Europos Sąjungos
oficialusis leidinys

LT
L serija

2023/2841

2023 12 18

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS (ES, Euratomas) 2023/2841

2023 m. gruodžio 13 d.

kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti

EUROPOS PARLAMENTAS IR EUROPOS SĄJUNGOS TARYBA,

atsižvelgdami į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 298 straipsnį,

atsižvelgdami į Europos atominės energijos bendrijos steigimo sutartį, ypač į jos 106a straipsnį,

atsižvelgdami į Europos Komisijos pasiūlymą,

teisėkūros procedūra priimamo akto projektą perdavus nacionaliniams parlamentams,

laikydamiesi įprastos teisėkūros procedūros ([1]),

kadangi:

(1) skaitmeniniame amžiuje informacinės ir ryšių technologijos yra atviros, veiksmingos ir nepriklausomos Europos administracijos kertinis akmuo. Dėl technologijų raidos ir didesnio skaitmeninių sistemų sudėtingumo bei tarpusavio sąsajų didėja kibernetinio saugumo rizika, todėl Sąjungos subjektai tampa labiau pažeidžiami dėl kibernetinių grėsmių ir incidentų, o tai kelia grėsmę jų veiklos tęstinumui ir pajėgumui apsaugoti savo duomenis. Nors visai Sąjungos subjektų veiklai būdingas platus debesijos paslaugų naudojimas, visapusiškas informacinių ir ryšių technologijų (IRT) naudojimas, aukštas skaitmeninimo lygis, nuotolinis darbas ir besivystantys technologijos bei junglumas, skaitmeninis atsparumas vis dar užtikrintas nepakankamai;

(2) kibernetinių grėsmių, su kuriomis susiduria Sąjungos subjektai, padėtis nuolat kinta. Grėsmę keliančių subjektų naudojama taktika, metodai ir procedūros nuolat vystosi, tačiau aiškūs tokių išpuolių motyvai vargiai kinta: nuo vertingos konfidencialios informacijos vagystės iki pinigų pritraukimo, manipuliavimo viešąja nuomone ar kenkimo skaitmeninei infrastruktūrai. Grėsmę keliančių subjektų kibernetinių išpuolių vykdymo tempas vis didėja, o jų kampanijos tampa vis sudėtingesnės ir automatizuotos ir yra nukreiptos į matomą išpuolių perimetrą, kuris toliau plečiasi ir kuriame greitai išnaudojamas pažeidžiamumas;

(3) Sąjungos subjektų IRT aplinkose yra tarpusavyje priklausomų elementų ir integruotų duomenų srautų, o jų naudotojai glaudžiai bendradarbiauja. Tas tarpusavio ryšys reiškia, kad bet koks sutrikimas, net jei iš pradžių jis susijęs tik su vienu Sąjungos subjektu, gali turėti platesnį pakopinį poveikį, o šis gali turėti plataus masto ir ilgalaikių neigiamų padarinių kitiems Sąjungos subjektams. Be to, tam tikros Sąjungos subjektų IRT aplinkos yra susijusios su valstybių narių IRT aplinkomis, todėl incidentas viename Sąjungos subjekte kelia pavojų valstybių narių IRT aplinkos kibernetiniam saugumui ir atvirkščiai. Dalijimasis su incidentais susijusia informacija gali padėti aptikti panašias kibernetines grėsmes ar incidentus, darančius poveikį valstybėms narėms;

(4) Sąjungos subjektai yra patrauklūs taikiniai, kurie susiduria su aukštos kvalifikacijos ir išteklių turinčiais grėsmę keliančiais subjektais ir kitomis grėsmėmis. Tuo pačiu metu tų subjektų kibernetinio atsparumo lygis ir branda, gebėjimas aptikti kibernetinę kenkimo veiklą ir į ją reaguoti labai skiriasi. Todėl tam, kad Sąjungos subjektai veiktų, būtina, kad jie užtikrintų aukštą bendrą kibernetinio saugumo lygį, įgyvendindami kibernetinio saugumo priemones, kurios būtų proporcingos nustatytai atitinkamai kibernetinio saugumo rizikai, keisdamiesi informacija ir bendradarbiaudami;

([1]) 2023 m. lapkričio 21 d. Europos Parlamento pozicija (dar nepaskelbta Oficialiajame leidinyje) ir 2023 m. gruodžio 8 d. Tarybos sprendimas.

(5) Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 ([2]) siekiama toliau didinti viešųjų ir privačiųjų subjektų, kompetentingų institucijų ir įstaigų ir visos Sąjungos kibernetinį atsparumą ir reagavimo į incidentus pajėgumus. Todėl būtina užtikrinti, kad Sąjungos subjektai to laikytųsi, nustatydami taisykles, kurios atitiktų Direktyvą (ES) 2022/2555 ir atspindėtų jos užmojų mastą;

(6) aukštam bendram kibernetinio saugumo lygiui pasiekti būtina, kad kiekvienas Sąjungos subjektas nustatytų vidaus kibernetinio saugumo rizikos valdymo, administravimo ir kontrolės sistemą (toliau – Sistema), kuria būtų užtikrinamas veiksmingas ir apdairus visų kibernetinio saugumo rizikos veiksnių valdymas ir atsižvelgiama į veiklos tęstinumą ir krizių valdymą. Sistemoje turėtų būti nustatyta tinklo ir informacinių sistemų, kurios apima visą neįslaptintą IRT aplinką, kibernetinio saugumo politika, įskaitant tikslus ir prioritetus. Sistema turėtų būti grindžiama visus pavojus apimančiu požiūriu, kuriuo siekiama apsaugoti tinklų ir informacines sistemas bei tų sistemų fizinę aplinką nuo tokių įvykių kaip vagystė, gaisras, potvynis, telekomunikacijų ar energijos tiekimo triktys arba nuo neleistinos fizinės prieigos prie Sąjungos subjekto informacijos ir informacijos tvarkymo objektų ir žalos jiems ir jų trikdžių, kurie galėtų kelti pavojų saugomų, perduodamų, tvarkomų arba per tinklų ir informacines sistemas prieinamų duomenų prieinamumui, autentiškumui, vientisumui ar konfidencialumui;

(7) kad galėtų valdyti pagal Sistemą nustatytą kibernetinio saugumo riziką, kiekvienas Sąjungos subjektas turėtų imtis tinkamų ir proporcingų techninių, operacinių ir organizacinių priemonių. Tos priemonės turėtų apimti šiame reglamente nustatytas sritis ir kibernetinio saugumo rizikos valdymo priemones, kuriomis siekiama stiprinti kiekvieno Sąjungos subjekto kibernetinį saugumą;

(8) Sistemoje nustatytas turtas ir kibernetinio saugumo rizika, taip pat reguliarių kibernetinio saugumo brandos vertinimų išvados turėtų atsispindėti kiekvieno Sąjungos subjekto parengtame kibernetinio saugumo plane. Į kibernetinio saugumo planą turėtų būti įtrauktos priimtos kibernetinio saugumo rizikos valdymo priemonės;

(9) kadangi kibernetinio saugumo užtikrinimas yra nuolatinis procesas, turėtų būti reguliariai peržiūrimas visų priemonių, kurių imamasi pagal šį reglamentą, tinkamumas ir veiksmingumas, atsižvelgiant į kintančią Sąjungos subjektams kylančią kibernetinio saugumo riziką, jų kintantį turtą ir kibernetinio saugumo brandą. Sistema turėtų būti reguliariai, bent kas ketverius metus, peržiūrima, o kibernetinio saugumo planas turėtų būti peržiūrimas kas dvejus metus arba, prireikus – dažniau, po kibernetinio saugumo brandos vertinimų ar po bet kokios esminės Sistemos peržiūros;

(10) Sąjungos subjektų įdiegtos kibernetinio saugumo rizikos valdymo priemonės turėtų apimti politiką, kuria siekiama, kai įmanoma, užtikrinti pirminio kodo skaidrumą, atsižvelgiant į trečiųjų šalių arba Sąjungos subjektų teisių apsaugos priemones. Ta politika turėtų būti proporcinga kibernetinio saugumo rizikai ir ja turėtų būti siekiama palengvinti kibernetinių grėsmių analizę, kartu nesukuriant kitų pareigų, nenumatytų taikomose sutarčių sąlygose, atskleisti trečiosios šalies kodą arba suteikti prieigos prie jo teises;

(11) atvirojo kodo kibernetinio saugumo priemonėmis ir taikomosiomis programomis gali būti prisidedama prie didesnio atvirumo. Atviraisiais standartais sudaromos palankesnės sąlygos saugumo priemonių sąveikumui, o tai yra naudinga suinteresuotųjų subjektų saugumo požiūriu. Atvirojo kodo kibernetinio saugumo priemonėmis ir taikomosiomis programomis gali būti daromas sverto poveikis platesnei technologijų kūrėjų bendruomenei, sudarant galimybes tiekėjų diversifikacijai. Atvirasis kodas gali paskatinti skaidresnį su kibernetiniu saugumu susijusių priemonių tikrinimo procesą ir bendruomenės inicijuotą pažeidžiamumų nustatymo procesą. Todėl Sąjungos subjektai turėtų turėti galimybę skatinti atvirojo kodo programinės įrangos ir atviųjų standartų naudojimą, vykdydami politiką, susijusią su atviųjų duomenų ir atvirojo kodo naudojimu, kad skaidrumu būtų prisidėta prie saugumo užtikrinimo;

([2]) 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva) (OL L 333, 2022 12 27, p. 80).

(12) dėl Sąjungos subjektų skirtumų šio reglamento įgyvendinimo srityje reikia lankstumo. Šiame reglamente numatytos priemonės aukštam bendram kibernetinio saugumo lygiui užtikrinti neturėtų apimti jokių pareigų, kuriomis būtų tiesiogiai kišamasi į Sąjungos subjektų užduočių vykdymą arba kėsinamasi į jų institucinį savarankiškumą. Todėl tie subjektai turėtų sukurti savo Sistemas ir patvirtinti savo kibernetinio saugumo rizikos valdymo priemones ir kibernetinio saugumo planus. Įgyvendinant tokias priemones turėtų būti tinkamai atsižvelgiama į esamas Sąjungos subjektų tarpusavio sinergijas, kad būtų tinkamai valdomi ištekliai ir optimizuotos išlaidos. Taip pat reikėtų tinkamai atsižvelgti į tai, kad priemonės nedarytų neigiamo poveikio veiksmingam keitimuisi informacija ir bendradarbiavimui tarp Sąjungos subjektų ir tarp Sąjungos subjektų ir analogiškų valstybių narių subjektų;

(13) siekiant optimizuoti išteklių naudojimą, šiame reglamente turėtų būti numatyta galimybė dviem ar daugiau panašią struktūrą turinčių Sąjungos subjektų bendradarbiauti atliekant savo atitinkamų subjektų kibernetinio saugumo brandos vertinimus;

(14) siekiant neužkrauti Sąjungos subjektams neproporcingos finansinės ir administracinės naštos, kibernetinio saugumo rizikos valdymo reikalavimai turėtų būti proporcingi kibernetinio saugumo rizikai, kuri kyla atitinkamai tinklų ir informacinei sistemai, atsižvelgiant į tokių priemonių modernumą. Kiekvienas Sąjungos subjektas turėtų siekti skirti tinkamą savo IRT biudžeto procentinę dalį siekiant padidinti savo kibernetinio saugumo lygį. Ilguoju laikotarpiu tam turėtų būti siekiama orientacinio tikslo skirti bent 10 proc. IRT biudžeto. Kibernetinio saugumo brandos vertinime turėtų būti įvertinta, ar Sąjungos subjekto išlaidos kibernetiniam saugumui yra proporcingos jo patiriamai kibernetinio saugumo rizikai. Nedarant poveikio taisyklėms, susijusioms su Sąjungos metiniu biudžetu pagal Sutartis, pasiūlyme dėl pirmojo metinio biudžeto, kuris turi būti priimtas po šio reglamento įsigaliojimo, Komisija, vertindama Sąjungos subjektų biudžeto ir personalo poreikius, susijusius su jų išlaidų sąmatomis, turėtų atsižvelgti į iš šio reglamento kylančias pareigas;

(15) siekiant užtikrinti aukštą bendrą kibernetinio saugumo lygį kibernetinį saugumą turi prižiūrėti kiekvieno Sąjungos subjekto aukščiausias valdymo lygmuo. Sąjungos subjekto aukščiausio lygmens vadovybė turėtų būti atsakinga už šio reglamento įgyvendinimą, be kita ko, už Sistemos sukūrimą, kibernetinio saugumo rizikos valdymo priemonių taikymą ir kibernetinio saugumo plano patvirtinimą. Kibernetinio saugumo kultūra, t. y. kasdienė kibernetinio saugumo praktika, yra neatsiejama Sistemos ir atitinkamų kibernetinio saugumo rizikos valdymo priemonių visuose Sąjungos subjektuose dalis;

(16) yra itin svarbu užtikrinti tinklų ir informacinių sistemų, kuriose tvarkoma ES įslaptinta informacija (ESĮI), saugumą. ESĮI tvarkantys Sąjungos subjektai privalo taikyti nustatytas išsamias tokios informacijos apsaugos reguliavimo sistemas, įskaitant konkretų valdymą, politiką ir rizikos valdymo procedūras. Būtina, kad tinklų ir informacinės sistemos, kuriose tvarkoma ESĮI, atitiktų griežtesnius saugumo standartus nei neįslaptintų tinklų ir informacinių sistemų standartai. Taigi, tinklų ir informacinės sistemos, kuriose tvarkoma ESĮI, yra atsparesnės kibernetinėms grėsmėms ir incidentams. Todėl, pripažįstant, kad šiuo atžvilgiu reikia bendros sistemos, šis reglamentas neturėtų būti taikomas tinklų ir informacinėms sistemoms, kuriose tvarkoma ESĮI. Tačiau, jei to aiškiai paprašo Sąjungos subjektas, ES institucijų, įstaigų ir agentūrų kompiuterinių incidentų tyrimo tarnyba (CERT-EU) turėtų galėti teikti pagalbą tam Sąjungos subjektui dėl incidentų įslaptintoje IRT aplinkoje.

(17) Sąjungos subjektai turėtų įvertinti kibernetinio saugumo riziką, susijusią su santykiais su tiekėjais ir paslaugų teikėjais, įskaitant duomenų saugojimo ir tvarkymo paslaugų teikėjus arba valdomas saugumo paslaugas, ir imtis tinkamų priemonių jai sumažinti. Kibernetinio saugumo priemonės turėtų būti išsamiau išdėstytos CERT-EU parengtose gairėse arba rekomendacijose. Nustatant priemones ir gaires reikėtų tinkamai atsižvelgti į moderniausius ir, kai taikytina, aktualius Europos ir tarptautinius standartus, taip pat atitinkamus Sąjungos teisės aktus ir politiką, įskaitant Bendradarbiavimo grupės, įsteigtos pagal Direktyvos (ES) 2022/2555 14 straipsnį, pateiktus rizikos vertinimus ir rekomendacijas, pavyzdžiui, ES suderintą rizikos 5G tinklų kibernetiniam saugumui vertinimą ir ES 5G kibernetinio saugumo priemonių rinkinį. Be to, atsižvelgiant į grėsmių kibernetiniam saugumui padėtį ir tai,

kaip svarbu didinti Sąjungos subjektų kibernetinį atsparumą, pagal konkrečias Europos kibernetinio saugumo sertifikavimo schemas, priimtas pagal Europos Parlamento ir Tarybos reglamento (ES) 2019/881 ([3]) 49 straipsnį, galėtų būti reikalaujama sertifikuoti atitinkamus IRT produktus, IRT paslaugas ir IRT procesus;

(18) 2011 m. gegužės mėn. Sąjungos institucijų ir įstaigų generaliniai sekretoriai nusprendė įsteigti CERT-EU, kurią prižiūri tarpinstitucinė valdančioji taryba. 2012 m. liepos mėn. generaliniai sekretoriai patvirtino praktinę tvarką ir sutarė išlaikyti CERT-EU kaip nuolatinį subjektą, kuris toliau padėtų gerinti bendrą Sąjungos institucijų, įstaigų ir agentūrų informacinių technologijų saugumo lygį, kaip matomo tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje pavyzdį. 2012 m. rugsėjo mėn. CERT-EU buvo įsteigta kaip Komisijos darbo grupė, kuriai suteikti tarpinstituciniai įgaliojimai. 2017 m. gruodžio mėn. Sąjungos institucijos ir įstaigos sudarė tarpinstitucinį susitarimą dėl CERT-EU organizavimo ir veiklos ([4]). Šiuo reglamentu turėtų būti nustatytos išsamios taisyklės dėl CERT-EU darbo organizavimo, veikimo ir valdymo. Šio reglamento nuostatos yra viršesnės už 2017 m. gruodžio mėn. sudaryto Tarpinstitucinio susitarimo dėl CERT-EU darbo organizavimo ir veiklos nuostatas;

(19) CERT-EU turėtų būti pervadinta į Sąjungos institucijų, įstaigų, organų ir agentūrų kibernetinio saugumo tarnybą, tačiau dėl pavadinimo atpažinimo turėtų būti paliktas trumpasis pavadinimas CERT-EU;

(20) be to, kad CERT-EU pavedama daugiau užduočių ir išplečiamas jos vaidmuo, šiuo reglamentu įsteigiama Tarpinstitucinė kibernetinio saugumo taryba (toliau – TKST), siekiant sudaryti palankesnes sąlygas aukštam bendram Sąjungos subjektų kibernetinio saugumo lygiui užtikrinti. TKST turėtų būti suteiktas išskirtinis vaidmuo stebint, kaip Sąjungos subjektai įgyvendina šį reglamentą, padedant jiems jį įgyvendinti ir prižiūrint, kaip įgyvendinami bendrieji CERT-EU prioritetai ir tikslai, bei numatant CERT-EU strateginę kryptį. Todėl TKST turėtų užtikrinti atstovavimą Sąjungos institucijoms ir į ją turėtų būti įtraukta Sąjungos įstaigų, organų ir agentūrų atstovų, vykdančių veiklą per ES agentūrų tinklą. TKST veiklos organizavimas ir veikimas turėtų būti išsamiau reglamentuojami jos vidaus darbo tvarkos taisyklėmis, kurios gali apimti išsamesnį reguliarių TKST posėdžių, įskaitant metinius politinio lygmens susirinkimus, kuriuose kiekvieno TKST nario aukščiausio valdymo lygmens atstovai sudarytų sąlygas TKST surengti strategines diskusijas ir teikti strategines gaires TKST, apibūdinimą. Be to, TKST turėtų galėti įsteigti vykdomąjį komitetą, kuris padėtų jai atlikti savo darbą, ir deleguoti jam kai kurias savo užduotis ir įgaliojimus, visų pirma užduotis, kurioms atlikti reikia specialių jo narių ekspertinių žinių, pavyzdžiui, paslaugų katalogo ir visų vėlesnių jo atnaujinimų patvirtinimą, susitarimų dėl paslaugų lygio sąlygų patvirtinimą, Sąjungos subjektų TKST pagal šį reglamentą pateiktų dokumentų ir ataskaitų vertinimą, arba užduotis, susijusias su sprendimų dėl TKST patvirtintų atitikties užtikrinimo priemonių rengimu ir jų įgyvendinimo stebėsena. TKST turėtų nustatyti vykdomojo komiteto darbo tvarkos taisykles, įskaitant jo užduotis bei įgaliojimus;

(21) TKST tikslas – padėti Sąjungos subjektams pagerinti atitinkamą savo kibernetinio saugumo padėtį įgyvendinant šį reglamentą. Siekdama padėti Sąjungos subjektams, TKST turėtų teikti rekomendacijas CERT-EU vadovui, priimti daugiametę strategiją dėl Sąjungos subjektų kibernetinio saugumo lygio didinimo, nustatyti savanoriškų tarpusavio vertinimų metodiką ir kitus jų aspektus ir sudaryti palankesnes sąlygas įsteigti neformalią vietos kibernetinio saugumo pareigūnų grupę, kuriai padėtų Europos Sąjungos kibernetinio saugumo agentūra (ENISA) ir kurios tikslas būtų keistis geriausios praktikos pavyzdžiais ir informacija, susijusiais su šio reglamento įgyvendinimu;

([3]) 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15).

([4]) Parlamento, Europos Vadovų Tarybos, Europos Sąjungos Tarybos, Europos Komisijos, Europos Sąjungos Teisingumo Teismo, Europos Centrinio Banko, Europos Audito Rūmų, Europos išorės veiksmų tarnybos, Europos ekonomikos ir socialinių reikalų komiteto, Europos regionų komiteto ir Europos investicijų banko tarpinstitucinis susitarimas dėl Sąjungos institucijų, įstaigų ir agentūrų Kompiuterinių incidentų tyrimo tarnybos (CERT-EU) darbo organizavimo ir veiklos (OL C 12, 2018 1 13, p. 1).

(22) siekiant užtikrinti aukštą visų Sąjungos subjektų kibernetinio saugumo lygį, savo IRT aplinką valdančių Sąjungos įstaigų, organų ir agentūrų interesams TKST turėtų atstovauti trys ES agentūrų tinklo paskirti atstovai. Asmens duomenų tvarkymo saugumas, taigi ir jo kibernetinis saugumas, yra duomenų apsaugos kertinis akmuo. Atsižvelgiant į duomenų apsaugos ir kibernetinio saugumo sinergiją, Europos duomenų apsaugos priežiūros pareigūnui turėtų būti atstovaujama TKST kaip Sąjungos subjektui, kuriam taikomas šis reglamentas ir kuris turi specialių ekspertinių žinių duomenų apsaugos srityje, įskaitant elektroninių ryšių tinklų saugumą. Atsižvelgiant į inovacijų ir konkurencingumo svarbą kibernetinio saugumo srityje, Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrui turėtų būti atstovaujama TKST. Atsižvelgiant į ENISA, kaip ekspertinių žinių kibernetinio saugumo srityje centro, vaidmenį ir ENISA teikiamą paramą, taip pat į Sąjungos kosmoso infrastruktūros ir paslaugų kibernetinio saugumo svarbą, TKST turėtų būti atstovaujama ENISA ir Europos Sąjungos kosmoso programos agentūrai. Atsižvelgiant į CERT-EU pagal šį reglamentą pavestas funkcijas, TKST pirmininkas turėtų pakviesti CERT-EU vadovą į visus TKST posėdžius, išskyrus atvejus, kai TKST aptaria klausimus, tiesiogiai susijusius su CERT-EU vadovu;

(23) TKST turėtų stebėti, kaip laikomasi šio reglamento ir kaip įgyvendinamos gairės ir rekomendacijos bei raginimai imtis veiksmų. TKST techniniais klausimais turėtų padėti jos savo nuožiūra nustatytos sudėties techninės patariamosios grupės. Tos techninės patariamosios grupės prireikus turėtų glaudžiai bendradarbiauti su CERT-EU, Sąjungos subjektais bei kitais atitinkamais suinteresuotaisiais subjektais.

(24) jei TKST nustato, kad Sąjungos subjektas veiksmingai neįgyvendino šio reglamento arba pagal jį priimtų gairių, rekomendacijų ar raginimų imtis veiksmų, TKST turėtų galėti imtis atitikties užtikrinimo priemonių, nedarant poveikio atitinkamo Sąjungos subjekto vidaus procedūrų taikymui. TKST atitikties užtikrinimo priemones turėtų taikyti laipsniškai, kitaip tariant, TKST pirmiausia turėtų priimti mažiausiai griežtą priemonę, t. y. pagrįstą nuomonę ir prireikus priimti vis griežtesnes priemones, kurių paskutinė būtų griežčiausia, t. y. rekomendacija laikinai sustabdyti duomenų srautus į atitinkamą Sąjungos subjektą. Tokia rekomendacija turėtų būti taikoma tik išimtiniais atvejais, kai atitinkamas Sąjungos subjektas padaro ilgalaikius, tyčinius, pakartotinius ar sunkius šio reglamento pažeidimus;

(25) pagrįsta nuomonė yra mažiausiai griežta atitikties užtikrinimo priemonė, kuria šalinamos pastebėtos šio reglamento įgyvendinimo spragos. TKST turėtų galėti imtis tolesnių veiksmų, susijusių su pagrįsta nuomone, pateikdama gaires, kad padėtų Sąjungos subjektui užtikrinti, jog jo Sistema, kibernetinio saugumo rizikos valdymo priemonės, kibernetinio saugumo planas ir pranešimų teikimas atitiktų šį reglamentą, o tada per nustatytą laikotarpį pateikti perspėjimą, kaip pašalinti nustatytus Sąjungos subjekto trūkumus. Jei perspėjime nurodyti trūkumai pakankamai nepašalinami, TKST turėtų galėti pateikti pagrįstą pranešimą;

(26) TKST turėtų galėti rekomenduoti atlikti Sąjungos subjekto auditą. Tuo tikslu Sąjungos subjektas turėtų galėti naudotis savo vidaus audito funkcija. TKST taip pat turėtų galėti prašyti, kad auditą atliktų trečiosios šalies audito tarnyba, įskaitant abipusiai sutartą privačiojo sektoriaus paslaugų teikėją;

(27) išimtiniais atvejais, kai Sąjungos subjektas padaro ilgalaikius, tyčinius, pakartotinius ar sunkius šio reglamento pažeidimus, TKST turėtų galėti kaip kraštutinę priemonę rekomenduoti visoms valstybėms narėms ir Sąjungos subjektams laikinai sustabdyti duomenų srautus į tą Sąjungos subjektą, kuri būtų taikoma tol, kol Sąjungos subjektas nenustos daryti pažeidimo. Tokia rekomendacija turėtų būti perduodama tinkamais ir saugiais ryšių kanalais;

(28) siekiant užtikrinti teisingą šio reglamento įgyvendinimą, TKST, jei mano, kad nuolatinį šio reglamento pažeidimą, kurį daro Sąjungos subjektas, tiesiogiai sukėlė to subjekto darbuotojo, įskaitant aukščiausią valdymo lygmenį, veiksmai ar neveikimas, turėtų prašyti atitinkamo Sąjungos subjekto imtis tinkamų veiksmų, įskaitant prašymą, kad jis apsvarstytų galimybę imtis drausminio pobūdžio veiksmų, laikantis taisyklių ir procedūrų, nustatytų Europos Sąjungos pareigūnų tarnybos nuostatuose ir kitų Sąjungos tarnautojų įdarbinimo sąlygose, nustatytuose Tarybos reglamente (EEB, Euratomas, EAPB) Nr. 259/68 ([5]) (toliau – Tarnybos nuostatai), ir kitų taikytinų taisyklių ir procedūrų;

(29) CERT-EU turėtų prisidėti prie visų Sąjungos subjektų IRT aplinkos saugumo. Svarstydama, ar Sąjungos subjekto prašymu teikti techninės konsultacijas ar informaciją atitinkamais politikos klausimais, CERT-EU turėtų užtikrinti, kad tai jai netrukdytų vykdyti kitų šiuo reglamentu jai pavestų vykdyti užduočių. CERT-EU turėtų veikti Sąjungos subjektų vardu kaip koordinatoriaus, paskirto koordinuoto pažeidžiamumų atskleidimo tikslais pagal Direktyvos (ES) 2022/2555 12 straipsnio 1 dalį, atitikmuo;

(30) CERT-EU turėtų padėti įgyvendinti priemones, skirtas aukštam bendram kibernetinio saugumo lygiui užtikrinti, teikdama pasiūlymus dėl gairių ir rekomendacijų TKST arba skelbdama raginimus imtis veiksmų. Tokias gaires ir rekomendacijas turėtų tvirtinti TKST. Prireikus CERT-EU turėtų priimti raginimus imtis veiksmų, kuriuose aprašomos skubios saugumo priemonės, kurių Sąjungos subjektai raginami imtis per nustatytą laikotarpį. TKST turėtų nurodyti CERT-EU paskelbti, atsiimti arba pakeisti pasiūlymą dėl gairių, rekomendacijos arba kvietimo imtis veiksmų;

(31) CERT-EU taip pat turėtų atlikti Direktyvoje (ES) 2022/2555 numatytą vaidmenį, susijusį su bendradarbiavimu ir keitimusi informacija su reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) tinklu, įsteigtu pagal tos direktyvos 15 straipsnį. Be to, pagal Komisijos rekomendaciją (ES) 2017/1584 ([6]) CERT-EU turėtų bendradarbiauti ir koordinuoti reagavimo veiksmus su atitinkamais suinteresuotaisiais subjektais. Siekdama prisidėti prie aukšto kibernetinio saugumo lygio visoje Sąjungoje, CERT-EU turėtų dalytis su incidentais susijusia informacija su analogiškais valstybių narių centrais. Gavusi išankstinį TKST pritarimą CERT-EU taip pat turėtų bendradarbiauti su kitais viešaisiais ir privačiaisiais partneriais, įskaitant Šiaurės Atlanto sutarties organizaciją;

(32) siekdama remti operatyvinį kibernetinį saugumą CERT-EU turėtų pasinaudoti ENISA ekspertinėmis žiniomis, vykdydama Reglamente (ES) 2019/881 numatytą struktūrinį bendradarbiavimą. Kai tinkama, turėtų būti sudaryti specialūs šių dviejų subjektų susitarimai, siekiant nustatyti, kaip toks bendradarbiavimas bus įgyvendinamas praktiškai, ir išvengti veiklos dubliavimo. CERT-EU turėtų bendradarbiauti su ENISA kibernetinių grėsmių analizės srityje ir reguliariai dalytis su ENISA grėsmių padėties ataskaita;

(33) CERT-EU turėtų galėti bendradarbiauti ir keistis informacija su atitinkamomis kibernetinio saugumo bendruomenėmis Sąjungoje ir jos valstybėse narėse, kad būtų skatinamas operatyvinis bendradarbiavimas ir sudarytos sąlygos esamiems tinklams išnaudoti visą savo potencialą apsaugant Sąjungą.

(34) kadangi CERT-EU paslaugos ir užduotys atitinka Sąjungos subjektų interesus, kiekvienas IRT išlaidų turintis Sąjungos subjektas turėtų sąžiningai prisidėti prie tų paslaugų teikimo ir užduočių vykdymo. Tie įnašai nedaro poveikio Sąjungos subjektų biudžetiniam savarankiškumui;

([5]) 1968 m. vasario 29 d. Tarybos reglamentas (EEB, Euratomas, EAPB) Nr. 259/68, nustatantis Europos Bendrijų pareigūnų tarnybos nuostatus ir kitų Europos Bendrijų tarnautojų įdarbinimo sąlygas bei Komisijos pareigūnams laikinai taikomas specialias priemones (OL L 56, 1968 3 4, p. 1).

([6]) 2017 m. rugsėjo 13 d. Komisijos rekomendacija (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes (OL L 239, 2017 9 19, p. 36).

(35) daugelis kibernetinių išpuolių yra platesnių kampanijų, nukreiptų prieš Sąjungos subjektų grupes arba interesų bendruomenes, įskaitant Sąjungos subjektus, dalis. Kad būtų galima imtis aktyvaus atskleidimo, reagavimo į incidentus, rizikos mažinimo priemonių ir veiklos atstatymo po incidentų, Sąjungos subjektai turėtų galėti pranešti CERT-EU apie incidentus, kibernetines grėsmes ir vos neįvykusius incidentus ir dalytis tinkama technine informacija, kad būtų galima atskleisti arba sumažinti panašius incidentus, kibernetines grėsmes, pažeidžiamumą ir vos neįvykusius incidentus kituose Sąjungos subjektuose ir į juos reaguoti. Vadovaujantis tokiu pačiu požiūriu, koks yra nustatytas Direktyvoje (ES) 2022/2555, Sąjungos subjektai turėtų privalėti per 24 valandas nuo tada, kai sužinojo apie reikšmingą incidentą, pateikti ankstyvąjį perspėjimą CERT-EU. Toks keitimasis informacija turėtų sudaryti sąlygas CERT-EU skleisti informaciją kitiems Sąjungos subjektams, taip pat atitinkamiems analogiškiems partneriams, siekiant padėti apsaugoti Sąjungos subjektų IRT aplinką ir Sąjungos subjektų analogiškų partnerių IRT aplinką nuo panašių incidentų;

(36) šiuo reglamentu nustatomas kelių etapų pranešimų apie reikšmingus incidentus teikimo metodas, siekiant užtikrinti tinkamą pusiausvyrą tarp, viena vertus, greito pranešimų teikimo, kuris padeda sumažinti galimą reikšmingų incidentų plitimą ir suteikia galimybę Sąjungos subjektams prašyti pagalbos, ir, kita vertus, išsamių pranešimų, kuriuose atsižvelgiama į vertingą su pavieniais incidentais susijusią patirtį ir kuriais ilgainiui didinamas atskirų Sąjungos subjektų kibernetinis atsparumas bei prisidedama prie bendros jų kibernetinio saugumo būklės gerinimo. Tuo atžvilgiu į šį reglamentą turėtų būti įtraukti pranešimai apie incidentus, kurie, remiantis atitinkamo Sąjungos subjekto atliktu pradiniu vertinimu, galėtų sukelti didelių veikimo sutrikdymų arba padaryti finansinių nuostolių atitinkamam Sąjungos subjektui, arba padaryti poveikį kitiems fiziniams ar juridiniams asmenims, sukeldami didelę turtinę ar neturtinę žalą. Atliekant tokį pradinį vertinimą turėtų būti atsižvelgiama, *inter alia*, į paveiktas tinklų ir informacines sistemas, visų pirma į jų svarbą Sąjungos subjekto veikimui, kibernetinės grėsmės rimtumą bei technines charakteristikas ir bet kokį pagrindinį pažeidžiamumą, kuriuo pasinaudojama, taip pat į Sąjungos subjekto patirtį, įgytą panašių incidentų metu. Nustatant, ar veiklos sutrikdymas yra didelis, svarbus vaidmuo galėtų tekti tokiems rodikliams kaip poveikio Sąjungos subjekto veikimui mastas, incidento trukmė arba paveiktų fizinių ar juridinių asmenų skaičius;

(37) kadangi atitinkamo Sąjungos subjekto ir valstybės narės, kurioje yra tas Sąjungos subjektas, infrastruktūra ir tinklų ir informacinės sistemos yra tarpusavyje susijusios, labai svarbu, kad ta valstybė narė būtų nepagrįstai nedelsiant informuojama apie reikšmingą incidentą tame Sąjungos subjekte. Tuo tikslu paveiktas Sąjungos subjektas apie įvykusį reikšmingą incidentą, apie kurį jis praneša CERT-EU, turėtų informuoti visus atitinkamus analogiškus valstybių narių subjektus, paskirtus ar įsteigtus pagal Direktyvos (ES) 2022/2555 8 ir 10 straipsnius. Kai CERT-EU sužino apie reikšmingą incidentą, vykstantį valstybėje narėje, ji apie tą reikšmingą incidentą turėtų pranešti visiems atitinkamiems analogiškiems tos valstybės narės centrams;

(38) turėtų būti įgyvendintas mechanizmas, kuriuo būtų užtikrinamas veiksmingas Sąjungos subjektų keitimasis informacija, veiksmų koordinavimas ir bendradarbiavimas didelių incidentų atveju, įskaitant aiškų susijusių Sąjungos subjektų funkcijų ir pareigų nustatymą. Siekiant palengvinti TKST keitimąsi svarbia informacija su Europos ryšių palaikymo dėl kibernetinių krizių organizaciniu tinklu (EU-CyCLONe), susijusia su dideliais incidentais, kontaktinis asmuo, laikantis kibernetinių krizių valdymo plano, turėtų būti Komisijos atstovas TKST, taip prisidedant prie bendro informuotumo apie esamą padėtį. Komisijos atstovo TKST, kaip kontaktinio asmens, vaidmuo neturėtų daryti poveikio atskiram ir konkrečiam Komisijos vaidmeniui, kurį jis atlieka EU-CyCLONe pagal Direktyvos (ES) 2022/2555 16 straipsnio 2 dalį;

(39) tvarkant asmens duomenis pagal šį reglamentą, taikomas Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 ([7]). Asmens duomenys galėtų būti tvarkomi įgyvendinant priemones, priimtas kibernetinio saugumo rizikos valdymo, pažeidžiamumų ir incidentų valdymo, dalijimosi informacija apie incidentus, kibernetines grėsmes ir pažeidžiamumą, taip pat reagavimo į incidentus koordinavimo ir bendradarbiavimo srityse. Dėl tokių priemonių galėtų prireikti tvarkyti tam tikrų kategorijų asmens duomenis, pavyzdžiui, IP adresus, universaliuosius išteklių adresus (URL), domenų vardus, e. pašto adresus, duomenų subjekto organizacinius vaidmenis, laiko žymas, e. pašto laiškų temas arba rinkmenų pavadinimus. Visos priemonės, kurių imamasi pagal šį

([7]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39).

reglamentą, turėtų atitikti duomenų apsaugos ir privatumo sistemą, o Sąjungos subjektai, CERT-EU ir, kai aktualu, TKST turėtų imtis visų atitinkamų techninių ir organizacinių apsaugos priemonių, kad atskaitingai užtikrintų tokį reikalavimų laikymąsi;

(40) šiuo reglamentu nustatomas Sąjungos subjektų, CERT-EU ir, kai aktualu, TKST atliekamo asmens duomenų tvarkymo pagal Reglamento (ES) 2018/1725 5 straipsnio 1 dalies b punktą jų užduočių ir pareigų pagal šį reglamentą vykdymo tikslais teisinis pagrindas. CERT-EU gali veikti kaip duomenų tvarkytoja arba duomenų valdytoja, priklausomai nuo užduočių, kurias ji atlieka pagal Reglamentą (ES) 2018/1725.

(41) tam tikrais atvejais, savo pareigų pagal šį reglamentą užtikrinti aukštą kibernetinio saugumo lygį vykdymo tikslais, visų pirma pažeidžiamumo ir incidentų valdymo kontekste, Sąjungos subjektams ir CERT-EU gali prireikti tvarkyti specialių kategorijų asmens duomenis, kaip nurodyta Reglamento (ES) 2018/1725 10 straipsnio 1 dalyje. Šiuo reglamentu nustatomas Sąjungos subjektų ir CERT-EU atliekamo specialių kategorijų asmens duomenų tvarkymo pagal Reglamento (ES) 2018/1725 10 straipsnio 2 dalies g punktą teisinis pagrindas. Specialių kategorijų asmens duomenų tvarkymas pagal šį reglamentą turėtų būti griežtai proporcingas siekiamam tikslui. Laikantis to reglamento 10 straipsnio 2 dalies g punkte nustatytų sąlygų, Sąjungos subjektai ir CERT-EU turėtų galėti tvarkyti tokius duomenis tik tiek, kiek tai būtina ir kai tai aiškiai numatyta šiame reglamente. Tvarkydami specialių kategorijų asmens duomenis Sąjungos subjektai ir CERT-EU turėtų paisyti esminių teisės į duomenų apsaugą nuostatų ir numatyti tinkamas ir konkrečias priemones asmenų pagrindinėms teisėms ir interesams apsaugoti;

(42) pagal Reglamento (ES) 2018/1725 33 straipsnį Sąjungos subjektai ir CERT-EU, atsižvelgdami į naujausias technologijas, įgyvendinimo sąnaudas ir duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat į įvairios tikimybės ir sunkumo riziką, kylančią fizinių asmenų teisėms ir laisvėms, turėtų įgyvendinti tinkamas technines ir organizacines priemones, kad užtikrintų tinkamo lygmens asmens duomenų apsaugą, pavyzdžiui, ribotų prieigos teisių suteikimą vadovaujantis principu „būtina žinoti“, taikytų audito sekos principus, naudotų duomenų saugojimo grandinę, nenaudojamus duomenis saugotų kontroliuojamoje ir patikrinamoje aplinkoje, taikytų standartizuotas veiklos procedūras ir privatumo apsaugos priemones, pavyzdžiui, pseudoniminimą ar šifravimą. Tos priemonės neturėtų būti įgyvendinamos taip, kad būtų daromas poveikis incidentų valdymo ir įrodymų vientisumo tikslų įgyvendinimui. Kai Sąjungos subjektas arba CERT-EU perduoda su incidentu susijusius asmens duomenis, įskaitant specialių kategorijų asmens duomenis, analogiškam subjektui arba partneriui šio reglamento tikslais, vykdant tokį perdavimą turėtų būti laikomasi Reglamento (ES) 2018/1725. Kai specialių kategorijų asmens duomenys perduodami trečiajai šaliai, Sąjungos subjektai ir CERT-EU turėtų užtikrinti, kad trečioji šalis taikytų asmens duomenų apsaugos priemones, kurių lygmuo būtų lygiavertis priemonių pagal Reglamentą (ES) 2018/1725 lygmeniui;

(43) šio reglamento tikslais tvarkomi asmens duomenys turėtų būti saugomi tik tiek laiko, kiek tai būtina pagal Reglamentą (ES) 2018/1725. Sąjungos subjektai ir, kai taikytina, CERT-EU, veikdami kaip duomenų valdytojai, turėtų nustatyti saugojimo laikotarpius, kurie neviršija to, kas būtina nurodytiems tikslams pasiekti. Visų pirma, kiek tai susiję su incidentų valdymo tikslais surinktais asmens duomenimis, Sąjungos subjektai ir CERT-EU turėtų atskirti asmens duomenis, kurie renkami siekiant nustatyti kibernetinę grėsmę jų IRT aplinkoje, kad būtų užkirstas kelias incidentui, ir asmens duomenis, kurie renkami incidento padarinių švelninimo, reagavimo į jį ir veiklos atstatymo įvykus incidentui tikslais. Nustatant kibernetinę grėsmę svarbu atsižvelgti į tai, kiek laiko grėsmę keliantis subjektas gali likti sistemoje neaptiktas. Švelninant incidento padarinius, į jį reaguojant ir atstatant veiklą įvykus incidentui svarbu apsvarstyti, ar asmens duomenys yra būtini pasikartojančiam incidentui ar panašaus pobūdžio incidentui, dėl kurio būtų galima įrodyti egzistuojančią koreliaciją, atsekti ir valdyti;

(44) CERT-EU ir Sąjungos subjektai informaciją turėtų tvarkyti pagal taikomas taisykles dėl informacijos saugumo. Žmogiškųjų išteklių saugumo įtraukimas į kibernetinio saugumo rizikos valdymo priemonę taip pat turėtų atitikti taikytinas taisykles.

(45) dalijimosi informacija tikslais matomomis žymomis nurodoma, kad informacijos gavėjai turi dalytis informacija laikydamiesi tam tikrų ribų, visų pirma remdamiesi informacijos neatskleidimo susitarimais arba neoficialiais informacijos neatskleidimo susitarimais, pavyzdžiui, srauto kontrolės protokolu arba kitais aiškiais šaltinio nurodymais. Srauto kontrolės protokolas turi būti suprantamas kaip būdas teikti informaciją kaip priemonė informacijai apie bet kokius apribojimus, taikomus tolesnei informacijos sklaidai, teikti. Jį naudoja beveik visos CSIRT ir kai kurie informacijos analizės ir dalijimosi ja centrai;

(46) šis reglamentas turėtų būti reguliariai vertinamas atsižvelgiant į būsimas derybas dėl daugiamečių finansinių programų, suteikiant galimybę tolesnius sprendimus priimti atsižvelgiant į CERT-EU veikimą ir institucinį vaidmenį, įskaitant galimą CERT-EU, kaip Sąjungos tarnybos, steigimą;

(47) TKST, padedant CERT-EU, turėtų peržiūrėti ir įvertinti šio reglamento įgyvendinimą ir pateikti savo išvadas Komisijai. Remdamasi tuo indėliu Komisija turėtų teikti ataskaitą Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. Toje ataskaitoje, TKST pateikus indėlį, turėtų būti įvertinta, ar tikslinga į šio reglamento taikymo sritį įtraukti tinklų ir informacines sistemas, kuriose tvarkoma ESĮI, visų pirma tais atvejais, kai nėra nustatyta Sąjungos subjektams bendrų informacijos saugumo taisyklių;

(48) vadovaujantis proporcingumo principu ir siekiant pagrindinio tikslo – užtikrinti aukštą bendrą kibernetinio saugumo lygį Sąjungos subjektuose, – būtina ir dera nustatyti kibernetinio saugumo taisykles, taikomas Sąjungos subjektams. Šiuo reglamentu remiantis Europos Sąjungos sutarties 5 straipsnio 4 dalimi neviršijama to, kas būtina nurodytam tikslui pasiekti;

(49) šiame reglamente atsižvelgiama į tai, kad Sąjungos subjektų dydis ir pajėgumai, įskaitant finansinius ir žmogiškuosius išteklius, yra skirtingi;

(50) vadovaujantis Reglamento (ES) 2018/1725 42 straipsnio 1 dalimi buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu, ir jis pateikė nuomonę 2022 m. gegužės 17 d. ([8]),

PRIĖMĖ ŠĮ REGLAMENTĄ:

I SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas

Šiuo reglamentu nustatomos priemonės, kuriomis siekiama užtikrinti aukštą bendrą kibernetinio saugumo lygį Sąjungos subjektuose, dėl:

a) kiekvieno Sąjungos subjekto pagal 6 straipsnį sukuriamos vidaus kibernetinio saugumo rizikos valdymo ir kontrolės sistemos;

b) kibernetinio saugumo rizikos valdymo, pranešimų teikimo ir dalijimosi informacija;

c) pagal 10 straipsnį įsteigtos Tarpinstitucinės kibernetinio saugumo tarybos organizavimo, veikimo ir valdymo ir Sąjungos institucijų, įstaigų, organų ir agentūrų kibernetinio saugumo tarnybos (toliau – CERT-EU) organizavimo, veikimo ir valdymo;

d) šio reglamento įgyvendinimo stebėsenos.

([8]) OL C 258, 2022 7 5, p. 10.

2 straipsnis

Taikymo sritis

1. Šis reglamentas taikomas Sąjungos subjektams, pagal 10 straipsnį įsteigtai Tarpinstitucinei kibernetinio saugumo tarybai ir CERT-EU.

2. Šis reglamentas taikomas nedarant poveikio Sutartyse numatytam instituciniam savarankiškumui.

3. Išskyrus 13 straipsnio 8 dalį, šis reglamentas netaikomas tinklų ir informacinėms sistemoms, kuriose tvarkoma ES įslaptinta informacija (ESĮI).

3 straipsnis

Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1) Sąjungos subjektai – Sąjungos institucijos, įstaigos, organai ir agentūros, įsteigti Europos Sąjungos sutartimi, Sutartimi dėl Europos Sąjungos veikimo (SESV) arba Europos atominės energijos bendrijos steigimo sutartimi arba jomis remiantis;

2) tinklų ir informacinė sistema – tinklų ir informacinė sistema, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 1 punkte;

3) tinklų ir informacinių sistemų saugumas – tinklų ir informacinių sistemų saugumas, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 2 punkte;

4) kibernetinis saugumas – kibernetinis saugumas, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 1 punkte;

5) aukščiausias valdymo lygmuo – už Sąjungos subjekto veikimą atsakingas aukščiausio administracinio lygmens vadovas, valdymo organas arba koordinavimo ir priežiūros organas, įgaliotas priimti arba patvirtinti sprendimus, atitinkančius to Sąjungos subjekto aukšto lygio valdymo tvarką, nedarant poveikio oficialioms kitų valdymo lygmenų pareigoms už atitiktį ir kibernetinio saugumo rizikos valdymą jų atitinkamose atsakomybės srityse;

6) vos neįvykęs incidentas – vos neįvykęs incidentas, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 5 punkte;

7) incidentas – incidentas, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 6 punkte;

8) didelis incidentas – incidentas, į kurio sukeltą sutrikimą Sąjungos subjektas ir CERT-EU nepajėgia reaguoti arba kuris daro didelį poveikį bent dviem Sąjungos subjektams;

9) didelio masto kibernetinio saugumo incidentas – didelio masto kibernetinio saugumo incidentas, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 7 punkte;

10) incidento valdymas – incidento valdymas, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 8 punkte;

11) kibernetinė grėsmė – kibernetinė grėsmė, kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 8 punkte;

12) didelė kibernetinė grėsmė – didelė kibernetinė grėsmė, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 11 punkte;

(13) pažeidžiamumas – pažeidžiamumas, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 15 punkte;

(14) kibernetinio saugumo rizika – rizika, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 9 punkte;

(15) debesijos kompiuterijos paslauga – debesijos kompiuterijos paslauga, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 30 punkte.

4 straipsnis

Asmens duomenų tvarkymas

1. CERT-EU, pagal 10 straipsnį įsteigta Tarpinstitucinė kibernetinio saugumo taryba arba Sąjungos subjektai asmens duomenis pagal šį reglamentą tvarko pagal Reglamentą (ES) 2018/1725.

2. Kai CERT-EU, pagal 10 straipsnį įsteigta Tarpinstitucinė kibernetinio saugumo taryba ir Sąjungos subjektai atlieka užduotis arba vykdo pareigas pagal šį reglamentą, jie asmens duomenis tvarko ir jais keičiasi tik tiek, kiek tai būtina toms užduotims atlikti arba toms pareigoms vykdyti.

3. Specialių kategorijų asmens duomenų tvarkymas, kaip nurodyta Reglamento (ES) 2018/1725 10 straipsnio 1 dalyje, laikomas būtinu dėl svarbių viešojo intereso priežasčių pagal to reglamento 10 straipsnio 2 dalies g punktą. Tokie duomenys gali būti tvarkomi tik tiek, kiek tai būtina šio reglamento 6 ir 8 straipsniuose nurodytoms kibernetinio saugumo rizikos valdymo priemonėms įgyvendinti, CERT-EU paslaugoms teikti pagal šio reglamento 13 straipsnį, dalytis su incidentais susijusia informacija pagal 17 straipsnio 3 dalį ir 18 straipsnio 3 dalį, dalytis informacija pagal 20 straipsnį, vykdyti pareigas pranešti pagal 21 straipsnį, reagavimo į incidentus koordinavimui ir bendradarbiavimui pagal 22 straipsnį ir didelių incidentų valdymui pagal 23 straipsnį. Sąjungos subjektai ir CERT-EU, veikdami kaip duomenų valdytojai, taiko technines priemones, kad užkirstų kelią specialių kategorijų asmens duomenų tvarkymui kitais tikslais, ir numato tinkamas ir konkrečias priemones duomenų subjektų pagrindinėms teisėms ir interesams apsaugoti.

II SKYRIUS

PRIEMONĖS AUKŠTAM BENDRAM KIBERNETINIO SAUGUMO LYGIUI UŽTIKRINTI

5 straipsnis

Priemonių įgyvendinimas

1. Ne vėliau kaip 2024 m. rugsėjo 8 d. pagal 10 straipsnį įsteigta Tarpinstitucinė kibernetinio saugumo taryba, pasikonsultavusi su Europos Sąjungos kibernetinio saugumo agentūra (toliau – ENISA) ir gavusi rekomendacijų iš CERT-EU, pateikia gaires Sąjungos subjektams, kuriomis vadovaujantis būtų galima atlikti pradinę kibernetinio saugumo peržiūrą ir nustatyti vidaus kibernetinio saugumo rizikos valdymo, administravimo ir kontrolės sistemą pagal 6 straipsnį, atlikti kibernetinio saugumo brandos vertinimus pagal 7 straipsnį, imtis kibernetinio saugumo rizikos valdymo priemonių pagal 8 straipsnį ir priimti kibernetinio saugumo planą pagal 9 straipsnį.

2. Įgyvendindami 6–9 straipsnius, Sąjungos subjektai atsižvelgia į šio straipsnio 1 dalyje nurodytas gaires, taip pat į atitinkamas gaires ir rekomendacijas, priimtas pagal 11 ir 14 straipsnius.

6 straipsnis

Kibernetinio saugumo rizikos valdymo, administravimo ir kontrolės sistema

1. Ne vėliau kaip 2025 m. balandžio 8 d.] kiekvienas Sąjungos subjektas, atlikęs pradinę kibernetinio saugumo peržiūrą, pavyzdžiui, auditą, nustato vidaus kibernetinio saugumo rizikos valdymo, administravimo ir kontrolės sistemą (toliau – Sistema). Sistemos sukūrimą prižiūri ir už jį atsako Sąjungos subjekto aukščiausias valdymo lygmuo.

2. Sistema apima visą atitinkamo Sąjungos subjekto neįslaptintą IRT aplinką, įskaitant bet kokias vietoje esančias IRT aplinką, operacinį technologijų tinklą, užsakomąjį turtą ir paslaugas debesijos kompiuterijos aplinkoje arba kurių prieglobą teikia trečiosios šalys, mobiliuosius įrenginius, įmonių tinklus, prie interneto neprijungtus verslo tinklus ir bet kokius su tomis aplinkomis susijusius įrenginius (toliau – IRT aplinka). Sistema grindžiama visus pavojus apimančiu požiūriu.

3. Sistema užtikrinamas aukštas kibernetinio saugumo lygis. Sistemoje nustatoma tinklų ir informacinių sistemų saugumo vidaus kibernetinio saugumo politika, įskaitant tikslus ir prioritetus, taip pat Sąjungos subjekto darbuotojų, kuriems pavesta užtikrinti, kad šis reglamentas būtų veiksmingai įgyvendinamas, funkcijos ir pareigos. Į Sistemą taip pat įtraukiami įgyvendinimo veiksmingumo vertinimo mechanizmai.

4. Sistema turėtų būti reguliariai peržiūrima atsižvelgiant į kintančią kibernetinio saugumo riziką ir ne rečiau kaip kas ketverius metus. Kai tinkama ir gavus pagal 10 straipsnį įsteigtos Tarpinstitucinės kibernetinio saugumo tarybos prašymą, Sąjungos subjekto Sistema gali būti atnaujinama remiantis CERT-EU rekomendacijomis dėl nustatytų incidentų ar galimų spragų, pastebėtų įgyvendinant šį reglamentą.

5. Kiekvieno Sąjungos subjekto aukščiausias valdymo lygmuo yra atsakingas už šio reglamento įgyvendinimą ir prižiūri, kaip jo organizacija laikosi su Sistema susijusių pareigų.

6. Kiekvieno Sąjungos subjekto aukščiausias valdymo lygmuo, kai tikslinga ir nedarant poveikio jo atsakomybei už šio reglamento įgyvendinimą, gali konkrečias pareigas pagal šį reglamentą deleguoti atitinkamo Sąjungos subjekto vyresniesiems pareigūnams, kaip tai suprantama Tarnybos nuostatų 29 straipsnio 2 dalyje, arba kitiems lygiaverčio lygmens pareigūnams. Neatsižvelgiant į tokį pareigų delegavimą, aukščiausias valdymo lygmuo gali būti laikomas atsakingu už atitinkamo Sąjungos subjekto padarytus šio reglamento pažeidimus.

7. Kiekvienas Sąjungos subjektas turi turėti veiksmingus mechanizmus, kuriais užtikrinama, kad kibernetiniam saugumui būtų išleidžiama tinkama IRT biudžeto lėšų procentinė dalis. Nustatant tą procentinę dalį tinkamai atsižvelgiama į Sistemą.

8. Kiekvienas Sąjungos subjektas paskiria vietos kibernetinio saugumo pareigūną arba lygiavertę funkciją atliekantį pareigūną, kuris visais kibernetinio saugumo aspektais veikia kaip vienas kontaktinis punktas. Vietos kibernetinio saugumo pareigūnas sudaro palankias sąlygas įgyvendinti šį reglamentą ir aukščiausiam valdymo lygmeniui reguliariai tiesiogiai teikia ataskaitas apie įgyvendinimo padėtį. Nedarant poveikio tam, kad vietos kibernetinio saugumo pareigūnas veikia kaip vienas kontaktinis punktas kiekviename Sąjungos subjekte, Sąjungos subjektas gali CERT-EU deleguoti tam tikras vietos kibernetinio saugumo pareigūno užduotis, susijusias su šio reglamento įgyvendinimu, remdamasis to Sąjungos subjekto ir CERT-EU sudarytu susitarimu dėl paslaugų lygio, arba tas užduotis gali dalytis keli Sąjungos subjektai. Kai tos užduotys deleguojamos CERT-EU, pagal 10 straipsnį įsteigta Tarpinstitucinė kibernetinio saugumo taryba, atsižvelgdama į atitinkamo Sąjungos subjekto žmogiškuosius ir finansinius išteklius, nusprendžia, ar tos paslaugos turi būti teikiamos kaip CERT-EU pagrindinių paslaugų dalis. Kiekvienas Sąjungos subjektas nepagrįstai nedelsdamas praneša CERT-EU apie paskirtą vietos kibernetinio saugumo pareigūną ir apie visus vėlesnius jo pakeitimus.

CERT-EU nuolat parengia ir nuolat atnaujina paskirtų vietos kibernetinio saugumo pareigūnų sąrašą.

9. Kiekvieno Sąjungos subjekto vyresnieji pareigūnai, kaip tai suprantama Tarnybos nuostatų 29 straipsnio 2 dalyje, arba lygiaverčio lygmens pareigūnai, taip pat visi atitinkami darbuotojai, kuriems pavesta įgyvendinti kibernetinio saugumo rizikos valdymo priemones ir vykdyti šiame reglamente nustatytas pareigas, reguliariai dalyvauja specialiuose mokymuose, kad įgytų pakankamai žinių ir įgūdžių, kurių reikia siekiant suprasti ir įvertinti kibernetinio saugumo riziką ir su ja susijusią valdymo praktiką bei jos poveikį Sąjungos subjekto veiklai.

7 straipsnis

Kibernetinio saugumo brandos vertinimai

1. Ne vėliau kaip 2025 m. liepos 8 d., o vėliau – bent kas dvejus metus kiekvienas Sąjungos subjektas atlieka kibernetinio saugumo brandos vertinimą, apimantį visus jo IRT aplinkos elementus.

2. Kai tinkama, kibernetinio saugumo brandos vertinimai atliekami padedant specializuotai trečiajai šaliai.

3. Panašias struktūras turintys Sąjungos subjektai gali bendradarbiauti atlikdami savo atitinkamų subjektų kibernetinio saugumo brandos vertinimus.

4. Remiantis pagal 10 straipsnį įsteigtos Tarpinstitucinės kibernetinio saugumo tarybos prašymu ir gavus aiškų atitinkamo Sąjungos subjekto sutikimą, kibernetinio saugumo brandos vertinimo rezultatai gali būti aptarti toje taryboje arba neoficialioje vietos kibernetinio saugumo pareigūnų grupėje, siekiant mokytis iš patirties ir dalytis geriausios praktikos pavyzdžiais.

8 straipsnis

Kibernetinio saugumo rizikos valdymo priemonės

1. Kiekvienas Sąjungos subjektas, prižiūrimas jo aukščiausio valdymo lygmens, nepagrįstai nedelsdamas ir bet kuriuo atveju ne vėliau kaip 2025 m. rugsėjo 8 d. imasi tinkamų ir proporcingų techninių, operacinių ir organizacinių priemonių, kuriomis valdoma pagal Sistemą nustatyta kibernetinio saugumo rizika ir užkertamas kelias incidentams arba kuo labiau sumažinamas incidentų poveikis. Atsižvelgiant į naujausias technologijas ir, kai taikoma, atitinkamus Europos ir tarptautinius standartus, tomis priemonėmis užtikrinamas tinklų ir informacinių sistemų saugumo lygis visoje IRT aplinkoje, proporcingas kylančiai kibernetinio saugumo rizikai. Vertinant tų priemonių proporcingumą, tinkamai atsižvelgiama į Sąjungos subjekto patiriamos kibernetinio saugumo rizikos laipsnį, jo dydį ir incidentų tikimybę ir jų sunkumą, įskaitant jų poveikį visuomenei, ekonomikai ir tarpinstitucinį poveikį.

2. Sąjungos subjektai, įgyvendindami kibernetinio saugumo rizikos valdymo priemones, imasi priemonių bent šiose konkrečiose srityse:

a) kibernetinio saugumo politikos, įskaitant priemones, būtinas 6 straipsnyje ir šio straipsnio 3 dalyje nurodytiems tikslams ir prioritetams pasiekti;

b) kibernetinio saugumo rizikos analizės ir informacinių sistemų saugumo politikos;

c) politikos tikslų, susijusių su debesijos kompiuterijos paslaugų naudojimu;

d) kai tinkama, kibernetinio saugumo audito, kuris gali apimti kibernetinio saugumo rizikos, pažeidžiamumo ir kibernetinių grėsmių vertinimą ir skverbimosi testavimą, kurį reguliariai atlieka patikimas privatus paslaugų teikėjas;

e) rekomendacijų, pateiktų atlikus d punkte nurodytus kibernetinio saugumo auditus, įgyvendinimo pasitelkiant kibernetinio saugumo priemones ir politikos atnaujinimus;

f) kibernetinio saugumo organizavimo, įskaitant funkcijų ir pareigų nustatymą;

g) turto valdymo, įskaitant IRT turto aprašo ir IRT tinklo kartografijos sudarymą;

h) žmogiškųjų išteklių saugumo ir prieigos kontrolės;

i) operacijų saugumo;

j) ryšių saugumo;

k) sistemos įsigijimo, plėtojimo ir techninės priežiūros, įskaitant pažeidžiamumo valdymo ir atskleidimo politiką;

l) kai įmanoma, pirminio kodo skaidrumo politikos;

m) tiekimo grandinės saugumo, įskaitant su saugumu susijusius aspektus, susijusius su kiekvieno Sąjungos subjekto ir jo tiesioginių tiekėjų ar paslaugų teikėjų santykiais;

n) incidentų valdymo ir bendradarbiavimo su CERT-EU, pvz., saugumo stebėsenos ir registravimo užtikrinimo;

o) veiklos tęstinumo valdymo, pvz., atsarginių kopijų valdymo ir veiklos atkūrimo po ekstremaliųjų įvykių, taip pat krizių valdymo; ir

p) švietimo, įgūdžių, informuotumo didinimo, pratybų ir mokymo programų kibernetinio saugumo srityje skatinimo ir plėtojimo.

Pirmos pastraipos m punkto taikymo tikslais Sąjungos subjektai atsižvelgia į kiekvienam tiesioginiam tiekėjui ir paslaugų teikėjui būdingą pažeidžiamumą ir bendrą savo tiekėjų bei paslaugų teikėjų produktų kokybę ir kibernetinio saugumo praktiką, įskaitant jų saugaus plėtojimo procedūras.

3. Sąjungos subjektai imasi bent šių konkrečių kibernetinio saugumo rizikos valdymo priemonių:

a) techninių priemonių, kuriomis sudaromos sąlygos nuotoliniam darbui ir jis palaikomas;

b) konkrečių veiksmų siekiant nulinio pasitikėjimo principų;

c) naudoja daugiaveiksnio tapatumo nustatymo būdą kaip visose tinklų ir informacinėse sistemose taikomą standartą;

d) naudoja kriptografiją ir šifravimą, visų pirma ištisinį šifravimą, taip pat saugų skaitmeninį pasirašymą;

e) kai taikytina, naudoja saugius balso, vaizdo ir teksto ryšius bei saugias avarinių ryšių sistemas Sąjungos subjekte;

f) iniciatyvių kenkimo programinės įrangos ir šnipinėjimo programų aptikimo ir pašalinimo priemonių;

g) užtikrina programinės įrangos tiekimo grandinės saugumą, taikydami saugios programinės įrangos kūrimo ir vertinimo kriterijus;

h) parengia ir patvirtina mokymo programas kibernetinio saugumo srityje, atitinkančias Sąjungos subjekto aukščiausio valdymo lygmeniui ir darbuotojams, kuriems pavesta užtikrinti veiksmingą šio reglamento įgyvendinimą, nustatytus uždavinius ir numatytus gebėjimus;

i) vykdo reguliarius darbuotojų mokymus kibernetinio saugumo klausimais;

j) prireikus dalyvauja atliekant dėl Sąjungos subjektų sujungiamumo kylančios rizikos analizę;

k) sugriežtina viešųjų pirkimų taisykles, kad būtų sudarytos palankesnės sąlygos užtikrinti aukštą bendrą kibernetinio saugumo lygį:

   i) pašalindami sutartines kliūtis, dėl kurių ribojamas IRT paslaugų teikėjų keitimasis informacija su CERT-EU apie incidentus, pažeidžiamumą ir kibernetines grėsmes;

   ii) nustatydami sutartinius įsipareigojimus pranešti apie incidentus, pažeidžiamumą ir kibernetines grėsmes ir įdiegti tinkamus reagavimo į incidentus bei jų stebėsenos mechanizmus.

9 straipsnis

Kibernetinio saugumo planai

1. Remdamasi išvadomis, padarytomis atlikus kibernetinio saugumo brandos vertinimą pagal 7 straipsnį, ir atsižvelgdama į Sistemoje nustatytą turtą ir kibernetinio saugumo riziką bei į kibernetinio saugumo rizikos valdymo priemones, kurių imtasi pagal 8 straipsnį, kiekvieno Sąjungos subjekto aukščiausias valdymo lygmuo nepagrįstai nedelsdamas ir bet kuriuo atveju ne vėliau kaip 2026 m. sausio 8 d. patvirtina kibernetinio saugumo planą. Kibernetinio saugumo planu siekiama padidinti bendrą atitinkamo Sąjungos subjekto kibernetinį saugumą ir taip juo prisidedama prie aukšto bendro kibernetinio saugumo lygio pasiekimo arba padidinimo Sąjungos subjektuose. Į kibernetinio saugumo planą įtraukiamos bent kibernetinio saugumo rizikos valdymo priemonės, kurių imtasi pagal 8 straipsnį. Kibernetinio saugumo planas peržiūrimas kas dvejus metus arba, prireikus – dažniau, po kibernetinio saugumo brandos vertinimų, atliktų pagal 7 straipsnį, arba po kiekvienos esminės Sistemos peržiūros.

2. Kibernetinio saugumo planas apima Sąjungos subjekto kibernetinės krizės valdymo planą įvykus dideliems incidentams.

3. Sąjungos subjektas parengtą kibernetinio saugumo planą pateikia pagal 10 straipsnį įsteigtai Tarpinstitucinei kibernetinio saugumo tarybai.

III SKYRIUS

TARPINSTITUCINĖ KIBERNETINIO SAUGUMO TARYBA

10 straipsnis

Tarpinstitucinė kibernetinio saugumo taryba

1. Įsteigiama Tarpinstitucinė kibernetinio saugumo taryba (toliau – TKST).

2. TKST pareigos:

a) stebėti, kaip Sąjungos subjektai įgyvendina šį reglamentą, ir padėti jiems jį įgyvendinti;

b) prižiūrėti, kaip CERT-EU įgyvendina bendruosius prioritetus ir tikslus, ir nustatyti CERT-EU strateginę kryptį.

3. TKST sudaro:

a) po vieną kiekvieno iš šių subjektų skiriamą atstovą:

   i) Europos Parlamentas;

   ii) Europos Vadovų Taryba;

   iii) Europos Sąjungos Taryba;

   iv) Komisija;

   v) Europos Sąjungos Teisingumo Teismas;

   vi) Europos Centrinis Bankas;

   vii) Audito Rūmai;

   viii) Europos išorės veiksmų tarnyba;

   ix) Europos ekonomikos ir socialinių reikalų komitetas;

   x) Europos regionų komitetas;

   xi) Europos investicijų bankas;

   xii) Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras;

   xiii) ENISA;

   xiv) Europos duomenų apsaugos priežiūros pareigūnas (EDAPP);

   xv) Europos Sąjungos kosmoso programos agentūra.

b) trys atstovai, kuriuos skiria ES agentūrų tinklas savo IRT patariamojo komiteto siūlymu, kad jie atstovautų Sąjungos organų, įstaigų ir agentūrų, kurie valdo savo pačių IRT aplinką, išskyrus nurodytuosius a punkte, interesams.

TKST atstovaujami Sąjungos subjektai siekia, kad tarp paskirtų atstovų būtų užtikrinta lyčių pusiausvyra.

4. TKST nariams gali padėti pakaitiniai nariai. Pirmininkas gali kviesti kitus 3 dalyje nurodytų Sąjungos subjektų arba kitų Sąjungos subjektų atstovus dalyvauti TKST posėdžiuose be balsavimo teisės.

5. CERT-EU vadovas ir atitinkamai pagal Direktyvos (ES) 2022/2555 14, 15 ir 16 straipsnius įsteigtų Bendradarbiavimo grupės, CSIRT tinklo ir EU-CyCLONe pirmininkai arba jų pakaitiniai nariai gali dalyvauti TKST posėdžiuose kaip stebėtojai. Išimtiniais atvejais TKST, laikydamasi savo vidaus darbo tvarkos taisyklių, gali nuspręsti kitaip.

6. TKST patvirtina savo vidaus darbo tvarkos taisykles.

7. Pagal savo vidaus darbo tvarkos taisykles TKST iš savo narių trejų metų laikotarpiui paskiria pirmininką. Pirmininko pakaitinis narys tam pačiam laikotarpiui tampa tikruoju TKST nariu.

8. TKST renkasi bent tris kartus per metus savo pirmininko iniciatyva, CERT-EU prašymu arba bet kurio iš jos narių prašymu.

9. Kiekvienas TKST narys turi po vieną balsą. TKST sprendimai priimami paprasta balsų dauguma, išskyrus atvejus, kai šiame reglamente numatyta kitaip. TKST pirmininkas nebalsuoja, išskyrus atvejus, kai balsai pasiskirsto po lygiai – tokiu atveju pirmininkas gali pasinaudoti lemiamo balso teise.

10. TKST gali priimti sprendimus taikydama supaprastintą rašytinę procedūrą, inicijuotą pagal jos vidaus darbo tvarkos taisykles. Pagal tą procedūrą laikoma, kad atitinkamas sprendimas yra patvirtintas per pirmininko nustatytą laikotarpį, išskyrus atvejus, kai narys pareiškia prieštaravimų.

11. Sekretoriato paslaugas TKST teikia Komisija ir sekretoriatas yra atskaitingas TKST pirmininkui.

12. Sąjungos agentūrų tinklo paskirti atstovai perduoda TKST sprendimus Sąjungos agentūrų tinklo nariams. Bet kuris Sąjungos agentūrų tinklo narys turi teisę pateikti tiems TKST atstovams ar pirmininkui bet kokį klausimą, į kurį, jo nuomone, turėtų būti atkreiptas TKST dėmesys.

13. TKST gali įsteigti vykdomąjį komitetą, kuris padėtų jam vykdyti savo darbą, ir deleguoti jam kai kurias savo užduotis ir įgaliojimus. TKST nustato vykdomojo komiteto darbo tvarkos taisykles, įskaitant jo užduotis bei įgaliojimus ir jo narių kadencijos trukmę.

14. TKST ne vėliau kaip 2025 m. sausio 8 d., o vėliau – kasmet teikia Europos Parlamentui ir Tarybai ataskaitą, kurioje išsamiai aprašoma pažanga, padaryta įgyvendinant šį reglamentą, ir, visų pirma, nurodomas CERT-EU bendradarbiavimo su analogiškais valstybės narės centrais kiekvienoje valstybėje narėje mastas. Ataskaita laikoma indėliu kas dvejus metus rengiant pagal Direktyvos (ES) 2022/2555 18 straipsnį teikiamą ataskaitą dėl kibernetinio saugumo padėties Sąjungoje.

11 straipsnis

TKST užduotys

Vykdydama savo pareigas TKST visų pirma:

a) teikia rekomendacijas CERT-EU vadovui;

b) veiksmingai stebi ir prižiūri, kaip įgyvendinamas šis reglamentas, ir padeda Sąjungos subjektams stiprinti savo kibernetinį saugumą, be kita ko, kai tinkama, prašydama iš Sąjungos subjektų ir CERT-EU *ad hoc* ataskaitų;

c) po strateginių diskusijų priima daugiametę strategiją dėl kibernetinio saugumo lygio didinimo Sąjungos subjektuose ir reguliariai, ir bet kuriuo atveju kas penkerius metus, tą strategiją įvertina ir, prireikus, iš dalies pakeičia;

d) nustato Sąjungos subjektų savanoriškų tarpusavio vertinimų atlikimo metodiką ir organizacinius aspektus, siekiant mokytis iš bendros patirties, stiprinti tarpusavio pasitikėjimą, pasiekti aukštą bendrą kibernetinio saugumo lygį, taip pat stiprinti Sąjungos subjektų kibernetinio saugumo pajėgumus, užtikrinant, kad tokius tarpusavio vertinimus atliktų kito Sąjungos subjekto nei vertinamas Sąjungos subjektas paskirti kibernetinio saugumo ekspertai ir kad metodika būtų grindžiama Direktyvos (ES) 2022/2555 19 straipsniu ir, kai tinkama, būtų pritaikyta Sąjungos subjektams;

e) CERT-EU vadovo siūlymu tvirtina CERT-EU metinę darbo programą ir stebi, kaip ji įgyvendinama;

f) CERT-EU vadovo siūlymu tvirtina CERT-EU paslaugų katalogą ir visus jo atnaujinimus;

g) CERT-EU vadovo siūlymu tvirtina metinį finansinį CERT-EU veiklos pajamų ir išlaidų, įskaitant personalą, planavimą;

h) CERT-EU vadovo siūlymu tvirtina susitarimus dėl paslaugų lygio susitarimų;

i) nagrinėja ir tvirtina CERT-EU vadovo parengtą metinę ataskaitą, kurioje aptariama CERT-EU veikla ir lėšų valdymas;

j) tvirtina CERT-EU pagrindinius veiklos rezultatų rodiklius (toliau - PVRR), kurie nustatomi remiantis CERT-EU vadovo siūlymu, ir stebi jų įgyvendinimą;

k) tvirtina CERT-EU ir kitų subjektų bendradarbiavimo susitarimus, susitarimus dėl paslaugų lygio arba sutartis pagal 18 straipsnį;

l) priima gaires ir rekomendacijas, remdamasi CERT-EU siūlymu pagal 14 straipsnį, ir nurodo CERT-EU paskelbti, atsiimti arba pakeisti pasiūlymą dėl gairių ar rekomendacijų arba raginimą imtis veiksmų;

m) įsteigia konkrečias užduotis turinčias technines patariamąsias grupes, siekiant prisidėti prie TKST darbo, tvirtina jų įgaliojimus ir skiria atitinkamus jų pirmininkus;

n) gauna ir vertina Sąjungos subjektų pagal šį reglamentą pateiktus dokumentus ir ataskaitas, pvz., kibernetinio saugumo brandos vertinimus;

o) sudaro palankesnes sąlygas įsteigti neformalią Sąjungos subjektų vietos kibernetinio saugumo pareigūnų grupę, kuriai padėtų ENISA ir kurios tikslas – keistis geriausios praktikos pavyzdžiais ir informacija, susijusiais su šio reglamento įgyvendinimu;

p) atsižvelgdama į CERT-EU pateiktą informaciją apie nustatytą kibernetinio saugumo riziką ir įgytą patirtį, stebi Sąjungos subjektų IRT aplinkų sujungimo susitarimų tinkamumą ir pataria dėl galimų patobulinimų;

q) parengia kibernetinių krizių valdymo planą, kuriuo siekiama operaciniu lygmeniu remti koordinuotą didelių incidentų, darančių poveikį Sąjungos subjektams, valdymą ir prisidėti prie reguliaraus keitimosi atitinkama informacija, visų pirma susijusia su didelių incidentų poveikiu, sunkumu ir galimais jų poveikio mažinimo būdais;

r) koordinuoja atskirų Sąjungos subjektų kibernetinių krizių valdymo planų, nurodytų 9 straipsnio 2 dalyje, priėmimą;

s) atsižvelgdama į Sąjungos lygmeniu koordinuojamų ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimų, nurodytų Direktyvos (ES) 2022/2555 22 straipsnyje, rezultatus, priima rekomendacijas, susijusias su 8 straipsnio 2 dalies pirmos pastraipos m punkte minimu tiekimo grandinės saugumu, siekdama padėti Sąjungos subjektams priimti veiksmingas ir proporcingas kibernetinio saugumo rizikos valdymo priemones.

12 straipsnis

Reikalavimų laikymasis

1. TKST pagal 10 straipsnio 2 dalį ir 11 straipsnį veiksmingai stebi, kaip įgyvendinamas šis reglamentas ir priimtos gairės, rekomendacijos ir raginimai Sąjungos subjektams imtis veiksmų. TKST gali prašyti Sąjungos subjektų pateikti tam tikslui reikalingą informaciją ar dokumentus. Atitikties užtikrinimo priemonių priėmimo pagal šį straipsnį tikslais, kai atitinkamas Sąjungos subjektas yra tiesiogiai atstovaujamas TKST, tam Sąjungos subjektui balsavimo teisės nesuteikiamos.

2. Jei TKST nustato, kad Sąjungos subjektas veiksmingai neįgyvendino šio reglamento arba pagal jį priimtų gairių, rekomendacijų ar raginimų imtis veiksmų, ji, nedarydama poveikio atitinkamo Sąjungos subjekto vidaus procedūroms ir suteikusi galimybę atitinkamam Sąjungos subjektui pateikti savo pastabas, gali:

a) perduoti pagrįstą nuomonę atitinkamam Sąjungos subjektui su nustatytomis spragomis įgyvendinant šį reglamentą;

b) pasikonsultavusi su CERT-EU, pateikti atitinkamam Sąjungos subjektui gaires, kaip per nustatytą terminą užtikrinti, kad jo sistema, kibernetinio saugumo rizikos valdymo priemonės, kibernetinio saugumo planas ir teikiamos ataskaitos atitiktų šį reglamentą;

c) teikti perspėjimą, kad per nustatytą terminą būtų pašalinti nustatyti trūkumai, įskaitant rekomendacijas iš dalies pakeisti priemones, kurias atitinkamas Sąjungos subjektas priėmė pagal šį reglamentą;

d) pateikia pagrįstą pranešimą atitinkamam Sąjungos subjektui, jei pagal c punktą pateiktame perspėjime nustatyti trūkumai per nurodytą laikotarpį nebuvo pakankamai pašalinti;

e) pateikia:

i) rekomendaciją atlikti auditą arba

ii) prašymą, kad auditą atliktų trečiosios šalies audito tarnyba;

f) jei taikytina, informuoti Audito Rūmus, neviršijant jų įgaliojimų, apie įtariamą reikalavimų nesilaikymą;

g) pateikti rekomendaciją, kad visos valstybės narės ir Sąjungos subjektai laikinai sustabdytų duomenų srautus į atitinkamą Sąjungos subjektą.

Pirmos pastraipos c punkto tikslais perspėjimo auditorija tinkamai apribojama, kai tai būtina atsižvelgiant į kibernetinio saugumo riziką.

Pagal pirmą pastraipą teikiami perspėjimai ir rekomendacijos skiriami atitinkamo Sąjungos subjekto aukščiausiam valdymo lygmeniui.

3. Jeigu TKST yra patvirtinusi priemones pagal 2 dalies pirmos pastraipos a–g punktus, atitinkamas Sąjungos subjektas pateikia išsamią informaciją apie priemones ir veiksmus, kurių imtasi TKST nustatytiems įtariamiems trūkumams pašalinti. Sąjungos subjektas pateikia tą išsamią informaciją per pagrįstą laikotarpį, dėl kurio turi būti susitarta su TKST.

4. Jei TKST mano, kad Sąjungos subjektas nuolat pažeidžia šį reglamentą tiesiogiai dėl Sąjungos pareigūno ar kito tarnautojo, įskaitant aukščiausią valdymo lygmenį, veiksmų ar neveikimo, TKST prašo, kad atitinkamas Sąjungos subjektas imtųsi tinkamų veiksmų, be kita ko, prašydamas jo apsvarstyti galimybę imtis drausminio pobūdžio veiksmų, laikantis taisyklių ir procedūrų, nustatytų Tarnybos nuostatuose, kitų taikytinų taisyklių ir procedūrų. Tuo tikslu TKST perduoda reikiamą informaciją atitinkamam Sąjungos subjektui.

5. Kai Sąjungos subjektas informuoja negalintis laikytis 6 straipsnio 1 dalyje ir 8 straipsnio 1 dalyje nustatytų terminų, tinkamai pagrįstais atvejais, atsižvelgdama į Sąjungos subjekto dydį, TKST gali leisti pratęsti tuos terminus.

IV SKYRIUS

CERT-EU

13 straipsnis

CERT-EU misija ir užduotys

1. CERT-EU misija – prisidėti prie Sąjungos subjektų neįslaptintos IRT aplinkos saugumo, konsultuojant juos kibernetinio saugumo klausimais, padedant jiems užkirsti kelią incidentams, juos atskleisti, valdyti, sušvelninti jų poveikį, į juos reaguoti ir atstatyti po jų veiklą, taip pat veikiant kaip jų keitimosi kibernetinio saugumo informacija ir reagavimo į incidentus koordinavimo centras.

2. CERT-EU neįslaptintoje IRT infrastruktūroje renka, tvarko, analizuoja informaciją apie kibernetines grėsmes, pažeidžiamumą bei incidentus ir ja dalijasi su Sąjungos subjektais. Ji koordinuoja reagavimą į incidentus tarpinstituciniu ir Sąjungos subjektų lygmeniu, be kita ko, teikdamas specializuotą operatyvinę pagalbą arba koordinuodamas jos teikimą.

3. Siekdama padėti Sąjungos subjektams, CERT-EU atlieka šias užduotis:

a) padeda jiems įgyvendinti šį reglamentą ir prisideda prie šio reglamento įgyvendinimo koordinavimo taikydama 14 straipsnio 1 dalyje išvardytas priemones arba teikdama TKST prašomas *ad hoc* ataskaitas;

b) siūlo standartines CSIRT paslaugas Sąjungos subjektams teikdama kibernetinio saugumo paslaugų, aprašytų savo paslaugų kataloge, paketą (toliau – pagrindinės paslaugos);

c) prižiūri kolegų ir partnerių tinklą, padedantį teikti paslaugas, kaip nurodyta 17 ir 18 straipsniuose;

d) atkreipia TKST dėmesį į visas problemas, susijusias su šio reglamento įgyvendinimu ir gairių, rekomendacijų bei raginimų imtis veiksmų įgyvendinimu;

e) remdamasi 2 dalyje nurodyta informacija ir glaudžiai bendradarbiaudama su ENISA prisideda prie informuotumo apie kibernetinę padėtį Sąjungoje;

f) koordinuoja didelių incidentų valdymą;

g) veikia Sąjungos subjektų vardu kaip koordinatoriaus, paskirto koordinuoto pažeidžiamumų atskleidimo tikslais pagal Direktyvos (ES) 2022/2555 12 straipsnio 1 dalį, atitikmuo;

h) Sąjungos subjekto prašymu atlieka aktyvų neintervencinį to Sąjungos subjekto viešai prieinamų tinklų ir informacinių sistemų tikrinimą.

Pirmos pastraipos e punkte nurodyta informacija dalijamasi su TKST, CSIRT tinklu ir Europos Sąjungos žvalgybos ir situacijų centru (EU INTCEN), kai taikytina ir tinkama, laikantis tinkamų konfidencialumo sąlygų.

4. CERT-EU gali atitinkamai pagal 17 arba 18 straipsnį bendradarbiauti su atitinkamomis kibernetinio saugumo bendruomenėmis Sąjungoje ir jos valstybėse narėse, be kita ko, šiose srityse:

a) parengties, incidentų koordinavimo, keitimosi informacija ir reagavimo į krizes techniniu lygmeniu su Sąjungos subjektais susijusiais atvejais;

b) operatyvinio bendradarbiavimo CSIRT tinkle, be kita ko, savitarpio pagalbos klausimais srityje;

c) žvalgybos informacijos apie kibernetines grėsmes, įskaitant informuotumą apie padėtį, srityje;

d) bet kurio klausimo, kuriam reikalingos CERT-EU techninės kibernetinio saugumo žinios, srityje.

5. Savo kompetencijos srityje CERT-EU vykdo struktūrinį bendradarbiavimą su ENISA pajėgumų stiprinimo, operatyvinio bendradarbiavimo ir ilgalaikės strateginės kibernetinių grėsmių analizės srityse pagal Reglamentą (ES) 2019/881. CERT-EU gali bendradarbiauti ir keistis informacija su Europolo Europos kovos su elektroniniu nusikalstamumu centru.

6. CERT-EU gali teikti šias paslaugas, kurios nėra aprašytos jos paslaugų kataloge (toliau – apmokestinamosios paslaugos):

a) paslaugas, kuriomis remiamas Sąjungos subjektų IRT aplinkos kibernetinis saugumas, išskyrus 3 dalyje nurodytas paslaugas, teikiamas remiantis susitarimais dėl paslaugų lygio ir atsižvelgiant į turimus išteklius, visų pirma plataus spektro tinklo stebėseną, įskaitant visą parą kasdien vykdomą labai didelių kibernetinių grėsmių stebėseną;

b) paslaugas, kuriomis remiamos Sąjungos subjektų kibernetinio saugumo operacijos ar projektai, išskyrus tas, kuriomis jie siekia apsaugoti savo IRT aplinką, teikiamas remiantis rašytiniais susitarimais ir gavus išankstinį TKST pritarimą;

c) gavus prašymą, aktyviai tikrina atitinkamo Sąjungos subjekto tinklų ir informacines sistemas, kad būtų galima nustatyti pažeidžiamumus, galinčius turėti didelį poveikį;

d) paslaugas, kuriomis remiamas organizacijų, kurios nėra Sąjungos subjektai, bet glaudžiai su jais bendradarbiauja, pavyzdžiui, vykdo pagal Sąjungos teisę pavestas užduotis ar pareigas, IRT aplinkos saugumas, teikiamas remiantis rašytiniais susitarimais ir iš anksto gavus TKST pritarimą.

Kalbant apie pirmos pastraipos d punktą, CERT-EU, gavusi išankstinį TKST pritarimą, išimtiniais atvejais gali sudaryti susitarimus dėl paslaugų lygio su subjektais, kurie nėra Sąjungos subjektai.

7. CERT-EU rengia kibernetinio saugumo pratybas ir gali jose dalyvauti, arba rekomenduoti dalyvauti vykdomose pratybose, kai tinkama, glaudžiai bendradarbiaudama su ENISA, kad patikrintų Sąjungos subjektų kibernetinio saugumo lygį.

8. CERT-EU gali teikti pagalbą Sąjungos subjektams dėl incidentų tinklų ir informacinėse sistemose, kuriose tvarkoma ESĮI, jei to aiškiai paprašo atitinkami Sąjungos subjektai pagal savo atitinkamas procedūras. CERT-EU pagalbos teikimas pagal šią dalį nedaro poveikio taikomoms taisyklėms dėl įslaptintos informacijos apsaugos.

9. CERT-EU informuoja Sąjungos subjektus apie incidentų valdymo procedūras ir procesus.

10. CERT-EU, užtikrindama aukštą konfidencialumo ir patikimumo lygį, naudodamasi tinkamais bendradarbiavimo mechanizmais ir atskaitomybės ryšiais, teikia aktualią ir anoniminę informaciją apie didelius incidentus ir apie tai, kaip jie buvo valdomi. Ta informacija įtraukiama į 10 straipsnio 14 dalyje nurodytą ataskaitą.

11. CERT-EU, bendradarbiaudama su EDAPP, padeda atitinkamiems Sąjungos subjektams reaguoti į incidentus, dėl kurių pažeidžiamas asmens duomenų saugumas, nedarant poveikio EDAPP, kaip priežiūros institucijos, kompetencijai ir užduotims pagal Reglamentą (ES) 2018/1725.

12. CERT-EU gali, jei to aiškiai paprašo Sąjungos subjektų politiniai skyriai, pateikti technines rekomendacijas arba nuomonę atitinkamais politiniais klausimais.

14 straipsnis

Gairės, rekomendacijos ir raginimai imtis veiksmų

1. CERT-EU padeda įgyvendinti šį reglamentą, teikdama:

a) raginimus imtis veiksmų, kuriuose aprašomos skubios saugumo priemonės, kurių Sąjungos subjektai raginami imtis per nustatytą laikotarpį;

b) pasiūlymus TKST dėl gairių, skirtų visiems Sąjungos subjektams arba jų daliai;

c) pasiūlymus TKST dėl atskiriems Sąjungos subjektams skirtų rekomendacijų.

Kiek tai susiję su pirmos pastraipos a punktu, atitinkamas Sąjungos subjektas, gavęs raginimą imtis veiksmų, nepagrįstai nedelsdamas informuoja CERT-EU apie tai, kaip buvo taikomos skubios saugumo priemonės.

2. Gairės ir rekomendacijos gali apimti:

a) bendras Sąjungos subjektų kibernetinio saugumo brandos vertinimo metodikas ir modelį, įskaitant atitinkamas skales arba PVRR, kuriais remiamasi siekiant nuolat gerinti kibernetinį saugumą Sąjungos subjektuose ir palengvinti kibernetinio saugumo sričių ir priemonių prioritetų nustatymą, atsižvelgiant į subjektų kibernetinio saugumo būklę;

b) susitarimus dėl kibernetinio saugumo rizikos valdymo ir kibernetinio saugumo rizikos valdymo priemonių ir jų tobulinimo sąlygas;

c) kibernetinio saugumo brandos vertinimo ir kibernetinio saugumo planų susitarimus;

d) kai tinkama, bendrų technologijų, architektūros, atvirojo kodo ir susijusios geriausios praktikos naudojimą siekiant užtikrinti sąveikumą ir bendrus standartus, įskaitanti suderintą požiūrį į tiekimo grandinių saugumą;

e) kai tinkama, informaciją, kuria sudaromos palankesnės sąlygos naudotis bendradarbiaujamųjų viešųjų pirkimų priemonėmis perkant atitinkamas kibernetinio saugumo paslaugas ir produktus iš trečiųjų šalių tiekėjų;

f) keitimosi informacija tvarką pagal 20 straipsnį.

15 straipsnis

CERT-EU vadovas

1. Komisija, gavusi dviejų trečdalių TKST narių balsų daugumos pritarimą, skiria CERT-EU vadovą. Su TKST konsultuojamasi visais skyrimo procedūros etapais, visų pirma rengiant pranešimus apie laisvas darbo vietas, nagrinėjant paraiškas ir skiriant atrankos komisijas dėl pareigybės. Atrankos procedūra, įskaitant galutinį kandidatų, iš kurių turi būti paskirtas CERT-EU vadovas, sąrašą, užtikrinama, kad būtų teisingai atstovaujama kiekvienai lyčiai, atsižvelgiant į pateiktas paraiškas.

2. CERT-EU vadovas yra atsakingas už sklandų CERT-EU veikimą ir eina pareigas savo pareigų kompetencijos srityje vadovaujant TKST. CERT-EU vadovas reguliariai teikia ataskaitas TKST pirmininkui ir jo prašymu teikia TKST *ad hoc* ataskaitas.

3. CERT-EU vadovas padeda atsakingam deleguotajam leidimus suteikiančiam pareigūnui pagal Europos Parlamento ir Tarybos reglamento (ES, Euratomas) 2018/1046 ([9]) 74 straipsnio 9 dalį parengti metinę veiklos ataskaitą, kurioje pateikiama finansinė ir valdymo informacija, įskaitant kontrolės rezultatus, ir reguliariai deleguotajam leidimus suteikiančiam pareigūnui teikia ataskaitas dėl priemonių, kurių atžvilgiu CERT-EU vadovui buvo perdeleguoti įgaliojimai, įgyvendinimo.

4. CERT-EU vadovas kasmet parengia savo veiklos administracinių pajamų ir išlaidų finansinį planą, siūlomą metinę darbo programą, siūlomą paslaugų katalogą, skirtą CERT-EU, siūlomus paslaugų katalogo pakeitimus, siūlomus susitarimus dėl paslaugų lygio sąlygų ir siūlomus PVRR, skirtus CERT-EU, kuriuos pagal 11 straipsnį turi patvirtinti TKST. Peržiūrėdamas CERT-EU paslaugų kataloge pateiktą paslaugų sąrašą, CERT-EU vadovas atsižvelgia į CERT-EU skirtus išteklius.

5. CERT-EU vadovas bent kartą per metus pateikia TKST ir TKST pirmininkui ataskaitas apie CERT-EU veiklą ir veiklos rezultatus ataskaitiniu laikotarpiu, įskaitant ataskaitas dėl biudžeto vykdymo, sudarytų susitarimų dėl paslaugų lygio ir rašytinių susitarimų, bendradarbiavimo su analogiškais centrais ir partneriais ir darbuotojų vykdomų misijų, įskaitant 11 straipsnyje nurodytas ataskaitas. Tose ataskaitose pateikiama kito laikotarpio darbo programa, pajamų ir išlaidų finansinis planavimas, įskaitant personalo srityje, planuojami CERT-EU paslaugų katalogo atnaujinimai ir numatomo tokių atnaujinimų poveikio finansiniams ir žmogiškiesiems ištekliams vertinimas.

16 straipsnis

Finansiniai ir personalo klausimai

1. CERT-EU integruojama į Komisijos generalinio direktorato administracinę struktūrą, kad galėtų naudotis Komisijos administravimo, finansų valdymo ir apskaitos paramos struktūromis, kartu išlaikant jos, kaip savarankiško tarpinstitucinio paslaugų visiems Sąjungos subjektams teikėjo statusą. Komisija informuoja TKST apie CERT-EU vietą administracinėje struktūroje ir su tuo susijusius pokyčius. Komisija reguliariai ir bet kuriuo atveju prieš sudarant bet kokią daugiametę finansinę programą pagal SESV 312 straipsnį peržiūri su CERT-EU susijusius administracinius susitarimus, kad būtų galima imtis tinkamų veiksmų. Atliekant peržiūrą svarstoma galimybė įsteigti CERT-EU kaip Sąjungos tarnybą.

2. Taikydamas administracines ir finansines procedūras, CERT-EU vadovas veikia vadovaudamasis Komisijos nurodymais ir prižiūrint TKST.

([9]) 2018 m. liepos 18 d. Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) 2018/1046 dėl Sąjungos bendrajam biudžetui taikomų finansinių taisyklių, kuriuo iš dalies keičiami reglamentai (ES) Nr. 1296/2013, (ES) Nr. 1301/2013, (ES) Nr. 1303/2013, (ES) Nr. 1304/2013, (ES) Nr. 1309/2013, (ES) Nr. 1316/2013, (ES) Nr. 223/2014, (ES) Nr. 283/2014 ir Sprendimas Nr. 541/2014/ES, bei panaikinamas Reglamentas (ES, Euratomas) Nr. 966/2012 (OL L 193, 2018 7 30, p. 1).

3. CERT-EU užduotys ir veikla, įskaitant pagal 13 straipsnio 3, 4, 5 ir 7 dalis ir 14 straipsnio 1 dalį CERT-EU teikiamas paslaugas Sąjungos subjektams, finansuojamas pagal daugiametės finansinės programos išlaidų kategoriją, skirtą Europos viešajam administravimui, finansuojamos pagal atskirą Komisijos biudžeto eilutę. CERT-EU skirti etatai išsamiai nurodomi Komisijos etatų plano išnašoje.

4. Kiti nei šio straipsnio 3 dalyje nurodyti Sąjungos subjektai pagal tą dalį skiria CERT-EU metinį finansinį įnašą CERT-EU teikiamų paslaugų sąnaudoms padengti. Įnašai nustatomi remiantis TKST pateiktomis gairėmis ir dėl jų kiekvienas Sąjungos subjektas ir CERT-EU susitaria paslaugų lygio susitarimuose. Įnašai sudaro teisingą ir proporcingą visų suteiktų paslaugų sąnaudų dalį. Jos gaunamos pagal šio straipsnio 3 dalyje nurodytą atskirą biudžeto eilutę kaip vidaus asignuotosios pajamos, kaip numatyta Reglamento (ES, Euratomas) 2018/1046 21 straipsnio 3 dalies c punkte.

5. Su pagal 13 straipsnio 6 dalį teikiamomis paslaugomis susijusios išlaidos susigrąžinamos iš CERT-EU paslaugas gaunančių Sąjungos subjektų. Pajamos priskiriamos išlaidoms padengti skirtoms biudžeto eilutėms.

17 straipsnis

CERT-EU bendradarbiavimas su analogiškais valstybės narės centrais

1. CERT-EU nepagrįstai nedelsdama bendradarbiauja ir keičiasi informacija su atitinkamais analogiškais valstybės narės centrais, visų pirma CSIRT, paskirtomis arba įsteigtomis pagal Direktyvos (ES) 2022/2555 10 straipsnį, arba, kai taikytina, su kompetentingomis institucijomis ir bendrais kontaktiniais punktais, paskirtais arba įsteigtais pagal tos direktyvos 8 straipsnį, klausimais, susijusiais su incidentais, kibernetinėmis grėsmėmis, pažeidžiamumais, vos neįvykusiais incidentais, galimomis atsakomosiomis priemonėmis ir geriausia praktika, taip pat visais klausimais, susijusiais su Sąjungos subjektų IRT aplinkos apsaugos gerinimu, be kita ko, pasitelkiant CSIRT tinklą, sukurtą pagal Direktyvos (ES) 2022/2555 15 straipsnį. CERT-EU padeda Komisijai EU-CyCLONe, įsteigtame pagal Direktyvos (ES) 2022/2555 16 straipsnį, koordinuoti didelio masto kibernetinio saugumo incidentų ir krizių valdymą.

2. Kai CERT-EU sužino apie reikšmingą incidentą, vykstantį atitinkamos valstybės narės teritorijoje, ji nedelsdama pagal 1 dalį praneša visiems analogiškiems tos valstybės narės centrams.

3. Su sąlyga, kad asmens duomenys yra saugomi pagal taikytinus Sąjungos duomenų apsaugos teisės aktus, CERT-EU nepagrįstai nedelsdama be paveikto Sąjungos subjekto leidimo keičiasi su analogiškais valstybės narės centrais atitinkama su incidentu susijusia informacija, kuri yra svarbi siekiant palengvinti panašių kibernetinių grėsmių ar incidentų nustatymą arba prisidėti prie incidento analizės. CERT-EU keičiasi su incidentu susijusia informacija, kurioje atskleidžiama kibernetinio saugumo incidento taikinio tapatybė, tik vienu iš šių atvejų:

a) laikomasi Sąjungos duomenų apsaugos teisės aktų, o paveiktas Sąjungos subjektas duoda sutikimą;

b) paveiktas Sąjungos subjektas neduoda sutikimo, kaip numatyta a punkte, tačiau atskleidus paveikto Sąjungos subjekto tapatybę padidėtų tikimybė, kad kitur bus išvengta incidentų arba jų poveikis bus sumažintas;

c) paveiktas Sąjungos subjektas jau viešai paskelbė, kad buvo paveiktas.

Sprendimus keistis su incidentu susijusia informacija, atskleidžiančia incidento taikinio tapatybę pagal pirmos pastraipos b punktą, tvirtina CERT-EU vadovas. Prieš priimdama tokį sprendimą CERT-EU raštu susisiekia su paveiktu Sąjungos subjektu ir aiškiai paaiškina, kaip atskleidus jo tapatybę būtų galima išvengti incidentų kitur arba sumažinti jų poveikį. CERT-EU vadovas pateikia paaiškinimą ir aiškiai paprašo Sąjungos subjekto per nustatytą laikotarpį nurodyti, ar jis sutinka. CERT-EU vadovas taip pat informuoja Sąjungos subjektą, kad, atsižvelgdamas į pateiktą paaiškinimą, jis pasilieka teisę atskleisti informaciją net ir negavus sutikimo. Prieš atskleidžiant informaciją, apie tai pranešama paveiktam Sąjungos subjektui.

18 straipsnis

CERT-EU bendradarbiavimas su kitais analogiškais centrais

1. CERT-EU gali bendradarbiauti su 17 straipsnyje nenurodytais analogiškais Sąjungos centrais, kuriems taikomi Sąjungos kibernetinio saugumo reikalavimai, įskaitant pramonės sektorių partnerius, klausimais, susijusiais su priemonėmis ir metodais, pavyzdžiui, specialia metodika, taktika, procedūromis ir geriausios praktikos pavyzdžiais, taip pat su kibernetinėmis grėsmėmis bei pažeidžiamumu. Kad galėtų visapusiškai bendradarbiauti su tokiais centrais CERT-EU kiekvienu atskiru atveju turi gauti išankstinį TKST pritarimą. Kai CERT-EU pradeda bendradarbiauti su tokiais analogiškais centrais, ji informuoja visus 17 straipsnio 1 dalyje nurodytus atitinkamus analogiškus valstybės narės centrus toje valstybėje narėje, kurioje centras yra įsisteigęs. Kai taikytina ir tinkama, toks bendradarbiavimas ir jo sąlygos, be kita ko, dėl kibernetinio saugumo, duomenų apsaugos ir informacijos tvarkymo, nustatomi specialiuose konfidencialumo susitarimuose, pvz., sutartyse ar administraciniuose susitarimuose. Konfidencialumo susitarimams nereikia išankstinio TKST pritarimo, tačiau apie juos informuojamas TKST pirmininkas. Iškilus skubiam ir neišvengiamam poreikiui keistis kibernetinio saugumo informacija Sąjungos subjektų ar kitos šalies interesais, CERT-EU gali tai daryti su subjektu, kurio konkreti kompetencija, pajėgumai ir ekspertinės žinios pagrįstai reikalingi siekiant patenkinti tokį skubų ir neišvengiamą poreikį, net jei CERT-EU su tuo subjektu nėra sudariusi konfidencialumo susitarimo. Tokiais atvejais CERT-EU nedelsdama informuoja TKST pirmininką ir atsiskaito TKST reguliariai teikdama ataskaitas arba rengdama posėdžius.

2. CERT-EU gali bendradarbiauti su partneriais, pvz., komerciniais subjektais, įskaitant konkretaus pramonės sektoriaus subjektus, tarptautinėmis organizacijomis, ne Europos Sąjungos nacionaliniais subjektais arba atskirais ekspertais, kad surinktų informaciją apie bendro pobūdžio ir konkrečias kibernetines grėsmes, vos neįvykusius incidentus, pažeidžiamumą ir galimas atsakomąsias priemones. Kad galėtų platesniu mastu bendradarbiauti su tokiais partneriais CERT-EU kiekvienu atskiru atveju turi gauti išankstinį TKST pritarimą.

3. CERT-EU, gavusi incidento paveikto Sąjungos subjekto sutikimą ir su sąlyga, kad su analogišku centru ar partneriu yra sudarytas informacijos neatskleidimo susitarimas arba sutartis, 1 ir 2 dalyse nurodytiems analogiškiems centrams ar partneriams gali teikti su incidentu susijusią informaciją tik tam, kad prisidėtų prie to incidento analizės.

V SKYRIUS

PAREIGOS BENDRADARBIAUTI IR PRANEŠTI

19 straipsnis

Duomenų tvarkymas

1. Sąjungos subjektai ir CERT-EU laikosi pareigos saugoti tarnybinę paslaptį pagal SESV 339 straipsnį arba lygiavertes taikytinas sistemas.

2. Paraiškoms dėl galimybės visuomenei susipažinti su CERT-EU turimais dokumentais taikomas Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1049/2001 ([10]), įskaitant tame reglamente nustatytą pareigą konsultuotis su kitais Sąjungos subjektais ir, kai tikslinga, su valstybėmis narėmis, kai prašymas susijęs su jų dokumentais.

3. Sąjungos subjektai ir CERT-EU duomenis tvarko pagal taikomas taisykles dėl informacijos saugumo.

([10]) 2001 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1049/2001 dėl galimybės visuomenei susipažinti su Europos Parlamento, Tarybos ir Komisijos dokumentais (OL L 145, 2001 5 31, p. 43).

20 straipsnis

Dalijimosi kibernetinio saugumo informacija susitarimai

1. Sąjungos subjektai gali savanoriškai pranešti CERT-EU apie jiems poveikį darančius incidentus, kibernetines grėsmes, vos neįvykusius incidentus ir pažeidžiamumą, ir teikti CERT-EU informaciją apie juos. Siekiant palengvinti keitimąsi informacija su Sąjungos subjektais, CERT-EU užtikrina, kad būtų galima naudotis veiksmingomis, aukšto lygio atsekamumo, konfidencialumo ir patikimumo komunikacijos priemonėmis. CERT-EU, tvarkydama pranešimus, gali teikti pirmenybę privalomų pranešimų tvarkymui, palyginti su savanoriškais pranešimais. Nedarant poveikio 12 straipsniui, dėl savanoriško pranešimo pranešimą teikiančiam Sąjungos subjektui nenustatoma jokių papildomų pareigų, kurios jam nebūtų taikomos, jei jis nebūtų pateikęs pranešimo.

2. Kad galėtų vykdyti savo misiją ir užduotis, pavestas pagal 13 straipsnį, CERT-EU gali reikalauti, kad Sąjungos subjektai jai teiktų informaciją iš savo atitinkamų IRT sistemų aprašų, įskaitant informaciją, susijusią su kibernetinėmis grėsmėmis, vos neįvykusiais incidentais, pažeidžiamumais, užvaldymo rodikliais, kibernetinio saugumo įspėjimais ir rekomendacijomis dėl kibernetinio saugumo priemonių konfigūracijos siekiant aptikti incidentus. Sąjungos subjektas, į kurį kreipiamasi, nepagrįstai nedelsdamas perduoda prašomą informaciją ir visus vėlesnius jos atnaujinimus.

3. CERT-EU gali su Sąjungos subjektais keistis su incidentu susijusia informacija, kurioje atskleidžiama nuo kibernetinio saugumo incidento nukentėjusio Sąjungos subjekto tapatybė su sąlyga, kad nukentėjęs Sąjungos subjektas sutinka. Jei Sąjungos subjektas sutikimo neduoda, jis CERT-EU pateikia tokį sprendimą pagrindžiančias priežastis.

4. Sąjungos subjektai, gavę prašymą, dalijasi informacija apie kibernetinio saugumo planų įgyvendinimą su Europos Parlamentu ir Taryba.

5. Gavus prašymą, atitinkamai TKST arba CERT-EU dalijasi gairėmis, rekomendacijomis ir raginimais imtis veiksmų su Europos Parlamentu ir Taryba.

6. Šiame straipsnyje nustatytos pareigos dalytis netaikomos:

a) ESĮI;

b) informacijai, kurios tolesnis platinimas uždraustas aiškiai pažymint, išskyrus atvejus, kai ja aiškiai leidžiama dalytis su CERT-EU.

21 straipsnis

Pareigos pranešti

1. Incidentas laikomas reikšmingu, jeigu:

a) dėl jo atitinkamas Sąjungos subjektas patyrė arba gali patirti didelių veikimo sutrikimų arba finansinių nuostolių;

b) jis paveikė arba gali paveikti kitus fizinius ar juridinius asmenis sukeldamas didelę materialinę arba neturtinę žalą.

2. Sąjungos subjektai CERT-EU pateikia:

a) nepagrįstai nedelsiant ir bet kuriuo atveju per 24 valandas nuo tada, kai sužinojo apie reikšmingą incidentą, – ankstyvąjį perspėjimą, kuriame, kai taikytina, nurodoma, kad reikšmingą incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai arba, kad jis galėtų daryti poveikį keliems subjektams ar tarpvalstybinį poveikį;

b) nepagrįstai nedelsdami ir bet kuriuo atveju per 72 valandas nuo tada, kai sužinojo apie didelį incidentą, – pranešimą apie incidentą, kuriame, kai taikytina, atnaujinama a punkte nurodyta informacija ir nurodomas didelio incidento, įskaitant jo sunkumą ir poveikį, pradinis vertinimas, taip pat nurodomi užvaldymo rodikliai, jei tokių yra;

c) CERT-EU prašymu – tarpinę ataskaitą apie atitinkamus atnaujintus duomenis apie padėtį;

d) ne vėliau kaip per vieną mėnesį nuo b punkte nurodyto pranešimo apie incidentą – galutinę ataskaitą, kurioje pateikiama ši informacija:

i) išsamus incidento, įskaitant jo sunkumą ir poveikį, aprašymas;

ii) grėsmės arba pagrindinės priežasties, dėl kurios incidentas galėjo būti sukeltas, rūšis;

iii) taikomos ir įgyvendinamos poveikio mažinimo priemonės;

iv) kai taikytina, tarpvalstybinis ar kelis subjektus apimantis incidento poveikis;

e) tuo atveju, jei d punkte nurodytos galutinės ataskaitos pateikimo metu incidentas tebevyksta, – to meto pažangos ataskaitą, o galutinę ataskaitą – per vieną mėnesį nuo tada, kai suvaldė incidentą.

3. Sąjungos subjektas nepagrįstai nedelsdamas ir bet kuriuo atveju per 24 valandas nuo tada, kai sužinojo apie reikšmingą incidentą, informuoja visus atitinkamus 17 straipsnio 1 dalyje nurodytus analogiškus valstybės narės centrus toje valstybėje narėje, kurioje yra subjektas, kad įvyko reikšmingas incidentas.

4. Sąjungos subjektai, *inter alia*, praneša bet kokią informaciją, kuri gali padėti CERT-EU nustatyti bet kokį poveikį keliems subjektams, poveikį priimančiajai valstybei narei arba tarpvalstybinį reikšmingo incidento poveikį. Nedarant poveikio 12 straipsnio taikymui, vien dėl pranešimo veiksmo negali būti padidinama Sąjungos subjekto atsakomybė.

5. Kai taikytina, Sąjungos subjektai nepagrįstai nedelsdami informuoja paveiktų tinklų ir informacinių sistemų arba kitų IRT aplinkos komponentų naudotojus, kuriuos reikšmingas incidentas arba didelė kibernetinė grėsmė galėjo paveikti ir kurie, kai tinkama, turi imtis poveikio mažinimo priemonių, apie visas priemones ar teisių gynimo priemones, kurių jie gali imtis reaguodami į tą incidentą arba tą grėsmę. Atitinkamais atvejais Sąjungos subjektai praneša tiems naudotojams apie pačią didelę kibernetinę grėsmę.

6. Kai reikšmingas incidentas ar didelė kibernetinė grėsmė daro poveikį tinklų ar informacinei sistemai arba Sąjungos subjekto IRT aplinkos komponentui, kuris, kaip žinoma, yra sujungtas su kito Sąjungos subjekto aplinka, CERT-EU paskelbia atitinkamą kibernetinio saugumo įspėjimą.

7. Sąjungos subjektai CERT-EU prašymu nepagrįstai nedelsdami suteikia CERT-EU skaitmeninę informaciją, sukurtą naudojant elektroninius įtaisus, susijusius su atitinkamais incidentais. CERT-EU gali pateikti išsamesnės informacijos apie tai, kokios rūšies informacijos jai reikia informuotumo apie padėtį ir reagavimo į incidentus tikslais.

8. CERT-EU kas tris mėnesius TKST, ENISA, ES INTCEN ir CSIRT tinklui pateikia apibendrinamąją ataskaitą, įskaitant nuasmenintus ir apibendrintus duomenis apie reikšmingus incidentus, incidentus, kibernetines grėsmes, vos neįvykusius incidentus ir pažeidžiamumus pagal 20 straipsnį ir reikšmingus incidentus, apie kuriuos pranešta pagal šio straipsnio 2 dalį. Apibendrinamoji ataskaita laikoma indėliu kas dvejus metus rengiant ataskaitą dėl kibernetinio saugumo padėties Sąjungoje, priimamą pagal Direktyvos (ES) 2022/2555 18 straipsnį.

9. TKST ne vėliau kaip 2024 m. liepos 8 d. paskelbia gaires arba rekomendacijas, kuriose toliau patikslinami pagal šį straipsnį teikiamų ataskaitų tvarka, forma ir turinys. Rengdama tokias gaires ar rekomendacijas, TKST atsižvelgia į visus pagal Direktyvos (ES) 2022/2555 23 straipsnio 11 dalį priimtus įgyvendinimo aktus, kuriuose nurodomi informacijos rūšis, formatas ir pranešimų teikimo procedūra. CERT-EU platina atitinkamą techninę informaciją, kad Sąjungos subjektai galėtų aktyviai aptikti incidentus, reaguoti į juos arba imtis rizikos mažinimo priemonių.

10. Šiame straipsnyje nustatytos pareigos pranešti netaikomos:

a) ESĮI;

b) informacijai, kurios tolesnis platinimas uždraustas aiškiai pažymint, išskyrus atvejus, kai ja aiškiai leidžiama dalytis su CERT-EU.

22 straipsnis

Reagavimo į incidentus koordinavimas ir bendradarbiavimas

1. CERT-EU, veikdama kaip keitimosi kibernetinio saugumo informacija ir reagavimo į incidentus koordinavimo centras, palengvina keitimąsi informacija apie incidentus, kibernetines grėsmes, pažeidžiamumus ir vos neįvykusius incidentus tarp:

a) Sąjungos subjektų;

b) 17 ir 18 straipsniuose nurodytų analogiškų centrų.

2. CERT-EU, kai tinkama, glaudžiai bendradarbiaudama su ENISA, palengvina Sąjungos subjektų reagavimo į incidentus koordinavimą, susijusį, be kita ko, su:

a) indėliu prie nuoseklios išorės komunikacijos;

b) savitarpio pagalba, pvz., dalijimusi Sąjungos subjektams svarbia informacija arba prireikus teikiant pagalbą tiesiogiai vietoje;

c) optimaliu veiklos išteklių naudojimu;

d) koordinavimu su kitais reagavimo į krizes mechanizmais Sąjungos lygmeniu.

3. CERT-EU, glaudžiai bendradarbiaudama su ENISA, teikia paramą Sąjungos subjektams, susijusią su informuotumu apie incidentų, kibernetinių grėsmių, pažeidžiamumų ir vos neįvykusių incidentų padėtį, taip pat dalijantis atitinkama informacija apie pokyčius kibernetinio saugumo srityje.

4. TKST, remdamasis CERT-EU pasiūlymu, ne vėliau kaip 2025 m. sausio 8 d. priima gaires arba rekomendacijas dėl reagavimo į incidentus koordinavimo ir bendradarbiavimo reikšmingų incidentų atveju. Kai įtariama, kad incidentas yra baudžiamojo pobūdžio, CERT-EU pataria, kaip nepagrįstai nedelsiant pranešti apie incidentą teisėsaugos institucijoms.

5. Gavusi konkretų valstybės narės prašymą ir sulaukusi atitinkamų Sąjungos subjektų pritarimo, CERT-EU gali pakviesti ekspertus iš 23 straipsnio 4 dalyje nurodyto sąrašo prisidėti reaguojant į didelį incidentą, kuris daro poveikį toje valstybėje narėje, arba į didelio masto kibernetinio saugumo incidentą pagal Direktyvos (ES) 2022/2555 15 straipsnio 3 dalies g punktą. TKST, remdamasi CERT-EU pasiūlymu, patvirtina konkrečias taisykles dėl Sąjungos subjektų techninių ekspertų paslaugų prieinamumo ir naudojimosi jomis.

23 straipsnis

Didelių incidentų valdymas

1. Siekdama operaciniu lygmeniu remti suderintą didelių incidentų, darančių poveikį Sąjungos subjektams, valdymą ir prisidėti prie reguliaraus Sąjungos subjektų tarpusavio keitimosi atitinkama informacija ir keitimosi ja su valstybėmis narėmis, TKST, glaudžiai bendradarbiaudama su CERT-EU ir ENISA, pagal 11 straipsnio q punktą parengia kibernetinių krizių valdymo planą, grindžiamą 22 straipsnio 2 dalyje nurodyta veikla. Į kibernetinių krizių valdymo planą įtraukiami bent šie aspektai:

a) susitarimai dėl Sąjungos subjektų veiksmų koordinavimo ir informacijos srautų, susijusių su didelių incidentų valdymu operaciniu lygmeniu;

b) bendros standartinės veiklos procedūros (SVP);

c) bendra didelių incidentų rimtumo ir krizę sukeliančių veiksnių taksonomija;

d) reguliarios pratybos;

e) naudotini saugūs ryšių kanalai.

2. Komisijos atstovas TKST, atsižvelgiant į pagal šio straipsnio 1 dalį priimtą kibernetinių krizių valdymo planą ir nedarant poveikio Direktyvos (ES) 2022/2555 16 straipsnio 2 dalies pirmai pastraipai, yra kontaktinis punktas keičiantis svarbia informacija, susijusia su dideliais incidentais EU-CyCLONe.

3. CERT-EU koordinuoja Sąjungos subjektų veiksmus valdant didelius incidentus. Ji tvarko turimų techninių ekspertinių žinių, kurių reikėtų reaguojant į incidentus didelių incidentų atveju, aprašą ir padeda TKST koordinuoti Sąjungos subjektų didelių incidentų sukeltos kibernetinės krizės valdymo planus, nurodytus 9 straipsnio 2 dalyje.

4. Sąjungos subjektai prisideda prie techninių ekspertinių žinių aprašo, pateikdami kasmet atnaujinamą atitinkamose jų organizacijose turimų ekspertų sąrašą, kuriame išsamiai nurodomi jų konkretūs techniniai įgūdžiai.

VI SKYRIUS

BAIGIAMOSIOS NUOSTATOS

24 straipsnis

Pradinis biudžeto perskirstymas

Siekdama užtikrinti tinkamą ir stabilų CERT-EU veikimą, Komisija gali pasiūlyti perkelti darbuotojus ir finansinius išteklius į Komisijos biudžetą, kad juos būtų galima naudoti CERT-EU operacijoms vykdyti. Perskirstymas įsigalioja tuo pačiu metu kaip ir pirmasis Sąjungos metinis biudžetas, priimtas įsigaliojus šiam reglamentui.

25 straipsnis

Peržiūra

1. TKST, padedant CERT-EU, ne vėliau kaip 2025 m. sausio 8 d., o vėliau – kasmet, teikia Komisijai šio reglamento įgyvendinimo ataskaitą. TKST gali teikti rekomendacijas Komisijai peržiūrėti šį reglamentą.

2. Komisija ne vėliau kaip 2027 m. sausio 8 d., o vėliau – kas dvejus metus, įvertina šio reglamento įgyvendinimą ir strateginiu bei veiklos lygmenimis įgytą patirtį ir pateikia ataskaitą Europos Parlamentui ir Tarybai.

Šios dalies pirmos pastraipos nurodytoje ataskaitoje pateikiama 16 straipsnio 1 dalyje nurodyta peržiūra dėl galimybės įsteigti CERT-EU kaip Sąjungos tarnybą.

3. Komisija ne vėliau kaip 2029 m. sausio 8 d. įvertina šio reglamento veikimą ir pateikia ataskaitą Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui bei Regionų komitetui. Komisija taip pat įvertina, ar tikslinga į šio reglamento taikymo sritį įtraukti tinklų ir informacines sistemas, kuriose tvarkoma ESĮI, atsižvelgdama į kitus toms sistemoms taikomus Sąjungos teisėkūros procedūra priimtus aktus. Kai būtina, prie ataskaitos pridedamas pasiūlymas dėl teisėkūros procedūra priimamo akto.

26 straipsnis

Įsigaliojimas

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Strasbūre 2023 m. gruodžio 13 d.

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkė	*Pirmininkas*
R. METSOLA	P. NAVARRO RÍOS