvršavanju svojih ovlasti iz stavka 2. točaka (d) ili (e) nadležna tijela navode svrhu zahtjeva, pobliže određuju tražene informacije ***i ograničavaju opseg incidenta ili problema koji izaziva zabrinutost.***

Amandman 151

Prijedlog direktive

Članak 31. – stavak 4.

Tekst koji je predložila Komisija

4. Države članice osiguravaju da povrede obveza utvrđenih u članku 18. ili članku 20. podliježu, u skladu sa stavcima 2. i 3. ovog članka, upravnim novčanim kaznama u maksimalnom iznosu od ***najmanje*** 10 000 000 EUR ili do 2 % ukupnog godišnjeg prometa na svjetskoj razini poduzeća kojem pripada ključni ili važni subjekt u prethodnoj finansijskoj

Izmjena

4. Države članice osiguravaju da povrede obveza utvrđenih u članku 18. ili članku 20. podliježu, u skladu sa stavcima 2. i 3. ovog članka, upravnim novčanim kaznama u maksimalnom iznosu od 10 000 000 EUR ili do 2 % ukupnog godišnjeg prometa na svjetskoj razini poduzeća kojem pripada ključni ili važni subjekt u prethodnoj finansijskoj godini,

godini, ovisno o tome koji je iznos veći.

ovisno o tome koji je iznos veći.

Amandman 152
Prijedlog direktive
Članak 32. – stavak 1.

Tekst koji je predložila Komisija

1. Ako nadležna tijela imaju naznake da povreda obveza utvrđenih u člancima 18. i 20. koju je počinio ključni ili važni subjekt obuhvaća povredu osobnih podataka iz članka 4. stavka 12. Uredbe (EU) 2016/679 o kojoj se obavještuje u skladu s člankom 33. te uredbe, ***u razumnom roku*** obavješćuju nadzorna tijela nadležna u skladu s člancima 55. i 56. te uredbe.

Izmjena

1. Ako nadležna tijela imaju naznake da povreda obveza utvrđenih u člancima 18. i 20. koju je počinio ključni ili važni subjekt obuhvaća povredu osobnih podataka iz članka 4. stavka 12. Uredbe (EU) 2016/679 o kojoj se obavještuje u skladu s člankom 33. te uredbe, obavješćuju nadzorna tijela nadležna u skladu s člancima 55. i 56. te uredbe ***bez nepotrebne odgode i u svakom slučaju u roku od 72 sata.***

Amandman 153
Prijedlog direktive
Članak 32. – stavak 3.

Tekst koji je predložila Komisija

3. Ako je nadzorno tijelo nadležno u skladu s Uredbom (EU) 2016/679 osnovano u državi članici drugačijoj od one u kojoj je osnovano nadležno tijelo, nadležno tijelo ***može obavijestiti*** nadzorno tijelo osnovano u istoj državi članici.

Izmjena

3. Ako je nadzorno tijelo nadležno u skladu s Uredbom (EU) 2016/679 osnovano u državi članici drugačijoj od one u kojoj je osnovano nadležno tijelo, nadležno tijelo ***obavješće i*** nadzorno tijelo osnovano u istoj državi članici.

Amandman 154
Prijedlog direktive
Članak 36. – stavak 2.

Tekst koji je predložila Komisija

2. Ovlast za donošenje delegiranih akata iz članka 18. stavka **6.** i članka **21.** stavka **2.** dodjeljuje se Komisiji na pet godina počevši od [...].

Izmjena

2. Ovlast za donošenje delegiranih akata iz članka 18. stavka **5.** i članka **20.** stavka **3.** dodjeljuje se Komisiji na pet godina počevši od [...].

Amandman 155
Prijedlog direktive
Članak 36. – stavak 3.

Tekst koji je predložila Komisija

3. *Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 18. stavka 6. i članka 21. 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.*

Amandman 156
Prijedlog direktive
Članak 36. – stavak 6.

Tekst koji je predložila Komisija

6. Delegirani akt donesen na temelju članka 18. stavka 6. i članka 21. 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 nikakav 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.

Izmjena

3. *Delegirani akt donesen na temelju članka 18. stavka 5. i članka 20. stavka 3. stupa na snagu samo ako ni Europski parlament ni Vijeće u roku od tri mjeseca od priopćenja tog akta Europskom parlamentu i Vijeću na njega ne podnesu nikakav prigovor ili ako su prije isteka tog roka i Europski parlament i Vijeće obavijestili Komisiju da neće podnijeti prigovore. Taj se rok produljuje za tri mjeseca na inicijativu Europskog parlamenta ili Vijeća.*

Izmjena

6. Delegirani akt donesen na temelju članka 18. stavka 5. i članka 20. stavka 3. 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 nikakav 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.

**PRILOG: POPIS SUBJEKATA ILI OSOBA
OD KOJIH JE IZVJESTITELJ PRIMIO INFORMACIJE**

Sljedeći popis sastavljen je na isključivo dobrovoljnoj osnovi pod izričitom odgovornošću izvjestitelja. Izvjestiteljica je primila informacije od sljedećih subjekata ili osoba tijekom pripreme izvješća do njegova usvajanja u odboru:

Osoba	Subjekt
	BSA (The Software Alliance)
	BusinessEurope
	Confederation of Danish Industries
	Danish Permanent Representation
	Deutsche Telekom
	Digital Europe
	DOT Europe
	ETNO (European Telecommunications Network Operators)
	French Permanent Representation
	German Permanent Representation
	HUAWEI
	IFPI
	INTEL
	ITI (The Information Technology Industry Council)
	Kaspersky
	MÆRSK
	Microsoft
	ICANN
	MOTION PICTURE ASSOCIATION
	Orgalim
	Palo Alto Networks

POSTUPAK U ODBORU KOJI DAJE MIŠLJENJE

Naslov	Measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148	
Referentni dokumenti	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)	
Nadležni odbor Datum objave na plenarnoj sjednici	ITRE	21.1.2021
Odbori koji su dali mišljenje Datum objave na plenarnoj sjednici	IMCO	21.1.2021
Rapporteur for the opinion Datum imenovanja	Morten Løkkegaard	9.2.2021
Razmatranje u odboru	26.5.2021	21.6.2021
Datum usvajanja	12.7.2021	
Rezultat konačnog glasovanja	+:	42
	-:	1
	0:	2
Zastupnici nazočni na konačnom glasovanju	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Brando Benifei, Adam Bielan, Hynek Blaško, Biljana Borzan, Vlad-Marius Botoş, Markus Buchheit, Andrea Caroppo, Anna Cavazzini, Dita Charanzová, Deirdre Clune, David Cormand, Carlo Fidanza, Evelyne Gebhardt, Alexandra Geese, Sandro Gozi, Maria Grapini, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Marcel Kolaja, Kateřina Konečná, Andrey Kovatchev, Jean-Lin Lacapelle, Maria-Manuel Leitão-Marques, Morten Løkkegaard, Antonius Manders, Leszek Miller, Anne-Sophie Pelletier, Miroslav Radačovský, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róza Thun und Hohenstein, Marco Zullo	
Zamjenici nazočni na konačnom glasovanju	Clara Aguilera, Maria da Graça Carvalho, Christian Doleschal, Claude Gruffat, Jiří Pospíšil, Kosma Złotowski	

POIMENIČNO KONAČNO GLASOVANJE U ODBORU KOJI DAJE MIŠLJENJE

42	+
ECR	Adam Bielan, Carlo Fidanza, Kosma Złotowski
ID	Alessandra Basso, Hynek Blaško, Markus Buchheit, Virginie Joron, Jean-Lin Lacapelle
PPE	Pablo Arias Echeverría, Andrea Caroppo, Maria da Graça Carvalho, Deirdre Clune, Christian Doleschal, Andrey Kovatchev, Antonius Manders, Jiří Pospíšil, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róza Thun und Hohenstein
Renew	Andrus Ansip, Vlad-Marius Botoș, Dita Charanzová, Sandro Gozi, Morten Løkkegaard, Marco Zullo
S&D	Alex Agius Saliba, Clara Aguilera, Brando Benifei, Biljana Borzan, Evelyne Gebhardt, Maria Grapini, Maria-Manuel Leitão-Marques, Leszek Miller, Christel Schaldemose
The Left	Kateřina Konečná, Anne-Sophie Pelletier
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Claude Gruffat, Marcel Kolaja

1	-
NI	Miroslav Radačovský

2	0
ECR	Eugen Jurzyca
Renew	Svenja Hahn

Korišteni znakovi:

- + : za
- : protiv
- 0 : suzdržani