2023/2841

18.12.2023.

UREDBA (EU, Euratom) 2023/2841 EUROPSKOG PARLAMENTA I VIJEĆA

od 13. prosinca 2023.

o utvrđivanju mjera za visoku zajedničku razinu kibernetičke sigurnosti u institucijama, tijelima, uredima i agencijama Unije

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 298.,

uzimajući u obzir Ugovor o osnivanju Europske zajednice za atomsku energiju, a posebno njegov članak 106.a,

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacrta zakonodavnog akta nacionalnim parlamentima,

u skladu s redovnim zakonodavnim postupkom ([1]),

budući da:

(1) U digitalnom dobu informacijska i komunikacijska tehnologija okosnica je otvorene, učinkovite i neovisne europske uprave. Zbog napretka tehnologije te povećane složenosti i međusobne povezanosti digitalnih sustava kibernetički sigurnosni rizici sve su veći čineći subjekte Unije osjetljivijima na kibernetičke prijetnje i kibernetičke incidente, što predstavlja prijetnju njihovu poslovnom kontinuitetu i sposobnosti da osiguraju svoje podatke. Iako su povećana upotreba usluga u oblaku, sveprisutna upotreba informacijske i komunikacijske tehnologije (IKT), visok stupanj digitalizacije, rad na daljinu te napredak tehnologije kao i povezanosti osnovne značajke svih aktivnosti subjekata Unije, digitalna otpornost još nije dovoljno integrirana u njihov rad.

(2) Kontekst kibernetičkih prijetnji s kojima se suočavaju subjekti Unije stalno se mijenja. Taktike, tehnike i postupci koje primjenjuju prijeteći akteri neprestano se razvijaju, dok se glavni motivi takvih napada, od krađe vrijednih neobjavljenih informacija do zarade, manipuliranja javnim mnijenjem ili ugrožavanja digitalne infrastrukture, ne mijenjaju mnogo. Tempo kojim prijeteći akteri provode svoje kibernetičke napade stalno se ubrzava, a njihove su kampanje sve sofisticiranije i automatiziranije, usmjerene na prostore izložene napadu kojih je sve više, te brzo iskorištavaju ranjivosti.

(3) IKT okruženja subjekata Unije međuovisna su i imaju integrirane protoke podataka, a njihovi korisnici blisko surađuju. Ta međupovezanost znači da svaki poremećaj, čak i onaj koji je prvotno ograničen na jednog subjekta Unije, može imati šire kaskadne učinke, što može dovesti do dalekosežnih i dugotrajnih negativnih učinaka na druge subjekte Unije. Osim toga, IKT okruženja pojedinih subjekata Unije povezana su s IKT okruženjima država članica, zbog čega incident u jednom subjektu Unije predstavlja kibernetički sigurnosni rizik za IKT okruženja država članica i obratno. Razmjena informacija specifičnih za određeni incident može olakšati otkrivanje sličnih kibernetičkih prijetnji ili incidenata koji pogađaju države članice.

(4) Subjekti Unije privlačne su mete koje se suočavaju s vrlo vještim i dobro opremljenim prijetećim akterima i drugim prijetnjama. Istodobno, razina i razvijenost kibernetičke otpornosti te sposobnost otkrivanja zlonamjernih kibernetičkih aktivnosti i odgovora na njih znatno se razlikuju od subjekta do subjekta. Stoga je za funkcioniranje subjekata Unije potrebno da oni postignu visoku zajedničku razinu kibernetičke sigurnosti provedbom mjera kibernetičke sigurnosti koje su razmjerne utvrđenim kibernetičkim sigurnosnim rizicima, razmjenom informacija i suradnjom.

([1]) Stajalište Europskog parlamenta od 21. studenoga 2023. (još nije objavljeno u Službenom listu) i odluka Vijeća od 8. prosinca 2023.

(5) Cilj je Direktive (EU) 2022/2555 Europskog parlamenta i Vijeća ([2]) daljnje poboljšanje kibernetičke otpornosti javnih i privatnih subjekata, nadležnih tijela i institucija te Unije u cjelini, kao i njihove sposobnosti odgovora na incidente. Stoga je potrebno osigurati da se subjekti Unije prilagode utvrđivanjem pravila koja su u skladu s Direktivom (EU) 2022/2555 i koja odražavaju njezinu razinu ambicije.

(6) Kako bi se postigla visoka zajednička razina kibernetičke sigurnosti, potrebno je da svaki subjekt Unije uspostavi unutarnji okvir za upravljanje kibernetičkim sigurnosnim rizicima, opće upravljanje njima i njihovu kontrolu („Okvir”), kojim se osigurava djelotvorno i razborito upravljanje svim kibernetičkim sigurnosnim rizicima te uzimaju u obzir kontinuitet poslovanja i upravljanje krizama. Okvirom bi trebalo uspostaviti politike kibernetičke sigurnosti, uključujući ciljeve i prioritete, za sigurnost mrežnih i informacijskih sustava koji obuhvaćaju cjelokupno neklasificirano IKT okruženje. Okvir bi se trebao temeljiti na pristupu kojim se uzimaju u obzir sve opasnosti čiji je cilj zaštita mrežnih i informacijskih sustava i fizičkog okruženja tih sustava od događaja poput krađe, požara, poplave, prekida u telekomunikacijama ili prekida opskrbe električnom energijom ili od neovlaštenog fizičkog pristupa te oštećenja i ometanja podataka i objekata za obradu podataka subjekta Unije, koji bi mogli ugroziti dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili podataka kojima se pristupa putem mrežnih i informacijskih sustava.

(7) Kako bi se upravljalo kibernetičkim sigurnosnim rizicima utvrđenima u Okviru, svaki subjekt Unije trebao bi poduzeti odgovarajuće i razmjerne tehničke, operativne i organizacijske mjere. Te bi se mjere trebale odnositi na područja i mjere upravljanja kibernetičkim sigurnosnim rizicima predviđene u ovoj Uredbi kako bi se ojačala kibernetička sigurnost svakog subjekta Unije.

(8) Plan za kibernetičku sigurnost, koji utvrđuje svaki subjekt Unije, trebao bi obuhvaćati imovinu i kibernetičke sigurnosne rizike utvrđene u Okviru te zaključke koji proizlaze iz redovitih procjena zrelosti kibernetičke sigurnosti. Plan za kibernetičku sigurnost trebao bi uključivati usvojene mjere upravljanja kibernetičkim sigurnosnim rizicima.

(9) Budući da je osiguravanje kibernetičke sigurnosti kontinuirani proces, prikladnost i djelotvornost mjera poduzetih na temelju ove Uredbe trebalo bi redovito revidirati s obzirom na promjene kibernetičkih sigurnosnih rizika, imovine i zrelosti kibernetičke sigurnosti subjekata Unije. Okvir bi trebalo preispitivati redovito, a najmanje svake četiri godine, dok bi plan za kibernetičku sigurnost trebalo revidirati svake dvije godine ili učestalije, prema potrebi, nakon procjena zrelosti kibernetičke sigurnosti ili svakog značajnog preispitivanja Okvira.

(10) Mjere upravljanja kibernetičkim sigurnosnim rizicima koje su uspostavili subjekti Unije trebale bi uključivati politike čiji je cilj, kad god je to moguće, učiniti izvorni kod transparentnim, uzimajući u obzir zaštitne mjere za prava trećih strana ili subjekata Unije. Te bi politike trebale biti razmjerne kibernetičkom sigurnosnom riziku i namijenjene su olakšavanju analize kibernetičkih prijetnji, a pritom ne stvaraju obveze otkrivanja koda treće strane ili prava na pristup kodu treće strane koja prelaze okvire primjenjivih ugovornih uvjeta.

(11) Alati i aplikacije za kibernetičku sigurnost otvorenog koda mogu doprinijeti većem stupnju otvorenosti. Otvoreni standardi olakšavaju interoperabilnost između sigurnosnih alata, pogodujući time sigurnosti dionika. Alati i aplikacije za kibernetičku sigurnost otvorenog koda mogu utjecati na širu zajednicu programera, omogućujući time diversifikaciju dobavljača. Otvoreni kod može dovesti do transparentnijeg procesa provjere alata koji se odnose na kibernetičku sigurnost i procesa otkrivanja ranjivosti koji pokreće zajednica. Subjekti Unije trebali bi, stoga, moći promicati upotrebu softvera otvorenog koda i otvorenih standarda provođenjem politika koje se odnose na korištenje otvorenih podataka i otvorenog koda kao dijela sigurnosti pomoću transparentnosti.

([2]) Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2) (SL L 333, 27.12.2022., str. 80.).

(12) Zbog razlika među subjektima Unije pri provedbi ove Uredbe potrebna je fleksibilnost. Mjere za visoku zajedničku razinu kibernetičke sigurnosti koje su predviđene u ovoj Uredbi ne bi trebale uključivati obveze koje izravno ometaju izvršavanje zadaća subjekata Unije ili zadiru u njihovu institucijsku autonomiju. Stoga bi ti subjekti trebali uspostaviti vlastite okvire i donijeti vlastite mjere upravljanja kibernetičkim sigurnosnim rizicima i planove za kibernetičku sigurnost. Pri provedbi takvih mjera trebalo bi na odgovarajući način uzeti u obzir postojeće sinergije među subjektima Unije, s ciljem pravilnog upravljanja resursima i optimizacije troškova. Trebalo bi na odgovarajući način uzeti u obzir i to da se mjerama ne utječe negativno na učinkovitu razmjenu informacija i suradnju među subjektima Unije te između subjekata Unije i partnera iz država članica.

(13) U interesu optimizacije upotrebe resursa ovom bi Uredbom trebalo predvidjeti mogućnost da dva ili više subjekata Unije sa sličnim strukturama surađuju u procjenjivanju zrelosti kibernetičke sigurnosti za svoje subjekte.

(14) Da bi se izbjeglo nerazmjerno financijsko i administrativno opterećenje za subjekte Unije, zahtjevi u pogledu upravljanja kibernetičkim sigurnosnim rizicima trebali bi biti razmjerni kibernetičkom sigurnosnom riziku kojem je izložen dotični mrežni i informacijski sustav, uzimajući u obzir najsuvremenije mjere upravljanja kibernetičkim sigurnosnim rizicima. Svaki subjekt Unije trebao bi nastojati dodijeliti odgovarajući postotak svojeg proračuna za IKT poboljšanju svoje razine kibernetičke sigurnosti. Dugoročno bi trebalo težiti okvirnom cilju od najmanje 10 %. Procjenom zrelosti kibernetičke sigurnosti trebalo bi utvrditi jesu li rashodi subjekta Unije za kibernetičku sigurnost razmjerni kibernetičkim sigurnosnim rizicima s kojima se taj subjekt suočava. Ne dovodeći u pitanje pravila koja se odnose na godišnji proračun Unije u skladu s Ugovorima, Komisija bi u svojem prijedlogu prvoga godišnjeg proračuna koji treba donijeti nakon stupanja na snagu ove Uredbe trebala uzeti u obzir obveze koje proizlaze iz ove Uredbe pri procjeni proračunskih potreba i potreba za osobljem subjekata Unije koje proizlaze iz njihovih procjena rashoda.

(15) Visoka zajednička razina kibernetičke sigurnosti zahtijeva da kibernetička sigurnost bude pod nadzorom najviše rukovodeće razine svakog subjekta Unije. Najviša rukovodeća razina subjekta Unije trebala bi biti odgovorna za provedbu ove Uredbe, među ostalim i za uspostavu Okvira, poduzimanje mjera upravljanja kibernetičkim sigurnosnim rizicima i odobravanje plana za kibernetičku sigurnost. Posvećivanje pozornosti kulturi kibernetičke sigurnosti, odnosno svakodnevna primjena kibernetičke sigurnosti, sastavni je dio Okvira te odgovarajućih mjera za upravljanje kibernetičkim sigurnosnim rizicima u svim subjektima Unije.

(16) Sigurnost mrežnih i informacijskih sustava u kojima se postupa s klasificiranim podatcima EU-a od ključne je važnosti. Subjekti Unije koji postupaju s klasificiranim podatcima EU-a dužni su primjenjivati sveobuhvatne regulatorne okvire za zaštitu takvih podataka, uključujući posebne postupke upravljanja, politike i postupke upravljanja rizicima. Potrebno je da mrežni i informacijski sustavi u kojima se postupa s klasificiranim podatcima EU-a ispunjavaju strože sigurnosne standarde od neklasificiranih mrežnih i informacijskih sustava. Stoga su mrežni i informacijski sustavi u kojima se postupa s klasificiranim podatcima EU-a otporniji na kibernertičke prijetnje i incidente. Slijedom toga, iako se prepoznaje potreba za zajedničkim okvirom u tom pogledu, ova se Uredba ne bi trebala primjenjivati na mrežne i informacijske sustave u kojima se postupa s klasificiranim podatcima EU-a. Međutim, ako to izričito zatraži subjekt Unije, tim za hitne računalne intervencije institucija, tijela i agencija EU-a (CERT-EU) trebao bi moći pružiti pomoć tom subjektu Unije u vezi s incidentima u klasificiranim IKT okruženjima.

(17) Subjekti Unije trebali bi procijeniti kibernetičke sigurnosne rizike povezane s odnosima s dobavljačima i pružateljima usluga, uključujući pružatelje usluga pohrane i obrade podataka ili upravljanih sigurnosnih usluga, te poduzeti odgovarajuće mjere za njihovo suzbijanje. Mjere kibernetičke sigurnosti trebalo bi pobliže utvrditi u smjernicama ili preporukama koje izdaje CERT-EU. Pri utvrđivanju mjera i smjernica trebalo bi uzeti u obzir najnovija dostignuća i, ako je to primjenjivo, relevantne europske i međunarodne norme, kao i relevantno pravo i politike Unije, uključujući procjene kibernetičkih sigurnosnih rizika i preporuke koje izdaje skupina za suradnju

osnovana na temelju članka 14. Direktive (EU) 2022/2555, kao što su koordinirana procjena rizika kibernetičke sigurnosti 5G mreža na razini EU-a i paket instrumenata EU-a za kibernetičku sigurnost 5G mreža. Osim toga, uzimajući u obzir kontekst kibernetičkih prijetnji i važnost jačanja kibernetičke otpornosti za subjekte Unije, može se zahtijevati certificiranje relevantnih IKT proizvoda, usluga i procesa u okviru posebnih europskih programa kibernetičke sigurnosne certifikacije donesenih na temelju članka 49. Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća ([3]).

(18) U svibnju 2011. glavni tajnici institucija i tijela Unije odlučili su osnovati pretkonfiguracijski tim za CERT-EU pod nadzorom međuinstitucijskog upravljačkog odbora. U srpnju 2012. glavni tajnici potvrdili su praktične aranžmane i dogovorili se da će zadržati CERT-EU u obliku trajnog subjekta radi daljnjeg doprinosa poboljšanju ukupne razine sigurnosti informacijskih tehnologija u institucijama, tijelima i agencijama Unije kao primjer vidljive međuinstitucijske suradnje u području kibernetičke sigurnosti. U rujnu 2012. osnovan je CERT-EU kao radna skupina Komisije s međuinstitucijskim ovlastima. U prosincu 2017. institucije i tijela Unije sklopili su Međuinstitucijski dogovor o organizaciji i radu CERT-EU-a ([4]). Ovom Uredbom trebalo bi predvidjeti sveobuhvatan skup pravila o organizaciji, funkcioniranju i radu CERT-EU-a. Odredbe ove Uredbe imaju prednost pred odredbama Međuinstitucijskog dogovora o organizaciji i radu CERT-EU-a, koji je sklopljen u prosincu 2017.

(19) CERT-EU trebalo bi preimenovati u Službu za kibernetičku sigurnost institucija, tijela, ureda i agencija Unije, ali bi zbog prepoznatljivosti trebalo zadržati skraćeni naziv CERT-EU.

(20) Uz davanje većeg broja zadaća CERT-EU-u i povećanje njegove uloge, ovom Uredbom osniva se Međuinstitucijski odbor za kibernetičku sigurnost (IICB) kako bi se olakšalo postizanje visoke zajedničke razine kibernetičke sigurnosti među subjektima Unije. IICB trebao bi imati kao isključivi zadatak praćenje provedbe ove Uredbe te pružanje podrške u provedbi ove Uredbe od strane subjekata Unije kao i nadzor provedbe općih prioriteta i ciljeva CERT-EU-a i pružanje strateškog usmjeravanja CERT-EU-u. IICB bi stoga trebao osigurati zastupljenost institucija Unije te bi trebao uključiti predstavnike tijela, ureda i agencija Unije putem Mreže agencija EU-a (EUAN). Organizaciju i funkcioniranje IICB-a trebalo bi dodatno urediti internim poslovnikom, koji može uključivati podrobnije određivanje redovitih sastanaka IICB-a, uključujući godišnja okupljanja na političkoj razini na kojima bi predstavnici najviše rukovodeće razine svakog člana IICB-a omogućili IICB-u da održi stratešku raspravu i da se pruže strateške smjernice IICB-u. Nadalje, IICB bi trebao imati mogućnost osnivanja izvršnog odbora koji bi mu pomogao u radu i kojem bi delegirao neke od svojih zadaća i ovlasti, osobito zadaće za koje je potrebno posebno stručno znanje njegovih članova, na primjer odobrenja kataloga usluga i svih njegovih naknadnih ažuriranja, dogovori o sporazumima o razini usluga, procjene dokumenata i izvješća koje subjekti Unije podnose IICB-u na temelju ove Uredbe ili zadaće povezane s pripremom odluka o mjerama usklađivanja koje izdaje IICB i s praćenjem njihove provedbe. IICB bi trebao utvrditi poslovnik izvršnog odbora, uključujući njegove zadaće i ovlasti.

(21) Cilj je IICB-a poduprijeti subjekte Unije u podizanju njihovih razina kibernetičke sigurnosti provedbom ove Uredbe. Kako bi pružio potporu subjektima Unije, IICB bi trebao voditelju CERT-EU-a pružati smjernice, donijeti višegodišnju strategiju za podizanje razine kibernetičke sigurnosti u subjektima Unije, utvrditi metodologiju i druge aspekte dobrovoljnih istorazinskih ocjenjivanja te poduprijeti uspostavu neformalne skupine lokalnih službenika za kibernetičku sigurnost, uz potporu Agencije Europske unije za kibersigurnost (ENISA), s ciljem razmjene najbolje prakse i informacija u vezi s provedbom ove Uredbe.

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

([4]) Dogovor između Europskog parlamenta, Europskog vijeća, Vijeća Europske unije, Europske komisije, Suda Europske unije, Europske središnje banke, Europskog revizorskog suda, Europske službe za vanjsko djelovanje, Europskog gospodarskog i socijalnog odbora, Europskog Odbora regija i Europske investicijske banke o organizaciji i radu tima za hitne računalne intervencije za institucije, tijela i agencije Unije (CERT-EU) (SL C 12, 13.1.2018., str. 1.).

(22) Kako bi se postigla visoka razina kibernetičke sigurnosti u svim subjektima Unije, interese tijela, ureda i agencija Unije koji upravljaju vlastitim IKT okruženjem trebala bi u IICB-u zastupati tri predstavnika koje imenuje EUAN. Sigurnost obrade osobnih podataka, a time i njezina kibernetička sigurnost, okosnica je zaštite podataka. S obzirom na sinergije između zaštite podataka i kibernetičke sigurnosti, Europski nadzornik za zaštitu podataka trebao bi biti zastupljen u IICB-u u svojstvu subjekta Unije koji podliježe ovoj Uredbi, s posebnim stručnim znanjem u području zaštite podataka, uključujući sigurnost elektroničkih komunikacijskih mreža. S obzirom na važnost inovacija i konkurentnosti u području kibernetičke sigurnosti, Europski stručni centar za industriju, tehnologiju i istraživanja u području kibernetičke sigurnosti trebao bi biti zastupljen u IICB-u. S obzirom na ulogu ENISA-e kao centra stručnosti u području kibernetičke sigurnosti i potporu koju ENISA pruža te s obzirom na važnost kibernetičke sigurnosti svemirske infrastrukture i usluga Unije, ENISA i Agencija Europske unije za svemirski program trebale bi biti zastupljene u IICB-u. S obzirom na ulogu dodijeljenu CERT-EU-u na temelju ove Uredbe, predsjednik IICB-a trebao bi pozvati voditelja CERT-EU-a na sve sastanke IICB-a, osim ako IICB raspravlja o pitanjima koja se izravno odnose na voditelja CERT-EU-a.

(23) IICB bi trebao pratiti usklađenost s ovom Uredbom kao i provedbu smjernica, preporuka i pozivâ na djelovanje. IICB bi u tehničkim pitanjima trebao imati potporu tehničkih savjetodavnih skupina čiji sastav IICB određuje prema vlastitu nahođenju. Te tehničke savjetodavne skupine trebale bi prema potrebi blisko surađivati s CERT-EU-om, subjektima Unije te drugim dionicima.

(24) Ako IICB utvrdi da subjekt Unije nije djelotvorno proveo ovu Uredbu ili smjernice, preporuke ili pozive na djelovanje izdane u skladu s ovom Uredbom, IICB bi trebao moći, ne dovodeći u pitanje interne postupke dotičnog subjekta Unije, poduzeti mjere usklađivanja. IICB bi trebao postupno primjenjivati mjere usklađivanja, drugim riječima, IICB bi najprije trebao donijeti najblažu mjeru, odnosno obrazloženo mišljenje te, samo ako je potrebno, donijeti sve strože mjere, što dovodi do najstrože mjere, odnosno preporuke o privremenoj suspenziji protokâ podataka prema dotičnom subjektu Unije. Takvu preporuku trebalo bi primjenjivati samo u iznimnim slučajevima u kojima dotični subjekt Unije čini dugoročna, namjerna, opetovana ili teška kršenja ove Uredbe.

(25) Obrazloženo mišljenje najblaža je mjera usklađivanja kojom se uklanjaju uočeni nedostatci u provedbi ove Uredbe. IICB bi nakon obrazloženog mišljenja trebao moći izdati smjernice kako bi pomogao subjektu Unije u osiguravanju usklađenosti njegova Okvira, njegovih mjera upravljanja kibernetičkim sigurnosnim rizicima, njegova plana za kibernetičku sigurnost i njegova izvješćivanja s ovom Uredbom, a zatim i upozorenje kako bi se u utvrđenom roku uklonili utvrđeni nedostatci subjekta Unije. Ako nedostatci utvrđeni u upozorenju nisu uklonjeni u dovoljnoj mjeri, IICB bi trebao moći izdati obrazloženu obavijest.

(26) IICB bi trebao moći preporučiti provedbu revizije subjekta Unije. Subjekt Unije trebao bi se moći koristiti svojom funkcijom unutarnje revizije u tu svrhu. IICB bi također trebao moći zatražiti da reviziju provede služba za reviziju treće strane, među ostalim pružatelj usluga iz privatnog sektora koji je zajednički dogovoren.

(27) U iznimnim slučajevima dugotrajnih, namjernih, opetovanih ili teških kršenja ove Uredbe od strane subjekta Unije, IICB bi trebao moći, kao krajnju mjeru, svim državama članicama i subjektima Unije preporučiti privremenu suspenziju protokâ podataka prema subjektu Unije, koja treba proizvoditi učinke sve dok subjekt Unije ne prestane s kršenjem. Takvu preporuku trebalo bi priopćiti odgovarajućim i sigurnim komunikacijskim kanalima.

(28) Kako bi se osigurala pravilna provedba ove Uredbe, IICB bi trebao, ako smatra da je ustrajno kršenje ove Uredbe od strane subjekta Unije izravno uzrokovano radnjama ili propustima člana njegova osoblja, među ostalim na najvišoj rukovodećoj razini, zatražiti od dotičnog subjekta Unije da poduzme odgovarajuću mjeru, među ostalim zatražiti od tog subjekta Unije da razmotri poduzimanje stegovne mjere, u skladu s pravilima i postupcima utvrđenima u Pravilniku o osoblju za dužnosnike Europske unije i Uvjetima zaposlenja ostalih službenika Unije, utvrđenima u Uredbi Vijeća (EEZ, Euratom, EZUČ) br. 259/68 ([5]) („Pravilnik o osoblju") i svim drugim primjenjivim pravilima i postupcima.

(29) CERT-EU trebao bi doprinositi sigurnosti IKT okruženja svih subjekata Unije. Pri razmatranju hoće li pružiti tehničke savjete ili tehnička mišljenja o relevantnim pitanjima politika slijedom zahtjeva subjekta Unije, CERT-EU trebao bi se pobrinuti da se time ne sprečava ispunjavanje drugih zadaća koje su mu povjerene na temelju ove Uredbe. CERT-EU bi u odnosu na subjekte Unije trebao djelovati kao ekvivalent koordinatora imenovanog za potrebe koordiniranog otkrivanja ranjivosti u skladu s člankom 12. stavkom 1. Direktive (EU) 2022/2555.

(30) CERT-EU trebao bi poduprijeti provedbu mjera za visoku zajedničku razinu kibernetičke sigurnosti prijedlozima za smjernice i preporuke IICB-u ili izdavanjem poziva na djelovanje. IICB bi trebao odobriti takve smjernice i preporuke. Prema potrebi, CERT-EU trebao bi izdavati pozive na djelovanje u kojima se opisuju hitne sigurnosne mjere u odnosu na koje se subjekte Unije potiče da ih poduzmu u zadanom roku. IICB bi trebao uputiti CERT-EU da izda, povuče ili izmijeni prijedlog smjernica ili preporuke ili poziv na djelovanje.

(31) CERT-EU trebao bi obavljati i ulogu koja mu je određena u Direktivi (EU) 2022/2555, a koja se odnosi na suradnju i razmjenu informacija s mrežom timova za odgovor na računalne sigurnosne incidente (CSIRT) uspostavljenom na temelju članka 15. te direktive. Nadalje, u skladu s Preporukom Komisije (EU) 2017/1584 ([6]) CERT-EU trebao bi surađivati i koordinirati odgovor s relevantnim dionicima. Kako bi doprinio visokoj razini kibernetičke sigurnosti u cijeloj Uniji, CERT-EU trebao bi s partnerima iz država članica dijeliti informacije specifične za određeni incident. CERT-EU trebao bi surađivati i s drugim javnim i privatnim partnerima, uključujući Organizaciju Sjevernoatlantskog ugovora (NATO), uz prethodno odobrenje IICB-a.

(32) Pri pružanju potpore operativnoj kibernetičkoj sigurnosti CERT-EU trebao bi se koristiti raspoloživim stručnim znanjem ENISA-e u okviru strukturirane suradnje, kako je predviđeno u Uredbi (EU) 2019/881. Prema potrebi trebalo bi uspostaviti posebne namjenske aranžmane između tih dvaju subjekata kako bi se utvrdila praktična provedba takve suradnje i izbjeglo udvostručivanje aktivnosti. CERT-EU trebao bi surađivati s ENISA-om na analizi kibernetičkih prijetnji i s ENISA-om redovito dijeliti svoje izvješće o stanju kibernetičkih prijetnji.

(33) CERT-EU trebao bi moći surađivati i razmjenjivati informacije s relevantnim zajednicama u području kibernetičke sigurnosti u Uniji i njezinim državama članicama kako bi se potaknula operativna suradnja i omogućilo postojećim mrežama da ostvare svoj puni potencijal za zaštitu Unije.

(34) Budući da su usluge i zadaće CERT-EU-a u interesu subjekata Unije, svaki subjekt Unije s rashodima za IKT trebao bi razmjerno doprinositi tim uslugama i zadaćama. Tim doprinosima ne dovodi se u pitanje proračunska autonomija subjekata Unije.

([5]) Uredba Vijeća (EEZ, Euratom, EZUČ) br. 259/68 od 29. veljače 1968. kojom se utvrđuje Pravilnik o osoblju za dužnosnike i Uvjeti zaposlenja ostalih službenika Europskih zajednica i kojom se uvode posebne mjere koje se privremeno primjenjuju na dužnosnike Komisije (SL L 56, 4.3.1968., str. 1).

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

(35) Mnogi kibernetički napadi dio su širih kampanja usmjerenih na skupine subjekata Unije ili na interesne zajednice koje uključuju subjekte Unije. Kako bi omogućili proaktivno otkrivanje incidenata, odgovor na incidente ili mjere ublažavanje, te oporavak od incidenata, subjekti Unije trebali bi moći obavijestiti CERT-EU o incidentima, kibernetičkim prijetnjama, ranjivostima i izbjegnutim incidentima te podijeliti odgovarajuće tehničke pojedinosti koje omogućuju otkrivanje ili ublažavanje sličnih incidenata, kibernetičkih prijetnji, ranjivosti i izbjegnutih incidenata u drugim subjektima Unije, kao i odgovor na njih. Na temelju istog pristupa kao u Direktivi (EU) 2022/2555 subjekti Unije trebali bi biti dužni dostaviti rano upozorenje CERT-EU-u u roku od 24 sata nakon što su saznali za značajni incident. Tom razmjenom informacija trebalo bi se omogućiti CERT-EU-u da te informacije proslijedi drugim subjektima Unije, kao i odgovarajućim partnerima, kako bi se pomoglo zaštititi IKT okruženja subjekata Unije i njihovih partnera od sličnih incidenata.

(36) Ovom se Uredbom utvrđuje pristup izvješćivanju o značajnim incidentima u više faza kako bi se uspostavila prava ravnoteža između, s jedne strane, brzog izvješćivanja koje doprinosi ublažavanju potencijalnog širenja značajnih incidenata i omogućuje subjektima Unije da traže pomoć te, s druge strane, detaljnog izvješćivanja kojim se iz pojedinačnih incidenata izvlače vrijedne pouke i s vremenom poboljšava kibernetička otpornost pojedinačnih subjekata Unije te doprinosi povećanju njihove opće razine kibernetičke sigurnosti. U tom bi pogledu ova Uredba trebala uključivati izvješćivanje o incidentima koji bi, na temelju početne procjene koju je proveo subjekt Unije, mogli uzrokovati ozbiljne poremećaje u funkcioniranju dotičnog subjekta Unije ili financijski gubitak dotičnom subjektu Unije ili, bi mogli utjecati na druge fizičke ili pravne osobe uzrokovanjem znatne materijalne ili nematerijalne štete. U takvoj početnoj procjeni trebalo bi uzeti u obzir, među ostalim, pogođene mrežne i informacijske sustave, posebno njihovu važnost za funkcioniranje subjekta Unije, ozbiljnost i tehničke značajke kibernetičke prijetnje i sve temeljne ranjivosti koje se iskorištavaju, kao i iskustvo subjekta Unije sa sličnim incidentima. Pokazatelji kao što su mjera u kojoj je ugroženo funkcioniranje subjekta Unije, trajanje incidenta ili broj pogođenih fizičkih ili pravnih osoba mogli bi imati važnu ulogu u utvrđivanju je li poremećaja u radu ozbiljan.

(37) Budući da su infrastruktura te mrežni i informacijski sustavi relevantnog subjekta Unije i države članice u kojoj se nalazi taj subjekt Unije međusobno povezani, ključno je da se tu državu članicu bez nepotrebne odgode obavijesti o značajnom incidentu unutar tog subjekta Unije. U tu bi svrhu pogođeni subjekt Unije trebao obavijestiti sve relevantne partnere iz država članica, koji su imenovani ili uspostavljeni u skladu s člancima 8. i 10. Direktive (EU) 2022/2555, o pojavi značajnog incidenta o kojem subjekt Unije izvješćuje CERT-EU. Ako CERT-EU sazna za značajni incident do kojeg je došlo u državi članici, trebao bi obavijestiti svakog relevantnog partnera iz te države članice.

(38) Trebalo bi uvesti mehanizam za osiguravanje djelotvorne razmjene informacija, koordinaciju i suradnju subjekata Unije u slučaju velikih incidenata, koji obuhvaća jasno utvrđivanje uloga i odgovornosti uključenih subjekata Unije. Predstavnik Komisije u IICB-u trebao bi, podložno planu za upravljanje kibernetičkim krizama, biti kontaktna točka za olakšavanje razmjene relevantnih informacija o većim incidentima koju IICB provodi s Europskom mrežom organizacija za vezu za kibernetičke krize (EU-CyCLONe) kao doprinos zajedničkoj informiranosti o stanju. Ulogom predstavnika Komisije u IICB-u kao kontaktne točke ne bi se trebala dovoditi u pitanje odvojena i posebna uloga Komisije u mreži EU-CyCLONe u skladu s člankom 16. stavkom 2. Direktive (EU) 2022/2555.

(39) Na svaku obradu osobnih podataka na temelju ove Uredbe primjenjuje se Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća ([7]). Obrada osobnih podataka mogla bi se odvijati u vezi s mjerama donesenima u kontekstu upravljanja kibernetičkim sigurnosnim rizicima, postupanja s ranjivostima i incidentima, razmjene informacija o incidentima, kibernetičkim prijetnjama i ranjivostima te koordinacije i suradnje u odgovoru na incidente. Takve bi mjere mogle zahtijevati obradu određenih kategorija osobnih podataka, kao što su IP adrese, jedinstveni lokatori

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

resursa (URL-ovi), nazivi domena, adrese e-pošte, organizacijske uloge ispitanika, vremenski žigovi, predmeti e-pošte ili nazivi datoteka. Sve mjere poduzete na temelju ove Uredbe trebale bi biti u skladu s okvirom za zaštitu podataka i privatnost, a subjekti Unije, CERT-EU i, ako je relevantno, IICB trebali bi poduzeti sve relevantne tehničke i organizacijske zaštitne mjere kako bi se na odgovoran način osigurala takva usklađenost.

(40) Ovom se Uredbom utvrđuje pravna osnova za obradu osobnih podataka koju provode subjekti Unije, CERT-EU i, ako je relevantno, IICB, za potrebe obavljanja svojih zadaća i ispunjavanja svojih obveza na temelju ove Uredbe, u skladu s člankom 5. stavkom 1. točkom (b) Uredbe (EU) 2018/1725. CERT-EU može djelovati kao izvršitelj obrade ili voditelj obrade ovisno o zadaći koju obavlja u skladu s Uredbom (EU) 2018/1725.

(41) U određenim slučajevima, u svrhu ispunjavanja svojih obveza na temelju ove Uredbe kako bi se osigurala visoka razina kibernetičke sigurnosti, a posebno u kontekstu postupanja s ranjivostima i incidentima, može biti potrebno da subjekti Unije i CERT-EU obrađuju posebne kategorije osobnih podataka kako je navedeno u članku 10. stavku 1. Uredbe (EU) 2018/1725. Ovom se Uredbom utvrđuje pravna osnova za obradu posebnih kategorija osobnih podataka koju provode subjekti Unije i CERT-EU u skladu s člankom 10. stavkom 2. točkom (g) Uredbe (EU) 2018/1725. Obrada posebnih kategorija osobnih podataka na temelju ove Uredbe trebala bi biti strogo razmjerna cilju koji se želi postići. Podložno uvjetima iz članka 10. stavka 2. točke (g) te uredbe, subjekti Unije i CERT-EU trebali bi moći obrađivati takve podatke samo u mjeri u kojoj je to potrebno i ako je to izričito predviđeno u ovoj Uredbi. Subjekti Unije i CERT-EU trebali bi prilikom obrade posebnih kategorija osobnih podataka poštovati bit prava na zaštitu podataka i predvidjeti odgovarajuće i posebne mjere za zaštitu temeljnih prava i interesa ispitanika.

(42) U skladu s člankom 33. Uredbe (EU) 2018/1725 subjekti Unije i CERT-EU trebali bi, uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode fizičkih osoba, provesti odgovarajuće tehničke i organizacijske mjere kako bi se osigurala odgovarajuća razina sigurnosti osobnih podataka, kao što su pružanje prava ograničenog pristupa na temelju nužnosti pristupa, primjena načela postojanja revizijskog traga, utvrđivanje nadzornog lanca, pohrana podataka u mirovanju u kontroliranom i provjerljivom okruženju, standardizirani operativni postupci i mjere za očuvanje privatnosti, kao što su pseudonimizacija ili kriptiranje. Te bi se mjere trebale provoditi tako da ne utječu na svrhu postupanja s incidentom ni na cjelovitost dokaza. Ako subjekt Unije ili CERT-EU prenosi osobne podatke povezane s incidentom, uključujući posebne kategorije osobnih podataka, partneru ili suradniku za potrebe ove Uredbe, takvi prijenosi trebali bi biti u skladu s Uredbom (EU) 2018/1725. Ako se posebne kategorije osobnih podataka prenose trećoj strani, subjekti Unije i CERT-EU trebali bi osigurati da treća strana primjenjuje mjere koje se odnose na zaštitu osobnih podataka na razini istovjetnoj Uredbi (EU) 2018/1725.

(43) Osobne podatke koji se obrađuju za potrebe ove Uredbe trebalo bi čuvati samo onoliko dugo koliko je potrebno u skladu s Uredbom (EU) 2018/1725. Subjekti Unije i, ako je to primjenjivo, CERT-EU koji djeluje kao voditelj obrade, trebali bi utvrditi razdoblja pohrane koja su ograničena na ono što je potrebno za postizanje utvrđenih svrha. Kad je riječ osobito o osobnim podatcima prikupljenima za postupanje s incidentom, subjekti Unije i CERT-EU trebali bi razlikovati osobne podatke koji se prikupljaju za otkrivanje kibernetičke prijetnje u svojim IKT okruženjima kako bi se spriječio incident i osobne podatke koji se prikupljaju radi ublažavanja incidenta, odgovora na njega i oporavka od njega. Za otkrivanje kibernetičke prijetnje važno je uzeti u obzir koliko dugo prijeteći akter može ostati neotkriven u sustavu. Radi ublažavanja incidenta, odgovora na njega i oporavka od njega važno je razmotriti jesu li osobni podatci potrebni za otkrivanje incidenta i postupanje s incidentom koji se ponavlja ili incidenta slične prirode za koji bi se mogla dokazati korelacija.

(44) Postupanje subjekata Unije i CERT-EU-a s podatcima trebalo bi biti u skladu s primjenjivim pravilima o sigurnosti podataka. Uključivanje sigurnosti ljudskih resursa kao mjere upravljanja kibernetičkim sigurnosnim rizicima trebalo bi također biti u skladu s primjenjivim pravilima.

(45) Za potrebe razmjene informacija upotrebljavaju se vidljive oznake kako bi se naznačilo da primatelji informacija moraju primjenjivati ograničenja u njihovoj razmjeni, osobito ona na temelju sporazumâ o povjerljivosti podataka ili neformalnih dogovora o povjerljivosti podataka, kao što je Protokol o semaforu (eng. the traffic light protocol) ili druge jasne oznake koje je naveo izvor. Protokol o semaforu treba shvatiti kao sredstvo za pružanje informacija o svim ograničenjima u pogledu daljnjeg širenja informacija. Upotrebljava se u gotovo svim CSIRT-ovima i u pojedinim centrima za analizu i razmjenu informacija.

(46) Ovu bi Uredbu trebalo redovito evaluirati s obzirom na buduće pregovore o višegodišnjim financijskim okvirima, kojima će se omogućiti donošenje daljnjih odluka u pogledu funkcioniranja i institucionalne uloge CERT-EU-a, uključujući moguću uspostavu CERT-EU-a kao ureda Unije.

(47) IICB bi trebao, uz pomoć CERT-EU-a, preispitati i evaluirati provedbu ove Uredbe te podnijeti izvješće Komisiji o svojim zaključcima. Na temelju tih informacija Komisija bi trebala izvijestiti Europski parlament, Vijeće, Europski gospodarski i socijalni odbor i Odbor regija. U tom bi izvješću, uz doprinos IICB-a, trebalo evaluirati primjerenost uključivanja mrežnih i informacijskih sustava u kojima se postupa s klasificiranim podatcima EU-a u područje primjene ove Uredbe, osobito ako ne postoje pravila o informacijskoj sigurnosti koja su zajednička subjektima Unije.

(48) U skladu s načelom proporcionalnosti, radi ostvarenja temeljnog cilja postizanja visoke zajedničke razine kibernetičkoj sigurnosti u subjektima Unije potrebno je i primjereno utvrditi pravila o kibernetičkoj sigurnosti za subjekte Unije. Ova Uredba ne prelazi ono što je potrebno za ostvarivanje cilja u skladu s člankom 5. stavkom 4. Ugovora o Europskoj uniji.

(49) Ovom Uredbom odražava se činjenica da se subjekti Unije razlikuju po veličini i kapacitetima, među ostalim u pogledu financijskih i ljudskih resursa.

(50) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 te je on dao mišljenje 17. svibnja 2022. ([8]),

DONIJELI SU OVU UREDBU:

POGLAVLJE I.

OPĆE ODREDBE

Članak 1.

Predmet

Ovom se Uredbom utvrđuju mjere kojima se nastoji postići visoka zajednička razina kibernetičke sigurnosti unutar subjekata Unije koje se odnose na:

(a) uspostavu unutarnjeg okvira za upravljanje kibernetičkim sigurnosnim rizicima, opće upravljanje njima i njihovu kontrolu od strane svakog subjekta Unije u skladu s člankom 6.;

(b) upravljanje kibernetičkim sigurnosnim rizicima, izvješćivanje o njima i razmjenu informacija o njima;

(c) organizaciju, funkcioniranje i rad Međuinstitucijskog odbora za kibernetičku sigurnost osnovanog člankom 10. te organizaciju, funkcioniranje i rad Službe za kibernetičku sigurnost institucija, tijela, ureda i agencija Unije (CERT-EU);

(d) praćenje provedbe ove Uredbe.

([8]) SL C 258, 5.7.2022., str. 10.

Članak 2.

Područje primjene

1. Ova se Uredba primjenjuje na subjekte Unije, Međuinstitucijski odbor za kibernetičku sigurnost osnovan člankom 10. i na CERT-EU.

2. Ova se Uredba primjenjuje ne dovodeći u pitanje institucijsku autonomiju na temelju Ugovorâ.

3. Izuzev članka 13. stavka 8., ova se Uredba ne primjenjuje na mrežne i informacijske sustave u kojima se postupa s klasificiranim podatcima EU-a.

Članak 3.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

1. „subjekti Unije” znači institucije, tijela, uredi i agencije Unije koji su osnovani Ugovorom o Europskoj uniji, Ugovorom o funkcioniranju Europske unije (TFEU) ili Ugovorom o osnivanju Europske zajednice za atomsku energiju ili na temelju tih ugovora;

2. „mrežni i informacijski sustav” znači mrežni i informacijski sustav kako je definiran u članku 6. točki 1. Direktive (EU) 2022/2555;

3. „sigurnost mrežnih i informacijskih sustava” znači sigurnost mrežnih i informacijskih sustava kako je definirana u članku 6. točki 2. Direktive (EU) 2022/2555;

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

5. „najviša rukovodeća razina” znači rukovoditelj, rukovodeće tijelo ili koordinacijsko i nadzorno tijelo koji su odgovorni za funkcioniranje subjekta Unije, na najvišoj upravnoj razini, s mandatom za donošenje ili odobravanje odluka u skladu s upravljačkim aranžmanima na visokoj razini tog subjekta Unije, ne dovodeći u pitanje formalne odgovornosti drugih rukovodećih razina u pogledu usklađenosti i upravljanja kibernetičkim sigurnosnim rizikom u njihovim područjima odgovornosti;

6. „izbjegnuti incident” znači izbjegnuti incident kako je definiran u članku 6. točki 5. Direktive (EU) 2022/2555;

7. „incident” znači incident kako je definiran u članku 6. točki 6. Direktive (EU) 2022/2555;

8. „veliki incident” znači svaki incident koji uzrokuje razinu poremećaja koja premašuje sposobnost subjekta Unije i CERT-EU-a da na njega odgovore ili koji ima znatan učinak na najmanje dva subjekta Unije;

9. „kibernetički sigurnosni incident velikih razmjera” znači kibernetički sigurnosni incident velikih razmjera kako je definiran u članku 6. točki 7. Direktive (EU) 2022/2555;

10. „postupanje s incidentom” znači postupanje s incidentom kako je definirano u članku 6. točki 8. Direktive (EU) 2022/2555;

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

12. „ozbiljna kibernetička prijetnja” znači ozbiljna kibernetička prijetnja kako je definirana u članku 6. točki 11. Direktive (EU) 2022/2555;

13. „ranjivost” znači ranjivost kako je definirana u članku 6. točki 15. Direktive (EU) 2022/2555;

14. „kibernetički sigurnosni rizik” znači rizik kako je definiran u članku 6. točki 9. Direktive (EU) 2022/2555;

15. „usluga računalstva u oblaku” znači usluga računalstva u oblaku kako je definirana u članku 6. točki 30. Direktive (EU) 2022/2555.

Članak 4.

Obrada osobnih podataka

1. Obrada osobnih podataka koju na temelju ove Uredbe provode CERT-EU, Međuinstitucijski odbor za kibernetičku sigurnost osnovan člankom 10. i subjekti Unije provodi se u skladu s Uredbom (EU) 2018/1725.

2. Ako obavljaju zadaće ili ispunjavaju obveze na temelju ove Uredbe, CERT-EU, Međuinstitucijski odbor za kibernetičku sigurnost osnovan člankom 10. i subjekti Unije obrađuju i razmjenjuju osobne podatke samo u mjeri u kojoj je to potrebno i isključivo u svrhu obavljanja tih zadaća ili ispunjavanja tih obveza.

3. Obrada posebnih kategorija osobnih podataka iz članka 10. stavka 1. Uredbe (EU) 2018/1725 smatra se potrebnom ako postoji značajan javni interes u skladu s člankom 10. stavkom 2. točkom (g) te uredbe. Takvi se podatci mogu obrađivati samo u mjeri u kojoj je to potrebno za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima iz članaka 6. i 8., za pružanje usluga CERT-EU-a u skladu s člankom 13., za razmjenu informacija specifičnih za određeni incident u skladu s člankom 17. stavkom 3. i člankom 18. stavkom 3., za razmjenu informacija u skladu s člankom 20., za obveze izvješćivanja u skladu s člankom 21., za koordinaciju odgovora na incidente i za suradnju u skladu s člankom 22. te za upravljanje velikim incidentima u skladu s člankom 23. ove Uredbe. Kada djeluju kao voditelji obrade podataka, subjekti Unije i CERT-EU primjenjuju tehničke mjere za sprečavanje obrade posebnih kategorija osobnih podataka u druge svrhe te osiguravaju odgovarajuće i posebne mjere za zaštitu temeljnih prava i interesa ispitanika.

POGLAVLJE II.

MJERE ZA VISOKU ZAJEDNIČKU RAZINU KIBERNETIČKE SIGURNOSTI

Članak 5.

Provedba mjera

1. Do 8. rujna 2024. Međuinstitucijski odbor za kibernetičku sigurnost osnovan člankom 10., nakon savjetovanja s Agencijom Europske unije za kibersigurnost (ENISA) i nakon što primi smjernice od CERT-EU-a, izdaje smjernice subjektima Unije za potrebe provedbe početnog preispitivanja stanja kibernetičke sigurnosti i uspostave unutarnjeg okvira za upravljanje kibernetičkim sigurnosnim rizicima, opće upravljanje njima i njihovu kontrolu u skladu s člankom 6., provedbu procjena zrelosti kibernetičke sigurnosti u skladu s člankom 7., poduzimanje mjera upravljanja kibernetičkim sigurnosnim rizicima u skladu s člankom 8. i donošenja plana za kibernetičku sigurnost u skladu s člankom 9.

2. Pri provedbi članaka od 6. do 9. subjekti Unije uzimaju u obzir smjernice iz stavka 1. ovog članka, kao i relevantne smjernice i preporuke donesene na temelju članaka 11. i 14.

Članak 6.

Okvir za upravljanje kibernetičkim sigurnosnim rizicima, opće upravljanje njima i njihovu kontrolu

1. Do 8. travnja 2025. svaki subjekt Unije nakon provedbe početnog preispitivanja stanja kibernetičke sigurnosti, kao što je revizija, uspostavlja unutarnji okvir za upravljanje kibernetičkim sigurnosnim rizicima, opće upravljanje njima i njihovu kontrolu („Okvir”). Uspostavu Okvira nadzire i za nju je odgovorna najviša rukovodeća razina subjekta Unije.

2. Okvirom se obuhvaća cjelokupno neklasificirano IKT okruženje dotičnog subjekta Unije, uključujući lokalno IKT okruženje, lokalnu operativnu tehnološku mrežu, eksternalizirana sredstva i usluge računalstva u oblaku ili one kojima treće strane pružaju usluge smještaja na poslužitelju, mobilne uređaje, korporacijske mreže, poslovne mreže koje nisu povezane s internetom i sve uređaje povezane s tim okruženjima („IKT okruženje”). Okvir se temelji na pristupu kojim se obuhvaćaju sve opasnosti.

3. Okvirom se osigurava visoka razina kibernetičke sigurnosti. Okvirom se utvrđuju interne politike kibernetičke sigurnosti, među ostalim ciljevi i prioriteti, za sigurnost mrežnih i informacijskih sustava te uloge i odgovornosti osoblja subjekta Unije čija je zadaća osigurati djelotvornu provedbu ove Uredbe. Okvir također uključuje mehanizme za mjerenje djelotvornosti provedbe.

4. Okvir se, s obzirom na promjenjive kibernetičke sigurnosne rizike, preispituje redovito, a najmanje svake četiri godine. Prema potrebi i na zahtjev Međuinstitucijskog odbora za kibernetičku sigurnost osnovanog člankom 10., Okvir subjekta Unije može se ažurirati na temelju smjernice CERT-EU-a o utvrđenim incidentima ili mogućim nedostatcima uočenima u provedbi ove Uredbe.

5. Najviša rukovodeća razina svakog subjekta Unije odgovorna je za provedbu ove Uredbe i nadgleda usklađenost njegove organizacije s obvezama povezanima s Okvirom.

6. Prema potrebi i ne dovodeći u pitanje svoju odgovornost za provedbu ove Uredbe, najviša rukovodeća razina svakog subjekta Unije može delegirati posebne obveze na temelju ove Uredbe višim dužnosnicima u smislu članka 29. stavka 2. Pravilnika o osoblju ili drugim dužnosnicima na jednakoj razini unutar dotičnog subjekta Unije. Neovisno o takvom delegiranju, najviša rukovodeća razina može se smatrati odgovornom za kršenje ove Uredbe koje je počinio dotični subjekt Unije.

7. Svaki subjekt Unije dužan je imati uspostavljene učinkovite mehanizme kojima se osigurava da se odgovarajući postotak proračuna za IKT troši na kibernetičku sigurnost. Pri utvrđivanju tog postotka uzima se u obzir Okvir.

8. Svaki subjekt Unije imenuje lokalnog službenika za kibernetičku sigurnost ili osobu na jednakovrijednoj funkciji koji odnosno koja djeluje kao njegova jedinstvena kontaktna točka za sve aspekte kibernetičke sigurnosti. Lokalni službenik za kibernetičku sigurnost olakšava provedbu ove Uredbe i najvišu rukovodeću razinu redovito izravno izvješćuje o stanju provedbe. Ne dovodeći u pitanje činjenicu da je lokalni službenik za kibernetičku sigurnost jedinstvena kontaktna točka u svakom subjektu Unije, subjekt Unije može delegirati CERT-EU-u određene zadaće lokalnog službenika za kibernetičku sigurnost povezane s provedbom ove Uredbe na temelju sporazuma o razini usluga sklopljenog između tog subjekta Unije i CERT-EU-a ili te zadaće može dijeliti nekoliko subjekata Unije. Ako su te zadaće delegirane CERT-EU-u, Međuinstitucijski odbor za kibernetičku sigurnost osnovan člankom 10. odlučuje hoće li pružanje te usluge biti dio osnovnih usluga CERT-EU-a, uzimajući u obzir ljudske i financijske resurse dotičnog subjekta Unije. Svaki subjekt Unije bez nepotrebne odgode obavješćuje CERT-EU o imenovanom lokalnom službeniku za kibernetičku sigurnost i eventualnim naknadnim promjenama u vezi s time.

CERT-EU uspostavlja i ažurira popis imenovanih lokalnih službenika za kibernetičku sigurnost.

9. Viši dužnosnici u smislu članka 29. stavka 2. Pravilnika o osoblju ili drugi dužnosnici na jednakoj razini svakog subjekta Unije te svi relevantni članovi osoblja zaduženi za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima i ispunjavanje obveza utvrđenih u ovoj Uredbi redovito pohađaju posebna osposobljavanja kako bi stekli dovoljno znanja i vještina za razumijevanje i procjenu kibernetičkih sigurnosnih rizika i prakse upravljanja kibernetičkom sigurnošću te njihova utjecaja na poslovanje subjekta Unije.

Članak 7.

Procjene zrelosti kibernetičke sigurnosti

1. Do 8. srpnja 2025. i najmanje svake dvije godine nakon tog datuma svaki subjekt Unije provodi procjenu zrelosti kibernetičke sigurnosti koja uključuje sve elemente njegova IKT okruženja.

2. Procjene zrelosti kibernetičke sigurnosti provode se, prema potrebi, uz pomoć specijalizirane treće strane.

3. Subjekti Unije sa sličnim strukturama mogu surađivati u provedbi procjena zrelosti kibernetičke sigurnosti za svoje subjekte.

4. Na temelju zahtjeva Međuinstitucijskog odbora za kibernetičku sigurnost osnovanog člankom 10. i uz izričitu suglasnost dotičnog subjekta Unije, o rezultatima procjene zrelosti kibernetičke sigurnosti može se raspravljati u okviru tog Odbora ili u okviru neformalne skupine lokalnih službenika za kibernetičku sigurnost kako bi se izvukle pouke iz iskustava i razmijenila najbolja praksa.

Članak 8.

Mjere upravljanja kibernetičkim sigurnosnim rizicima

1. Svaki subjekt Unije bez nepotrebne odgode i u svakom slučaju do 8. rujna 2025., pod nadzorom najviše rukovodeće razine, poduzima odgovarajuće i razmjerne tehničke, operativne i organizacijske mjere za upravljanje kibernetičkim sigurnosnim rizicima utvrđenima u Okviru i za sprečavanje učinaka incidenata ili za svođenje učinaka incidenata na najmanju moguću mjeru. Uzimajući u obzir najnovija dostignuća i, ako je to primjenjivo, relevantne europske i međunarodne norme, tim se mjerama osigurava razina sigurnosti mrežnih i informacijskih sustava u cjelokupnom IKT okruženju koja je razmjerna nastalim kibernetičkim sigurnosnim rizicima. Pri procjeni razmjernosti tih mjera na odgovarajući se način uzima u obzir stupanj izloženosti subjekta Unije kibernetičkim sigurnosnim rizicima, njegova veličina, vjerojatnost pojave incidenata i njihova ozbiljnost, uključujući njihov društveni, gospodarski i međuinstitucijski učinak.

2. Subjekti Unije prilikom provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima razmatraju barem sljedeća pitanja:

(a) politiku kibernetičke sigurnosti, uključujući mjere potrebne za postizanje ciljeva i prioriteta iz članka 6. i stavka 3. ovog članka;

(b) politike analize kibernetičkih sigurnosnih rizika i sigurnosti informacijskih sustava;

(c) ciljeve politike u pogledu korištenja usluga računalstva u oblaku;

(d) prema potrebi, reviziju kibernetičke sigurnosti koja može uključivati procjenu kibernetičkih sigurnosnih rizika, ranjivosti i kibernetičkih prijetnji te penetracijska testiranja, koja redovito provodi pouzdani privatni pružatelj usluga;

(e) provedbu preporuka koje proizlaze iz revizija kibernetičke sigurnosti iz točke (d) putem ažuriranja stanja kibernetičke sigurnosti i politika;

(f) organizaciju kibernetičke sigurnosti, uključujući utvrđivanje uloga i odgovornosti;

(g) upravljanje imovinom, uključujući popis IKT imovine i kartografiju IKT mreže;

(h) sigurnost ljudskih resursa i kontrolu pristupa;

(i) sigurnost operacija;

(j) sigurnost komunikacija;

(k) nabavu, razvoj i održavanj sustavâ, uključujući politike za postupanje s ranjivostima i njihovo otkrivanje;

(l) ako je moguće, politike o transparentnosti izvornog koda;

(m) sigurnost lanca opskrbe, uključujući sigurnosne aspekte povezane s odnosima između svakog subjekta Unije i njegovih izravnih dobavljača ili pružatelja usluga;

(n) postupanje s incidentima i suradnji s CERT-EU-om, na primjer održavanju sustava sigurnosnog nadzora i bilježenju dnevničkih zapisa;

(o) upravljanje kontinuitetom poslovanja, na primjer upravljanju sigurnosnim kopijama i oporavku od katastrofe te upravljanju krizama; i

(p) promicanje i razvoj programâ obrazovanja, vještina, podizanja svijesti, vježbi i osposobljavanja u području kibernetičke sigurnosti.

Za potrebe prvog podstavka točke (m) subjekti Unije uzimaju u obzir ranjivosti specifične za svakog izravnog dobavljača i pružatelja usluga te ukupnu kvalitetu proizvoda i kibernetičke sigurnosne prakse svojih dobavljača i pružatelja usluga, uključujući njihove sigurne razvojne postupke.

3. Subjekti Unije poduzimaju barem sljedeće posebne mjere upravljanja kibernetičkim sigurnosnim rizicima:

(a) tehničke aranžmane za omogućavanje i održavanje rada na daljinu;

(b) konkretne korake za prijelaz na načela nultog povjerenja;

(c) upotrebu višefaktorske autentifikacije kao norme u svim mrežnim i informacijskim sustavima;

(d) upotrebu kriptografije i kriptiranja, a posebno prolaznog kriptiranja, te sigurnih digitalnih potpisa;

(e) prema potrebi, sigurne glasovne, video- i tekstualne komunikacije te sigurni komunikacijski sustav u hitnim slučajevima unutar subjekta Unije;

(f) proaktivne mjere za otkrivanje i uklanjanje zlonamjernog softvera i špijunskog softvera;

(g) uspostavljanje sigurnosti lanca opskrbe softverom s pomoću kriterija za siguran razvoj i evaluaciju softvera;

(h) izrada i donošenje programa za osposobljavanje u području kibernetičke sigurnosti koji odgovara predviđenim zadaćama i očekivanim sposobnostima najviše rukovodeće razine i osoblja subjekta Unije čija je zadaća osiguravanje djelotvorne provedbe ove Uredbe;

(i) redovito osposobljavanje osoblja u području kibernetičke sigurnosti;

(j) ako je to relevantno, sudjelovanje u analizama rizika s obzirom na međupovezanosti subjekata Unije;

(k) poboljšanje pravila javne nabave kako bi se olakšalo postizanje visoke zajedničke razine kibernetičke sigurnosti:

i. uklanjanjem ugovornih prepreka koje pružateljima IKT usluga otežavaju razmjenu informacija o incidentima, ranjivostima i kibernetičkim prijetnjama s CERT-EU-om;

ii. ugovornim obvezama prijavljivanja incidenata, ranjivosti i kibernetičkih prijetnji te uspostavljanjem primjerenih mehanizama odgovora na incidente i praćenja incidenata.

Članak 9.

Planovi za kibernetičku sigurnost

1. Na temelju zaključaka iz procjene zrelosti kibernetičke sigurnosti provedene u skladu s člankom 7. i uzimajući u obzir sredstva i kibernetičke sigurnosne rizike utvrđene u Okviru te mjere upravljanja kibernetičkim sigurnosnim rizicima poduzete u skladu s člankom 8., najviša rukovodeća razina svakog subjekta Unije odobrava plan za kibernetičku sigurnost bez nepotrebne odgode, a u svakom slučaju do 8. siječnja 2026. Planom za kibernetičku sigurnost nastoji se povećati ukupna kibernetička sigurnost subjekta Unije i time doprinijeti poboljšanju visoke zajedničke razine kibernetičke sigurnosti u subjektima Unije. Plan za kibernetičku sigurnost obuhvaća barem mjere za upravljanje kibernetičkim sigurnosnim rizicima poduzete na temelju članka 8. Plan za kibernetičku sigurnost revidira se svake dvije godine ili učestalije, prema potrebi, nakon procjena zrelosti kibernetičke sigurnosti provedenih u skladu s člankom 7. ili nakon svakog značajnog preispitivanja Okvira.

2. Plan za kibernetičku sigurnost obuhvaća plan subjekta Unije za upravljanje kibernetičkim krizama za velike incidente.

3. Subjekt Unije podnosi svoj dovršeni plan za kibernetičku sigurnost Međuinstitucijskom odboru za kibernetičku sigurnost osnovanom člankom 10.

POGLAVLJE III.

MEĐUINSTITUCIJSKI ODBOR ZA KIBERNETIČKU SIGURNOST

Članak 10.

Međuinstitucijski odbor za kibernetičku sigurnost

1. Osniva se Međuinstitucijski odbor za kibernetičku sigurnost (IICB).

2. IICB je odgovoran za:

(a) praćenje provedbe ove Uredbe od strane subjekata Unije i pružanje potpore u provedbi;

(b) nadzor nad provedbom općih prioriteta i ciljeva CERT-EU-a i strateško usmjeravanje CERT-EU-a.

3. IICB se sastoji od:

(a) po jednog predstavnika kojeg imenuje svako od sljedećih tijela:

i. Europski parlament,

ii. Europsko vijeće,

iii. Vijeće Europske unije,

iv. Komisija,

v. Sud Europske unije,

vi. Europska središnja banka,

vii. Revizorski sud,

viii. Europska služba za vanjsko djelovanje,

ix. Europski gospodarski i socijalni odbor,

x. Europski odbor regija,

xi. Europska investicijska banka,

xii. Europski stručni centar za industriju, tehnologiju i istraživanja u području kibernetičke sigurnosti,

xiii. ENISA,

xiv. Europski nadzornik za zaštitu podataka,

xv. Agencija Europske unije za svemirski program.

(b) tri predstavnika koje Mreža agencija EU-a (EUAN) imenuje na temelju prijedloga svojeg savjetodavnog odbora za IKT kako bi zastupali interese tijela, ureda i agencija Unije koji upravljaju vlastitim IKT okruženjem, osim onih iz točke (a).

Subjekti Unije zastupljeni u IICB-u nastoje postići rodnu ravnotežu među imenovanim predstavnicima.

4. Članovima IICB-a može pomagati zamjenik. Predsjednik može pozvati druge predstavnike subjekata Unije navedenih u stavku 3. ili drugih subjekata Unije da prisustvuju sastancima IICB-a bez prava glasa.

5. Voditelj CERT-EU-a i predsjednici Skupine za suradnju, mreže CSIRT-ova i EU-CyCLONe-a osnovanih člancima 14., 15. odnosno 16. Direktive (EU) 2022/2555 ili njihovi zamjenici mogu sudjelovati na sastancima IICB-a kao promatrači. U iznimnim slučajevima IICB može odlučiti drukčije, u skladu sa svojim internim poslovnikom.

6. IICB donosi svoj interni poslovnik.

7. U skladu sa svojim internim poslovnikom IICB iz redova svojih članova imenuje predsjednika na razdoblje od tri godine. Zamjenik predsjednika postaje punopravni član IICB-a na isto razdoblje.

8. IICB se sastaje najmanje triput godišnje na inicijativu svojeg predsjednika, na zahtjev CERT-EU-a ili na zahtjev bilo kojeg od svojih članova.

9. Svaki član IICB-a ima jedan glas. Odluke IICB-a donose se običnom većinom, osim ako je u ovoj Uredbi predviđeno drugačije. Predsjednik IICB-a ne smije glasovati, osim u slučaju izjednačenog broja glasova kad predsjednik može dati odlučujući glas.

10. IICB može donositi odluke u pojednostavnjenom pisanom postupku pokrenutom u skladu sa svojim internim poslovnikom. U okviru tog postupka relevantna odluka smatra se odobrenom u roku koji odredi predsjednik, osim ako se neki član protivi.

11. Poslove tajništva za IICB obavlja Komisija i ona odgovara predsjedniku IICB-a.

12. Predstavnici koje imenuje EUAN prosljeđuju odluke IICB-a članovima EUAN-a. Svaki član EUAN-a ima pravo tim predstavnicima ili predsjedniku IICB-a postaviti sva pitanja za koja smatra da bi na njih trebalo upozoriti IICB.

13. IICB može osnovati izvršni odbor da mu pomaže u radu i delegirati mu neke od svojih zadaća i ovlasti. IICB utvrđuje poslovnik izvršnog odbora, uključujući zadaće i ovlasti izvršnog odbora te mandat njegovih članova.

14. Do 8. siječnja 2025., a nakon tog datuma jednom godišnje, IICB podnosi izvješće Europskom parlamentu i Vijeću u kojem detaljno opisuje napredak u provedbi ove Uredbe i posebno navodi opseg suradnje CERT-EU-a s partnerima iz država članica u svakoj od država članica. Izvješće je doprinos dvogodišnjem izvješću o stanju kibernetičke sigurnosti u Uniji donesenom na temelju članka 18. Direktive (EU) 2022/2555.

Članak 11.

Zadaće IICB-a

Pri obavljanju svojih dužnosti IICB posebno:

(a) pruža smjernice voditelju CERT-EU-a;

(b) djelotvorno prati i nadzire provedbu ove Uredbe te podupire subjekte Unije u jačanju njihove kibernetičke sigurnosti, uključujući, prema potrebi, traženjem izrade ad hoc izvješća od subjekata Unije i CERT-EU-a;

(c) nakon strateške rasprave donosi višegodišnju strategiju za podizanje razine kibernetičke sigurnosti u subjektima Unije, redovito ocjenjuje tu strategiju, a u svakom slučaju svakih pet godina, te je prema potrebi mijenja;

(d) utvrđuje metodologiju i organizacijske aspekte za dobrovoljna istorazinska ocjenjivanja koja provode subjekti Unije s ciljem učenja iz zajedničkih iskustava, jačanja uzajamnog povjerenja, postizanja visoke zajedničke razine kibernetičke sigurnosti te jačanja kibernetičkih sigurnosnih kapaciteta subjekata Unije, osiguravanja da takva istorazinska ocjenjivanja provode stručnjaci za kibernetičku sigurnost koje je imenovao subjekt Unije koji nije subjekt Unije koji se ocjenjuje te da se metodologija temelji na članku 19. Direktive (EU) 2022/2555 i da je, prema potrebi, prilagođena subjektima Unije;

(e) na temelju prijedloga voditelja CERT-EU-a odobrava godišnji program rada CERT-EU-a i prati njegovu provedbu;

(f) na temelju prijedloga voditelja CERT-EU-a odobrava katalog usluga CERT-EU-a i sva ažuriranja tog kataloga;

(g) na temelju prijedloga voditelja CERT-EU-a odobrava godišnji financijski plan prihoda i rashoda, uključujući za osoblje, za aktivnosti CERT-EU-a;

(h) na temelju prijedloga voditelja CERT-EU-a odobrava dogovore o sporazumima o razini usluga;

(i) pregledava i odobrava godišnje izvješće koje sastavlja voditelj CERT-EU-a, a kojim su obuhvaćene aktivnosti CERT-EU-a i upravljanje njegovim sredstvima;

(j) odobrava i prati ključne pokazatelje uspješnosti CERT-EU-a utvrđene na temelju prijedloga voditelja CERT-EU-a;

(k) odobrava aranžmane za suradnju te dogovore ili ugovore o razini usluga između CERT-EU-a i drugih subjekata na temelju članka 18.;

(l) donosi smjernice i preporuke na temelju prijedloga CERT-EU-a u skladu s člankom 14. i upućuje CERT-EU da izda, povuče ili izmijeni prijedlog smjernica ili preporuke ili poziv na djelovanje;

(m) osniva tehničke savjetodavne skupine sa specifičnim zadaćama za pomoć u radu IICB-a, odobrava opise njihovih poslova i imenuje njihove predsjednike;

(n) prima i ocjenjuje dokumente i izvješća koje podnose subjekti Unije u skladu s ovom Uredbom, kao što su procjene zrelosti kibernetičke sigurnosti;

(o) podupire osnivanje neformalne skupine lokalnih službenika za kibernetičku sigurnost subjekata Unije, uz potporu ENISA-e, s ciljem razmjene najbolje prakse i informacija u vezi s provedbom ove Uredbe;

(p) uzimajući u obzir informacije CERT-EU-a o utvrđenim kibernetičkim sigurnosnim rizicima i stečenim iskustvima, prati primjerenost aranžmana međupovezanosti IKT okruženja subjekata Unije i savjetuje o mogućim poboljšanjima;

(q) uspostavlja plan za upravljanje kibernetičkim krizama s ciljem podupiranja, na operativnoj razini, koordiniranog upravljanja velikim incidentima koji utječu na subjekte Unije i s ciljem doprinošenja redovitoj razmjeni relevantnih informacija, posebno u pogledu učinaka i ozbiljnosti velikih incidenata te mogućih načina ublažavanja njihovih učinaka;

(r) koordinira donošenje pojedinačnih planova subjekata Unije za upravljanje kibernetičkim krizama iz članka 9. stavka 2.;

(s) donosi preporuke koje se odnose na sigurnost lanca opskrbe iz članka 8. stavka 2. prvog podstavka točke (m) uzimajući u obzir rezultate koordiniranih procjena sigurnosnih rizika ključnih lanaca opskrbe na razini Unije iz članka 22. Direktive (EU) 2022/2555 kako bi subjektima Unije pomogao u donošenju djelotvornih i razmjernih mjera upravljanja kibernetičkim sigurnosnim rizicima.

Članak 12.

Usklađenost

1. IICB u skladu člankom 10. stavkom 2. i člankom 11. djelotvorno prati kako subjekti Unije provode ovu Uredbu i donesene smjernice, preporuke i pozive na djelovanje. IICB može od subjekata Unije zatražiti informacije ili dokumentaciju koji su potrebni u tu svrhu. Za potrebe donošenja mjera usklađivanja na temelju ovog članka, ako je dotični subjekt Unije izravno zastupljen u IICB-u, taj subjekt Unije nema glasačka prava.

2. Ako IICB utvrdi da subjekt Unije ne provodi djelotvorno ovu Uredbu ili smjernice, preporuke ili pozive na djelovanje izdane na temelju ove Uredbe, IICB može, ne dovodeći u pitanje interne postupke dotičnog subjekta Unije i nakon što dotičnom subjektu Unije omogući da se očituje:

(a) dostaviti obrazloženo mišljenje dotičnom subjektu Unije u kojem navodi uočene nedostatke u provedbi ove Uredbe;

(b) nakon savjetovanja s CERT-EU-om dati smjernice dotičnom subjektu Unije kako bi osigurao da se njegov Okvir, njegove mjere upravljanja kibernetičkim sigurnosnim rizicima, njegov plan za kibernetičku sigurnost i njegovo izvješćivanje usklade s ovom Uredbom u utvrđenom roku;

(c) izdati upozorenje radi rješavanja utvrđenih nedostataka u utvrđenom roku, uključujući preporuke za izmjenu mjera koje je dotični subjekt Unije donio u skladu s ovom Uredbom;

(d) izdati obrazloženu obavijest dotičnom subjektu Unije u slučaju da nedostatci utvrđeni u upozorenju izdanom u skladu s točkom (c) nisu riješeni u dovoljnoj mjeri u utvrđenom roku;

(e) izdati:

i. preporuku za provođenje revizije, ili

ii. zahtjev da reviziju provede služba za reviziju treće strane;

(f) ako je primjenjivo, obavijestiti Revizorski sud, u okviru svojih ovlasti, o navodnoj neusklađenosti;

(g) izdati preporuku da sve države članice i subjekti Unije provedu privremenu suspenziju protokâ podataka dotičnom subjektu Unije.

Za potrebe prvog podstavka točke (c) broj primatelja upozorenja primjereno se ograničava ako je to potrebno s obzirom na kibernetički sigurnosni rizik.

Upozorenja i preporuke izdani u skladu s prvim podstavkom upućuju se najvišoj rukovodećoj razini dotičnog subjekta Unije.

3. Ako je IICB donio mjere u skladu sa stavkom 2. prvim podstavkom točkama od (a) do (g), dotični subjekt Unije dostavlja pojedinosti o mjerama i djelovanjima poduzetima radi otklanjanja navodnih nedostataka koje je utvrdio IICB. Subjekt Unije dostavlja te pojedinosti u razumnom roku koji treba dogovoriti s IICB-om.

4. Ako IICB smatra da subjekt Unije ustrajno krši ovu Uredbu, što je izravna posljedica radnji ili propusta dužnosnika ili drugog službenika Unije, među ostalim na najvišoj rukovodećoj razini, IICB zahtijeva da dotični subjekt poduzme odgovarajuće mjere, uključujući stegovne prirode, u skladu s pravilima i postupcima utvrđenima u Pravilniku o osoblju i drugim primjenjivim pravilima i postupcima. U tu svrhu IICB prenosi potrebne informacije dotičnom subjektu Unije.

5. Ako subjekti Unije obavijeste da nisu u mogućnosti poštovati rokove utvrđene u članku 6. stavku 1. i članku 8. stavku 1., IICB može u opravdanim slučajevima odobriti njihovo produljenje, uzimajući u obzir veličinu subjekta Unije.

POGLAVLJE IV.

CERT-EU

Članak 13.

Misija i zadaće CERT-EU-a

1. Misija CERT-EU-a jest doprinositi sigurnosti neklasificiranog IKT okruženja subjekata Unije tako što im pruža savjete o kibernetičkoj sigurnosti, pomaže im u sprečavanju, otkrivanju i ublažavanju incidenata, postupanju s njima, odgovoru na njih i oporavku od njih te tako što preuzima ulogu njihova koordinacijskog čvorišta za razmjenu informacija o kibernetičkoj sigurnosti i za odgovor na incidente.

2. CERT-EU prikuplja informacije o kibernetičkim prijetnjama, ranjivostima i incidentima u neklasificiranoj IKT infrastrukturi te upravlja njima, analizira ih i razmjenjuje sa subjektima Unije. Koordinira odgovore na incidente na međuinstitucijskoj razini i razini subjekata Unije, među ostalim pružanjem ili koordinacijom pružanja specijalizirane operativne pomoći.

3. CERT-EU obavlja sljedeće zadaće kako bi pomagao subjektima Unije:

(a) pruža im potporu u provedbi ove Uredbe i doprinosi koordinaciji provedbe ove Uredbe putem mjera navedenih u članku 14. stavku 1. ili putem ad hoc izvješća koja je zatražio IICB;

(b) nudi standardne usluge CSIRT-ova za subjekte Unije putem paketa kibernetičkih sigurnosnih usluga opisanih u njegovu katalogu usluga („osnovne usluge”);

(c) održava mrežu kolega i suradnika radi pružanja potpore uslugama, kako je navedeno u člancima 17. i 18.;

(d) skreće pozornost IICB-a na sve probleme koji se odnose na provedbu ove Uredbe i provedbu smjernica, preporuka i pozivâ na djelovanje;

(e) na temelju informacija iz stavka 2. doprinosi informiranosti o stanju kibernetičke sigurnosti situaciji u Uniji u bliskoj suradnji s ENISA-om;

(f) koordinira upravljanje velikim incidentima;

(g) u ime subjekata Unije djeluje kao ekvivalent koordinatora imenovanog za potrebe koordiniranog otkrivanja ranjivosti u skladu s člankom 12. stavkom 1. Direktive (EU) 2022/2555;

(h) na zahtjev subjekta Unije osigurava proaktivno neinvazivno skeniranje javno dostupnih mrežnih i informacijskih sustava tog subjekta Unije.

Informacije iz prvog podstavka točke (e) dijele se s IICB-om, mrežom CSIRT-ova i Obavještajnim i situacijskim centrom Europske unije (EU INTCEN), ako je to primjenjivo i primjereno, te podložno odgovarajućim uvjetima povjerljivosti.

4. CERT-EU može prema potrebi, u skladu s člankom 17. ili 18., surađivati s relevantnim zajednicama u području kibernetičke sigurnosti u Uniji i njezinim državama članicama, među ostalim u sljedećim područjima:

(a) pripravnost, koordinacija incidenata, razmjena informacija i odgovor na krize na tehničkoj razini u slučajevima povezanima sa subjektima Unije;

(b) operativna suradnja u pogledu mreže CSIRT-ova, među ostalim u pogledu uzajamne pomoći;

(c) saznanja o kibernetičkim prijetnjama, uključujući informiranost o stanju;

(d) sve teme za koje je potrebna tehnička stručnost CERT-EU-a u području kibernetičke sigurnosti.

5. CERT-EU u okviru svojih nadležnosti sudjeluje u strukturiranoj suradnji s ENISA-om na izgradnji kapaciteta, operativnoj suradnji i dugoročnim strateškim analizama kibernetičkih prijetnji u skladu s Uredbom (EU) 2019/881. CERT-EU može surađivati i razmjenjivati informacije s Europolovim Centrom za kibernetički kriminalitet.

6. CERT-EU može pružati sljedeće usluge koje nisu opisane u njegovu katalogu usluga („usluge uz naknadu”):

(a) usluge kojima se podupire kibernetička sigurnost IKT okruženja subjekata Unije, osim onih iz stavka 3., na temelju sporazumâ o razini usluga i ovisno o dostupnim resursima, osobito praćenje mreža širokog spektra, uključujući prvu liniju nadzora za vrlo ozbiljne kibernetičke prijetnje 24 sata dnevno sedam dana u tjednu;

(b) usluge kojima se podupiru kibernetičke sigurnosne operacije ili kibernetički sigurnosni projekti subjekata Unije koje ne služe za zaštitu njihova IKT okruženja, na temelju pisanih sporazuma i uz prethodno odobrenje IICB-a;

(c) na zahtjev, proaktivno skeniranje mrežnih i informacijskih sustava dotičnog subjekta Unije kako bi se otkrile ranjivosti koje bi mogle imati znatan učinak;

(d) usluge kojima se podupire sigurnost IKT okruženja organizacija koje nisu subjekti Unije, a koje blisko surađuju sa subjektima Unije, na primjer zbog zadaća ili dužnosti koje su im dodijeljene na temelju prava Unije, na temelju pisanih sporazuma i uz prethodno odobrenje IICB-a.

Kad je riječ o prvom podstavku točki (d), CERT-EU može iznimno sklapati sporazume o razini usluga sa subjektima koji nisu subjekti Unije uz prethodno odobrenje IICB-a.

7. CERT-EU organizira vježbe u području kibernetičke sigurnosti i može sudjelovati u njima ili preporučiti sudjelovanje u postojećim vježbama, ako je to primjenjivo u bliskoj suradnji s ENISA-om, kad je to primjenjivo, kako bi se testirala razina kibernetičke sigurnosti subjekata Unije.

8. CERT-EU može pružiti pomoć subjektima Unije u pogledu incidenata u mrežnim i informacijskim sustavima u kojima se postupa s kvalificiranim podatcima EU-a ako dotični subjekti Unije to izričito zatraže u skladu sa svojim postupcima. Pružanjem pomoći CERT-EU-a na temelju ovog stavka ne dovode se u pitanje primjenjiva pravila o zaštiti klasificiranih podataka.

9. CERT-EU obavješćuje subjekte Unije o svojim postupcima i procesima za postupanje s incidentima.

10. CERT-EU s visokom razinom povjerljivosti i pouzdanosti putem odgovarajućih mehanizama suradnje i linija izvješćivanja doprinosi relevantnim i anonimiziranim informacijama o velikim incidentima i načinu na koji se postupalo s njima. Te se informacije unose u izvješće iz članka 10. stavka 14.

11. CERT-EU u suradnji s Europskim nadzornikom za zaštitu podataka podupire dotične subjekte Unije pri rješavanju incidenata koji za posljedicu imaju povrede osobnih podataka, ne dovodeći u pitanje nadležnosti i zadaće Europskog nadzornika za zaštitu podatak kao nadzornog tijela u skladu s Uredbom (EU) 2018/1725.

12. Ako to resorni odjeli subjekata Unije izričito zatraže, CERT-EU može pružiti tehnički savjet ili tehnička mišljenja o relevantnim pitanjima vezanima uz politike.

Članak 14.

Smjernice, preporuke i pozivi na djelovanje

1. CERT-EU podupire provedbu ove Uredbe:

(a) izdavanjem poziva na djelovanje u kojima se opisuju hitne sigurnosne mjere koje subjekti Unije trebaju poduzeti u zadanom roku;

(b) podnošenjem prijedloga IICB-u za smjernice upućene svim subjektima Unije ili nekoj njihovoj podskupini;

(c) podnošenjem prijedloga IICB-u za preporuke upućene pojedinačnim subjektima Unije.

U pogledu prvog podstavka točke (a), dotični subjekt Unije bez nepotrebne odgode nakon primitka poziva na djelovanje obavješćuje CERT-EU o načinu primjene hitnih sigurnosnih mjera.

2. Smjernice i preporuke mogu sadržavati:

(a) zajedničke metodologije i model za procjenu zrelosti kibernetičke sigurnosti subjekata Unije, uključujući odgovarajuće ljestvice ili ključne pokazatelje uspješnosti, koji služe kao referenca za potporu kontinuiranom poboljšanju kibernetičke sigurnosti u svim subjektima Unije i olakšavaju određivanje prioriteta među područjima i mjerama kibernetičke sigurnosti uzimajući u obzir razinu kibernetičke sigurnosti subjekata;

(b) aranžmane za upravljanje kibernetičkim sigurnosnim rizicima i mjere za upravljanje kibernetičkim sigurnosnim rizicima ili za njihovo poboljšanje;

(c) aranžmane za procjenu zrelosti kibernetičke sigurnosti i planove za kibernetičku sigurnost

(d) prema potrebi, upotrebu zajedničke tehnologije, arhitekture, otvorenog koda i povezane najbolje prakse radi postizanja interoperabilnosti i zajedničkih standarda, uključujući koordinirani pristup sigurnosti lanca opskrbe;

(e) prema potrebi, informacije kojima se olakšava upotreba instrumenata zajedničke nabave za kupnju relevantnih kibernetičkih sigurnosnih usluga i proizvoda od vanjskih dobavljača;

(f) aranžmani za razmjenu informacija u skladu s člankom 20.

Članak 15.

Voditelj CERT-EU-a

1. Nakon što dobije odobrenje dvotrećinske većine članova IICB-a, Komisija imenuje voditelja CERT-EU-a. Savjetovanje s IICB-om obavezno je u svim fazama postupka imenovanja, osobito pri izradi obavijesti o slobodnom radnom mjestu, razmatranju prijava i imenovanju odbora za odabir za radno mjesto. Postupkom odabira, uključujući konačni uži popis kandidata s kojeg se imenuje voditelj CERT-EU-a, osigurava se pravedna zastupljenost svakog spola, uzimajući u obzir podnesene prijave.

2. Voditelj CERT-EU-a odgovoran je za pravilno funkcioniranje CERT-EU-a i djeluje u okviru svog djelokruga i pod vodstvom IICB-a. Voditelj CERT-EU-a redovito podnosi izvješća predsjedniku IICB-a i podnosi ad hoc izvješća IICB-u na njegov zahtjev.

3. Voditelj CERT-EU-a pomaže odgovornom dužnosniku kojem je delegirana ovlast ovjeravanja u sastavljanju godišnjeg izvješća o radu, koje sadržava financijske informacije i informacije o upravljanju, uključujući rezultate kontrola, koje se sastavlja u skladu s člankom 74. stavkom 9. Uredbe (EU, Euratom) 2018/1046 Europskog parlamenta i Vijeća ([9]) te redovito izvješćuje dužnosnika kojem je delegirana ovlast ovjeravanja o provedbi mjera u pogledu kojih su ovlasti dalje delegirane voditelju CERT-EU-a.

4. Voditelj CERT-EU-a svake godine izrađuje financijski plan administrativnih prihoda i rashoda za svoje aktivnosti, prijedlog godišnjeg programa rada, prijedlog kataloga usluga CERT-EU-a, prijedloge za reviziju kataloga usluga, prijedlog dogovora za sporazume o razini usluga i prijedlog ključnih pokazatelja uspješnosti za CERT-EU koje treba odobriti IICB u skladu s člankom 11. Pri reviziji popisa usluga u katalogu usluga CERT-EU-a voditelj CERT-EU-a uzima u obzir resurse dodijeljene CERT-EU-u.

5. Voditelj CERT-EU-a najmanje jednom godišnje podnosi IICB-u i predsjedniku IICB-a izvješća o aktivnostima i uspješnosti CERT-EU-a tijekom referentnog razdoblja, među ostalim o izvršenju proračuna, sklopljenim sporazumima o razini usluga i pisanim sporazumima, suradnji s partnerima i suradnicima te službenim putovanjima osoblja, uključujući izvješća iz članka 11. Ta izvješća uključuju program rada za sljedeće razdoblje, financijsko planiranje prihoda i rashoda, uključujući za osoblje, planirano ažuriranje kataloga usluga CERT-EU-a i procjenu očekivanog učinka koji bi takva ažuriranja mogla imati na financijske i ljudske resurse.

Članak 16.

Financijska pitanja i osoblje

1. CERT-EU integriran je u administrativnu strukturu glavne uprave Komisije kako bi imao koristi od potpornih struktura Komisije u području administracije, financijskog upravljanja i računovodstva, zadržavajući pritom svoj status neovisnog međuinstitucijskog pružatelja usluga za sve subjekte Unije. Komisija obavješćuje IICB o administrativnom sjedištu CERT-EU-a i svim njegovim promjenama. Komisija redovito preispituje administrativne aranžmane koji se odnose na CERT-EU, a u svakom slučaju prije donošenja višegodišnjeg financijskog okvira u skladu s člankom 312. UFEU-a, kako bi se omogućilo poduzimanje odgovarajućih mjera. Preispitivanje uključuje mogućnost uspostave CERT-EU-a kao ureda Unije.

2. Tijekom primjene upravnih i financijskih postupaka voditelj CERT-EU-a djeluje u okviru ovlasti Komisije i pod nadzorom IICB-a.

([9]) Uredba (EU, Euratom) 2018/1046 Europskog parlamenta i Vijeća od 18. srpnja 2018. o financijskim pravilima koja se primjenjuju na opći proračun Unije, o izmjeni uredaba (EU) br. 1296/2013, (EU) br. 1301/2013, (EU) br. 1303/2013, (EU) br. 1304/2013, (EU) br. 1309/2013, (EU) br. 1316/2013, (EU) br. 223/2014, (EU) br. 283/2014 i Odluke br. 541/2014/EU te o stavljanju izvan snage Uredbe (EU, Euratom) br. 966/2012 (SL L 193, 30.7.2018., str. 1.).

3. Zadaće i aktivnosti CERT-EU-a, uključujući usluge koje CERT-EU pruža u skladu s člankom 13. stavcima 3., 4., 5. i 7. i člankom 14. stavkom 1. subjektima Unije financiranima iz naslova višegodišnjeg financijskog okvira namijenjenog europskoj javnoj upravi, financiraju se iz posebne proračunske linije proračuna Komisije. Radna mjesta namijenjena CERT-EU-u detaljno se navode u bilješci uz plan radnih mjesta Komisije.

4. Subjekti Unije, osim onih iz stavka 3. ovog članka, daju godišnji financijski doprinos CERT-EU-u za pokrivanje usluga koje CERT-EU pruža u skladu s tim stavkom. Doprinosi se temelje na smjernicama koje je dao IICB i svi ih subjekti Unije dogovaraju s CERT-EU-om u sporazumima o razini usluga. Doprinosi odgovaraju pravednom i razmjernom udjelu u ukupnim troškovima pruženih usluga. Zaprimaju se u posebnoj proračunskoj liniji iz stavka 3. ovog članka kao unutarnji namjenski prihod, kako je predviđeno u članku 21. stavku 3. točki (c) Uredbe (EU, Euratom) 2018/1046.

5. Troškove usluga predviđenih u članku 13. stavku 6. nadoknađuju subjekti Unije koji se koriste uslugama CERT-EU-a. Prihodi se dodjeljuju proračunskim linijama kojima se financiraju navedeni troškovi.

Članak 17.

Suradnja CERT-EU-a s partnerima iz država članica

1. CERT-EU bez nepotrebne odgode surađuje i razmjenjuje informacije s partnerima iz država članica, osobito s CSIRT-ovima imenovanima ili uspostavljenima na temelju članka 10. Direktive (EU) 2022/2555, ili, ako je to primjenjivo, s nadležnim tijelima i jedinstvenim kontaktnim točkama imenovanima ili uspostavljenima na temelju članka 8. te direktive, u pogledu incidenata, kibernetičkih prijetnji, ranjivosti, izbjegnutih incidenata, mogućih protumjera te najbolje prakse i o svim pitanjima važnima za poboljšanje zaštite IKT okruženja subjekata Unije, među ostalim putem mreže CSIRT-ova uspostavljene na temelju članka 15. Direktive (EU) 2022/2555. CERT-EU podupire Komisiju u okviru mreže EU-CyCLONe osnovane člankom 16. Direktive (EU) 2022/2555 pri koordiniranom upravljanju kibernetičkim incidentima velikih razmjera i kibernetičkim krizama.

2. Ako CERT-EU sazna za značajni incident do kojeg je došlo na državnom području pojedine države članice, o tome bez odgode obavješćuje svakog relevantnog partnera u toj državi članici, u skladu sa stavkom 1.

3. Pod uvjetom da su osobni podatci zaštićeni u skladu s primjenjivim pravom Unije o zaštiti podataka CERT-EU bez nepotrebne odgode razmjenjuje relevantne informacije specifične za određeni incident s partnerima iz država članica kako bi se olakšalo otkrivanje sličnih kibernetičkih prijetnji ili incidenata ili kako bi se dao doprinos analizi incidenta, bez odobrenja pogođenog subjekta Unije. CERT-EU smije razmjenjivati informacije specifične za određeni incident kojima se otkriva identitet mete incidenta samo u slučaju jedne od sljedećih situacija:

(a) pogođeni subjekt Unije dao je suglasnost;

(b) pogođeni subjekt Unije nije dao suglasnost u skladu s točkom (a), ali bi se otkrivanjem identiteta pogođenog subjekta Unije povećala vjerojatnost da bi se incidenti drugdje izbjegli ili da bi se ublažili njihovi učinci;

(c) pogođeni subjekt Unije već je objavio da je bio pogođen incidentom.

Odluke o razmjeni informacija specifičnih za određeni incident kojima se otkriva identitet mete incidenta u skladu s prvim podstavkom točkom (b) potvrđuje voditelj CERT-EU-a. Prije donošenja takve odluke CERT-EU pisanim putem stupa u kontakt s pogođenim subjektom Unije i jasno objašnjava način na koji bi otkrivanje njegova identiteta pomoglo u izbjegavanju ili ublažavanju incidenata drugdje. Voditelj CERT-EU-a daje objašnjenje i izričito traži od subjekta Unije da se u utvrđenom roku izjasni daje li suglasnost. Voditelj CERT-EU-a također obavješćuje subjekt Unije da, s obzirom na dano objašnjenje, zadržava pravo na otkrivanje informacija čak i bez suglasnosti. Pogođeni subjekt Unije obavješćuje se prije otkrivanja informacija.

Članak 18.

Suradnja CERT-EU-a s ostalim partnerima

1. CERT-EU može s partnerima iz Unije koji nisu partneri iz članka 17., a koji podliježu zahtjevima Unije u pogledu kibernetičke sigurnosti, uključujući partnere iz određenih industrijskih sektora, surađivati u vezi s alatima i metodama, kao što su tehnike, taktike, postupci i najbolja praksa, te u vezi s kibernetičkim prijetnjama i ranjivostima. Za svu suradnju s takvim partnerima CERT-EU mora tražiti prethodno odobrenje IICB-a na pojedinačnoj osnovi. Ako CERT-EU uspostavi suradnju s takvim partnerima, obavješćuje sve relevantne partnere iz države članice iz članka 17. stavka 1. u državi članici u kojoj se nalazi partner. Ako je to primjenjivo i primjereno, takva suradnja i njezini uvjeti, među ostalim u pogledu kibernetičke sigurnosti, zaštite podataka i postupanja s informacijama, utvrđuju se u posebnim aranžmanima o povjerljivosti, kao što su ugovori ili administrativni dogovori. Aranžmani o povjerljivosti podataka ne zahtijevaju prethodno odobrenje IICB-a, ali se o tome obavješćuje predsjednika IICB-a. U slučaju hitne i neposredne potrebe za razmjenom informacija o kibernetičkoj sigurnosti u interesu subjekata Unije ili druge strane, CERT-EU može razmijeniti takve informacije sa subjektom čija su posebna stručnost, kapacitet i stručnost opravdano potrebni za pružanje pomoći u pogledu takve hitne i neposredne potrebe, čak i ako CERT-EU nije uspostavio aranžman o povjerljivosti s tim subjektom. U takvim slučajevima CERT-EU odmah obavješćuje predsjednika IICB-a i izvješćuje IICB podnošenjem redovitih izvješća ili na sastancima.

2. CERT-EU može surađivati sa suradnicima, kao što su komercijalni subjekti, uključujući subjekte iz određenih industrijskih sektora, međunarodne organizacije, nacionalni subjekti izvan Unije ili pojedinačni stručnjaci, kako bi prikupio informacije o općim i specifičnim kibernetičkim prijetnjama, izbjegnutim incidentima, ranjivostima i mogućim protumjerama. Za opsežniju suradnju s tim suradnicima CERT-EU mora tražiti prethodno odobrenje IICB-a na pojedinačnoj osnovi.

3. CERT-EU može, uz suglasnost subjekta Unije pogođenog incidentom i pod uvjetom da postoji aranžman ili ugovor o povjerljivosti podataka s relevantnim partnerom ili suradnikom, pružiti informacije o određenom incidentu drugim partnerima ili suradnicima iz stavaka 1. i 2. isključivo u svrhu doprinosa njegovoj analizi.

POGLAVLJE V.

OBVEZE SURADNJE I IZVJESCIVANJA

Članak 19.

Postupanje s informacijama

1. Subjekti Unije i CERT-EU poštuju obvezu čuvanja poslovne tajne u skladu s člankom 339. UFEU-a ili u skladu s jednakovrijednim primjenjivim okvirima.

2. Uredba (EZ) br. 1049/2001 Europskog parlamenta i Vijeća ([10]) primjenjuje se na zahtjeve za javni pristup dokumentima koje posjeduje CERT-EU, uključujući obvezu savjetovanja, na temelju te uredbe, s drugim subjektima Unije, ili, ako je relevantno, državama članicama, kad se zahtjev odnosi na njihove dokumente.

3. Postupanje subjekata Unije i CERT-EU-a s podatcima mora biti u skladu s primjenjivim pravilima o sigurnosti podataka.

([10]) Uredba (EZ) br. 1049/2001 Europskog parlamenta i Vijeća od 30. svibnja 2001. o javnom pristupu dokumentima Europskog parlamenta, Vijeća i Komisije (SL L 145, 31.5.2001., str. 43.).

Članak 20.

Aranžmani za razmjenu informacija o kibernetičkoj sigurnosti

1. Subjekti Unije mogu CERT-EU-u dobrovoljno dostaviti informacije o incidentima, kibernetičkim prijetnjama, izbjegnutim incidentima i ranjivostima koji na njih utječu. CERT-EU osigurava dostupnost učinkovitih sredstava komunikacije s visokom razinom sljedivosti, povjerljivosti i pouzdanosti u svrhu olakšavanja razmjene informacija sa subjektima Unije. Pri obradi obavijesti CERT-EU može dati prednost obradi obveznih obavijesti pred obradom obavijesti na dobrovoljnoj osnovi. Ne dovodeći u pitanje članak 12., subjektu Unije koji je obavijest podnio dobrovoljno ne smiju se zbog tog obavješćivanja nametati dodatne obveze, kojima ne bi podlijegao da nije podnio tu obavijest.

2. Kako bi obavio svoju misiju i zadaće koje su mu dodijeljene u skladu s člankom 13., CERT-EU može od subjekata Unije zatražiti da mu iz svojih evidencija IKT sustava dostave informacije, uključujući informacije koje se odnose na kibernetičke prijetnje, izbjegnute incidente, ranjivosti, pokazatelje ugroženosti, kibernetička sigurnosna upozorenja i preporuke o konfiguraciji kibernetičkih sigurnosnih alata za otkrivanje incidenata. Subjekt Unije kojem je podnesen zahtjev bez nepotrebne odgode dostavlja tražene informacije i sva njihova naknadna ažuriranja.

3. CERT-EU može razmjenjivati sa subjektima Unije informacije specifične za određeni incident kojima se otkriva identitet subjekta Unije pogođenog incidentom pod uvjetom da subjekt Unije pogođen incidentom za to dade suglasnost. Ako subjekt Unije uskrati suglasnost, on dostavlja CERT-EU-u razloge kojima potkrepljuje tu odluku.

4. Subjekti Unije na zahtjev razmjenjuju informacije s Europskim parlamentom i Vijećem o dovršetku planova za kibernetičku sigurnost.

5. IICB ili CERT-EU, ovisno o slučaju, dostavljaju smjernice, preporuke i pozive na djelovanje Europskom parlamentu i Vijeću na njihov zahtjev.

6. Obveze razmjene informacija utvrđene u ovom članku ne odnose se na:

(a) klasificirane podatke EU-a,

(b) informacije čija je daljnja distribucija isključena vidljivom oznakom, osim ako je njihova razmjena s CERT-EU-om izričito dopuštena.

Članak 21.

Obveze izvješćivanja

1. Incident se smatra značajnim:

(a) ako je uzrokovao ili može uzrokovati ozbiljne poremećaje u funkcioniranju dotičnog subjekta Unije ili financijski gubitak dotičnom subjektu Unije;

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

2. Subjekti Unije podnose CERT-EU-u:

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

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

(c) na zahtjev CERT-EU-a, privremeno izvješće o relevantnim ažuriranjima statusa;

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

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

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

iii. primijenjene mjere ublažavanja i mjere ublažavanja koje su u tijeku;

iv. ako je to primjenjivo, prekogranični učinak incidenta ili njegov učinak na ostale subjekte;

(e) u slučaju incidenta koji je u tijeku u trenutku podnošenja završnog izvješća iz točke (d), izvješće o napretku u tom trenutku i završno izvješće u roku od mjesec dana od postupanja u vezi s incidentom.

3. Subjekt Unije bez nepotrebne odgode, a u svakom slučaju u roku od 24 sata od kad sazna za značajni incident, obavješćuje sve relevantne partnere iz država članica iz članka 17. stavka 1. u državi članici u kojoj se nalazi o tome da se dogodio značajni incident.

4. Subjekti Unije obavješćuju, među ostalim, o svim informacijama koje CERT-EU-u omogućuju da utvrdi učinak incidenta na ostale subjekte, učinak na državu članicu domaćina ili prekogranični učinak nakon značajnog incidenta. Ne dovodeći u pitanje članak 12., subjekt Unije koji obavješćuje ne podliježe samo zbog toga povećanoj odgovornosti.

5. Ako je to primjenjivo, subjekti Unije bez nepotrebne odgode obavješćuju korisnike pogođenih mrežnih i informacijskih sustava ili drugih komponenti IKT okruženja na koje bi mogao utjecati značajan incident ili ozbiljna kibernetička prijetnja ili koji, prema potrebi, moraju poduzeti mjere ublažavanja, o svim mjerama ili postupcima koji se mogu poduzeti kao odgovor na taj incident ili tu prijetnju. Subjekti Unije prema potrebi obavješćuju te korisnike o samoj ozbiljnoj kibernetičkoj prijetnji.

6. Ako značajan incident ili ozbiljna kibernetička prijetnja utječe na mrežni i informacijski sustav ili komponentu IKT okruženja subjekta Unije za koje je poznato da su mu mrežni i informacijski sustav ili komponenta IKT okruženja povezani s IKT okruženjem drugog subjekta Unije, CERT-EU izdaje odgovarajuće kibernetičko sigurnosno upozorenje.

7. Subjekti Unije na zahtjev CERT-EU-a i bez nepotrebne odgode dostavljaju CERT-EU-u digitalne informacije nastale upotrebom elektroničkih uređaja u dotičnim incidentima. CERT-EU može dodatno pojasniti koje su mu vrste informacija potrebne za informiranost o stanju i odgovor na incident.

8. CERT-EU svaka tri mjeseca IICB-u, ENISA-i, EU INTCEN-u i mreži CSIRT-ova podnosi sažeto izvješće koje uključuje anonimizirane i agregirane podatke o značajnim incidentima, incidentima, kibernetičkim prijetnjama, izbjegnutim incidentima i ranjivostima u skladu s člankom 20. i značajnim incidentima prijavljenima u skladu sa stavkom 2. ovog članka. Sažeto izvješće doprinos je dvogodišnjem izvješću o stanju kibernetičke sigurnosti u Uniji donesenom na temelju članka 18. Direktive (EU) 2022/2555.

9. IICB do 8. srpnja 2024. izdaje smjernice ili preporuke kojima se pobliže određuju aranžmani te oblik i sadržaj izvješćivanja u skladu s ovim člankom. IICB pri pripremi takvih smjernica ili preporuka uzima u obzir sve provedbene akte donesene na temelju članka 23. stavka 11. Direktive (EU) 2022/2555 kojima se utvrđuju vrsta informacija, oblik i postupak izvješćivanja. CERT-EU prosljeđuje odgovarajuće tehničke pojedinosti kako bi se subjektima Unije omogućilo poduzimanje proaktivnih mjera za otkrivanje, odgovor na incidente ili ublažavanje njihovih učinaka.

10. Obveze izvješćivanja utvrđene u ovom članku ne odnose se na:

(a) klasificirane podatke EU-a;

(b) informacije čija je daljnja distribucija isključena vidljivom oznakom, osim ako je njihova razmjena s CERT-EU-om izričito dopuštena.

Članak 22.

Koordinacija i suradnja pri odgovoru na incidente

1. CERT-EU djeluje kao koordinacijsko čvorište za razmjenu informacija o kibernetičkoj sigurnosti i za odgovor na incidente te tako olakšava razmjenu informacija o incidentima, kibernetičkim prijetnjama, ranjivostima i izbjegnutim incidentima među:

(a) subjektima Unije;

(b) partnerima iz članaka 17. i 18.

2. CERT-EU, ako je relevantno u bliskoj suradnji s ENISA-om, olakšava koordinaciju odgovora na incidente među subjektima Unije, uključujući:

(a) doprinos dosljednoj vanjskoj komunikaciji;

(b) uzajamnu potporu, kao što je razmjena informacija relevantnih za subjekte Unije ili pružanje pomoći, prema potrebi izravno na licu mjesta;

(c) optimalnu upotrebu operativnih resursa;

(d) koordinaciju s drugim mehanizmima za odgovor na krize na razini Unije.

3. CERT-EU, u bliskoj suradnji s ENISA-om, pruža potporu subjektima Unije u pogledu informiranosti o incidentima, kibernetičkim prijetnjama, ranjivostima i izbjegnutim incidentima te im pruža informacije o najnovijim zbivanjima u području kibernetičke sigurnosti.

4. IICB do 8. siječnja 2025. na temelju prijedloga CERT-EU-a donosi smjernice ili preporuke o koordinaciji odgovora na incidente i suradnji u slučaju značajnih incidenata. Ako se sumnja da je incident kaznene prirode, CERT-EU bez nepotrebne odgode savjetuje o tome kako prijaviti incident tijelima za izvršavanje zakonodavstva.

5. Na poseban zahtjev države članice i uz odobrenje dotičnih subjekata Unije CERT-EU može pozvati stručnjake s popisa iz članka 23. stavka 4. kako bi doprinijeli odgovoru na veliki incident koji ima učinak u toj državi članici ili kibernetički sigurnosni incident velikih razmjera u skladu s člankom 15. stavkom 3. točkom (g) Direktive (EU) 2022/2555. IICB na prijedlog CERT EU-a odobrava posebna pravila o pristupu tehničkim stručnjacima iz subjekata Unije i njihovu djelovanju.

Članak 23.

Upravljanje velikim incidentima

1. Kako bi se na operativnoj razini pružila podrška koordiniranom upravljanju velikim incidentima koji utječu na subjekte Unije i doprinijelo redovitoj razmjeni relevantnih informacija među subjektima Unije i s državama članicama, IICB u skladu s člankom 11. točkom (q) uspostavlja plan upravljanja kibernetičkim krizama na temelju aktivnosti iz članka 22. stavka 2., u bliskoj suradnji s CERT-EU-om i ENISA-om. Plan za upravljanje kibernetičkim krizama sadržava barem sljedeće elemente:

(a) aranžmane koji se odnose na koordinaciju i protok informacija među subjektima Unije za upravljanje velikim incidentima na operativnoj razini;

(b) zajedničke standardne operativne postupke;

(c) zajedničku taksonomiju ozbiljnosti velikih incidenata i pokretačkih točaka krize;

(d) redovite vježbe;

(e) sigurne komunikacijske kanale koje treba upotrebljavati.

2. Predstavnik Komisije u IICB-u, podložno planu upravljanja kibernetičkim krizama uspostavljenom na temelju stavka 1. ovog članka i ne dovodeći u pitanje članak 16. stavak 2. prvi podstavak Direktive (EU) 2022/2555, kontaktna je točka za razmjenu relevantnih informacija o velikim incidentima s mrežom EU-CyCLONe.

3. CERT-EU koordinira upravljanje velikim incidentima među subjektima Unije. On vodi evidenciju dostupnog tehničkog stručnog znanja koje bi bilo potrebno za odgovor na incident u slučaju velikih incidenata i pomaže IICB-u u koordinaciji planova za upravljanje kibernetičkim krizama subjekata Unije iz članka 9. stavka 2. u slučaju velikih incidenata.

4. Subjekti Unije doprinose evidentiranju tehničkog stručnog znanja dostavljanjem popisa stručnjaka dostupnih u njihovim organizacijama koji se ažurira jedanput godišnje, a sadržava pojedinosti o specifičnim tehničkim vještinama stručnjaka.

POGLAVLJE VI.

ZAVRSNE ODREDBE

Članak 24.

Početna preraspodjela proračunskih sredstava

Kako bi se osiguralo pravilno i stabilno funkcioniranje CERT-EU-a, Komisija može predložiti preraspodjelu osoblja i financijskih sredstava u proračun Komisije za potrebe rada CERT-EU-a. Preraspodjela počinje proizvoditi učinke istodobno s prvim godišnjim proračunom Unije koji se donese nakon stupanja na snagu ove Uredbe.

Članak 25.

Preispitivanje

1. IICB uz potporu CERT-EU-a do 8. siječnja 2025., a nakon tog datuma jednom godišnje, podnosi Komisiji izvješće o provedbi ove Uredbe. IICB može Komisiji preporučiti da preispita ovu Uredbu.

2. Komisija do 8. siječnja 2027. i svake dvije godine nakon tog datuma ocjenjuje provedbu ove Uredbe i iskustva stečena na strateškoj i operativnoj razini te o tome izvješćuje Europski parlament i Vijeće.

Izvješće iz prvog podstavka ovog stavka obuhvaća preispitivanje iz članka 16. stavka 1. o mogućnosti uspostave CERT-EU-a kao ureda Unije.

3. Komisija do 8. siječnja 2029. evaluira funkcioniranje ove Uredbe i podnosi izvješće Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija. Komisija također evaluira primjerenost uključivanja mrežnih i informacijskih sustava u kojima se postupa s klasificiranim podatcima EU-a u područje primjene ove Uredbe, uzimajući u obzir druge zakonodavne akte Unije koji se primjenjuju na te sustave. Uz izvješće se prema potrebi prilaže zakonodavni prijedlog.

Članak 26.

Stupanje na snagu

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

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Strasbourgu 13. prosinca 2023.

Za Europski parlament	*Za Vijeće*
Predsjednica	*Predsjednik*
R. METSOLA	P. NAVARRO RÍOS