SPRENDIMAI

KOMISIJOS SPRENDIMAS (ES, Euratomas) 2017/46

2017 m. sausio 10 d.

dėl Europos Komisijos ryšių ir informacinių sistemų saugumo

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 249 straipsnį,

atsižvelgdama į Europos atominės energijos bendrijos steigimo sutartį,

kadangi:

(1) Komisijos ryšių ir informacinės sistemos yra neatsiejama jos veikimo dalis, o IT saugumo incidentų poveikis Komisijos veiklai, taip pat trečiosioms šalims, įskaitant asmenis, įmones ir valstybes nares, gali būti didelis;

(2) yra daug grėsmių Komisijos ryšių ir informacinių sistemų ir jose tvarkomos informacijos konfidencialumui, vientisumui ir prieinamumui. Šios grėsmės, be kita ko, gali būti avarijos, klaidos, tyčiniai išpuoliai ar gamtos reiškiniai ir turi būti pripažįstamos veiklos rizika;

(3) reikia užtikrinti ryšių ir informacinių sistemų apsaugos lygį, atitinkantį joms gresiančios rizikos tikimybę, poveikį ir pobūdį;

(4) Komisijos IT saugumo priemonėmis turėtų būti užtikrinta, kad Komisijos ryšių ir informacinėse sistemose (RIS) tvarkoma informacija būtų apsaugota ir kad teisėtų naudotojų valdomos sistemos veiktų taip, kaip reikia, ir tada, kada reikia;

(5) Komisijos IT saugumo politika turėtų būti įgyvendinama taip, kad būtų suderinama su Komisijos saugumo politikos nuostatomis;

(6) Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktoratas yra bendrai atsakingas už saugumą Komisijoje, o jį prižiūri ir už jį atsako už saugumą atsakingas Komisijos narys;

(7) Komisijos koncepcija turėtų būti formuojama atsižvelgiant į ES politikos iniciatyvas ir teisės aktus dėl tinklų ir informacijos saugumo, pramonės standartus ir gerąją patirtį, kad būtų laikomasi visų atitinkamų teisės aktų ir būtų užtikrintas sąveikumas ir suderinamumas;

(8) už ryšių ir informacines sistemas atsakingi Komisijos padaliniai turėtų parengti ir įgyvendinti tinkamas priemones, o siekiant užtikrinti efektyvumą ir veiksmingumą, IT saugumo priemonės, skirtos ryšių ir informacinėms sistemoms apsaugoti, turėtų būti koordinuojamos Komisijos mastu;

(9) prieigos prie informacijos taisyklės ir procedūros, kuriomis užtikrinamas IT saugumas, įskaitant IT saugumo incidentų valdymą, turėtų būti proporcingos grėsmei Komisijai ar jos darbuotojams ir atitikti Europos Parlamento ir Tarybos reglamente (EB) Nr. 45/2001 [1] dėl asmenų apsaugos Sąjungos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo nustatytus principus ir būti nustatytos atsižvelgiant į profesinės paslapties principą, kaip numatyta SESV 339 straipsnyje;

[1] 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (OL L 8, 2001 1 12, p. 1).

(10) ryšių ir informacinių sistemų, kuriose tvarkoma ES įslaptinta informacija (ESĮI), neskelbtina neįslaptinta informacija ir neįslaptinta informacija, politika ir taisyklės turi visiškai atitikti Komisijos sprendimus (ES, Euratomas) 2015/443 ([1]) ir (ES, Euratomas) 2015/444 ([2]);

(11) Komisija turi peržiūrėti ir atnaujinti nuostatas dėl Komisijos naudojamų ryšių ir informacinių sistemų saugumo;

(12) todėl Komisijos sprendimas C(2006) 3602 turėtų būti panaikintas,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas ir taikymo sritis

1. Šis sprendimas taikomas visoms ryšių ir informacinėms sistemoms (RIS), kurias Komisija turi, įsigyja, valdo arba naudoja, taip pat toms, kurios naudojamos Komisijos vardu, ir visam Komisijos tų sistemų naudojimui.

2. Šiuo sprendimu nustatomi tų RIS saugumo pagrindiniai principai, tikslai, organizavimas ir su juo susijusios pareigos, taikomi visų pirma Komisijos padaliniams, kurie turi, perka, valdo arba naudoja RIS, įskaitant vidaus IT paslaugų teikėjo teikiamas RIS. Kai RIS pagal dvišalį susitarimą arba sutartį su Komisija teikia, turi, valdo arba ja naudojasi išorės šalis, susitarimo arba sutarties sąlygos turi atitikti šį sprendimą.

3. Šis sprendimas taikomas visiems Komisijos padaliniams ir vykdomosioms įstaigoms. Kai Komisijos RIS pagal dvišalį susitarimą su Komisija naudojasi kitos įstaigos ir institucijos, susitarimo sąlygos turi atitikti šį sprendimą.

4. Nepaisant konkrečių nuorodų dėl tam tikrų darbuotojų grupių, šis sprendimas taikomas Komisijos nariams, Komisijos darbuotojams, kuriems taikomi Europos Sąjungos pareigūnų tarnybos nuostatai (toliau – Tarnybos nuostatai) ir kitų tarnautojų įdarbinimo sąlygos (toliau – Įdarbinimo sąlygos) ([3]), į Komisiją deleguotiems nacionaliniams ekspertams (toliau – KNE) ([4]), išorės paslaugų teikėjams ir jų darbuotojams, stažuotojams ir visiems asmenims, turintiems prieigą prie RIS, kurioms taikomas šis sprendimas.

5. Šis sprendimas taikomas Europos kovos su sukčiavimu tarnybai (OLAF) tiek, kiek tai suderinama su Sąjungos teisės aktais ir Komisijos sprendimu 1999/352/EB, EAPB, Euratomas ([5]). Visų pirma, šiame sprendime numatytos priemonės, įskaitant instrukcijas, patikrinimus, tyrimus ir lygiavertes priemones, gali būti netaikomos Tarnybos RIS, kai tai nėra suderinama su jos tyrimų veiklos nepriklausomumu ir (arba) informacijos, kurią ji gavo vykdydama šią veiklą, konfidencialumu.

2 straipsnis

Apibrėžtys

Šiame sprendime vartojamų terminų apibrėžtys:

1) atskaitingas – atsakingas už veiksmus, sprendimus ir veiklos efektyvumą;

([1]) 2015 m. kovo 13 d. Komisijos sprendimas (ES, Euratomas) 2015/443 dėl saugumo Komisijoje (OL L 72, 2015 3 17, p. 41).
([2]) 2015 m. kovo 13 d. Komisijos sprendimas (ES, Euratomas) 2015/444 dėl ES įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių (OL L 72, 2015 3 17, p. 53).
([3]) Nustatytos 1968 m. vasario 29 d. Tarybos reglamentu (EEB, Euratomas, EAPB) Nr. 259/68, nustatančio Europos Bendrijų pareigūnų tarnybos nuostatus ir kitų tarnautojų įdarbinimo sąlygas (OL L 56, 1968 3 4, p. 1).
([4]) 2008 m. lapkričio 12 d. Komisijos sprendimas 1999/352/EB, kuriuo nustatomos nacionalinių ekspertų ir į profesinius mokymus siunčiamų nacionalinių ekspertų delegavimo į Komisiją taisyklės (C(2008) 6866 galutinis).
([5]) 1999 m. balandžio 28 d. Komisijos sprendimas dėl Europos kovos su sukčiavimu tarnybos (OLAF) įsteigimo (OL L 136, 1999 5 31, p. 20).

2) ES CERT – ES institucijų ir agentūrų kompiuterinių incidentų tyrimo tarnyba. Jos užduotis – padėti Europos institucijoms apsisaugoti nuo tyčinių ir piktavališkų išpuolių, kurie pakenktų jų IT išteklių vientisumui ir padarytų žalos ES interesams. ES CERT veiklos sritis apima prevenciją, aptikimą, reagavimą ir atkūrimą;

3) Komisijos padalinys – Komisijos generalinis direktoratas, tarnyba arba Komisijos nario kabinetas;

4) Komisijos saugumo institucija – institucija, kurios funkcijos nustatytos Sprendime (ES, Euratomas) 2015/444;

5) ryšių ir informacinė sistema (RIS) – bet kokia sistema, užtikrinanti galimybę tvarkyti informaciją elektroniniu būdu, įskaitant visas priemones, kurių reikia jos veikimui užtikrinti, taip pat infrastruktūrą, organizacinius, personalo ir informacijos išteklius. Ši apibrėžtis apima verslo taikomąsias programas, bendro naudojimo IT paslaugas, trečiųjų šalių teikiamas sistemas ir galutinių naudotojų įrenginius;

6) organizacinio valdymo taryba (OVT) – organas, vykdantis aukščiausio lygio organizacinio valdymo priežiūrą, susijusią su Komisijos veikla ir administravimu;

7) duomenų savininkas – asmuo, atsakingas už tam tikro RIS tvarkomo duomenų rinkinio apsaugą ir naudojimą;

8) duomenų rinkinys – informacija, skirta tam tikram verslo procesui arba tam tikrai Komisijos veiklai;

9) skubos procedūra – iš anksto nustatyti reagavimo į skubias situacijas metodai ir pareigos, kuriais siekiama išvengti didelio poveikio Komisijai;

10) informacijos saugumo politika – informacijos saugumo tikslai, kurie yra arba turi būti nustatyti, įgyvendinti ir kontroliuojami. Ji apima sprendimus (ES, Euratomas) 2015/444 ir (ES, Euratomas) 2015/443, bet jais neapsiriboja;

11) informacijos saugumo valdyba (ISV) – valdymo organas, padedantis organizacinio valdymo tarybai vykdyti su IT saugumu susijusias užduotis;

12) vidaus IT paslaugų teikėjas – Komisijos padalinys, teikiantis bendro naudojimo IT paslaugas;

13) IT saugumas, arba RIS saugumas – RIS ir jose tvarkomų duomenų rinkinių konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

14) IT saugumo gairės – rekomenduojamos, bet neprivalomos priemonės, kurios padeda užtikrinti, kad būtų laikomasi IT saugumo standartų, arba kuriomis remiamasi, kai nenustatyta taikomų standartų;

15) IT saugumo incidentas – bet koks įvykis, galintis neigiamai paveikti informacijos konfidencialumą, vientisumą ar RIS prieinamumą;

16) IT saugumo priemonė – techninė arba organizacinė priemonė, kuria siekiama sumažinti IT saugumo riziką;

17) IT saugumo poreikis – tiksliai ir nedviprasmiškai apibrėžti informacijos vieneto arba IT sistemos konfidencialumo, vientisumo ir prieinamumo lygiai, kuriais remiantis nustatomas reikiamas apsaugos lygis;

18) IT saugumo tikslas – teiginys apie ketinimą atremti nustatytas grėsmes ir (arba) užtikrinti atitiktį nustatytiems organizaciniams saugumo reikalavimams arba prielaidoms;

19) IT saugumo planas – IT saugumo priemonių, būtinų RIS saugumo poreikiams patenkinti, dokumentai;

20) IT saugumo politika – IT saugumo tikslai, kurie yra arba turi būti nustatyti, įgyvendinti ir kontroliuojami. Ji apima šį sprendimą ir jo įgyvendinimo taisykles;

21) IT saugumo reikalavimas – iš anksto nustatyta tvarka oficialiai įformintas IT saugumo poreikis;

22) IT saugumo rizika – galimas IT saugumo grėsmės poveikis RIS, kuris gali būti padarytas pasinaudojant silpnomis RIS vietomis. IT saugumo riziką apibūdina du veiksniai: 1) netikrumas, t. y. tikimybė, kad grėsmė IT saugumui galėtų sukelti nepageidaujamą įvykį, ir 2) poveikis, t. y. galimi tokio nepageidaujamo įvykio padariniai RIS;

23) IT saugumo standartai – specialios privalomos IT saugumo priemonės, padedančios užtikrinti ir remti IT saugumo politikos įgyvendinimą;

24) IT saugumo strategija – projektai ir veiksmai, kuriais siekiama Komisijos tikslų ir kurie turi būti sukurti, įgyvendinti ir kontroliuojami;

25) grėsmė IT saugumui – veiksnys, kuris gali lemti nepageidaujamą įvykį, per kurį būtų pakenkta RIS. Tokia grėsmė gali būti atsitiktinė arba tyčinė ir jai būdingi grėsmės elementai, galimi taikiniai ir puolimo būdai;

26) vietos informatikos saugumo pareigūnas (VISP) – pareigūnas, atsakingas už Komisijos padalinio IT saugumo ryšius;

27) terminai „asmens duomenys“, „asmens duomenų tvarkymas“, „duomenų valdytojas“ ir „asmens duomenų kaupimo rinkmenose sistema“ apibrėžti Reglamente (EB) Nr. 45/2001, ypač jo 2 straipsnyje;

28) informacijos tvarkymas – visos RIS funkcijos, susijusios su duomenų rinkiniais, įskaitant informacijos kūrimą, keitimą, rodymą, saugojimą, perdavimą, šalinimą ir archyvavimą. RIS informacijos tvarkymas gali būti teikiamas kaip naudotojams skirtų funkcijų rinkinys ir kaip kitoms RIS skirtų IT paslaugų rinkinys;

29) profesinė paslaptis – verslo informacijos, kuriai taikomas įpareigojimas saugoti profesinę paslaptį, visų pirma informacijos apie įmones, jų verslo ryšius ar išlaidų sudedamąsias dalis, kaip nustatyta SESV 339 straipsnyje, apsauga;

30) atsakingas – įpareigotas veikti ir priimti sprendimus, kad būtų pasiekti reikiami rezultatai;

31) saugumas Komisijoje – asmenų, turto ir informacijos saugumas Komisijoje, visų pirma fizinė asmenų ir turto neliečiamybė, informacijos, ryšių ir informacinių sistemų vientisumas, konfidencialumas ir prieinamumas, taip pat nevaržomas Komisijos veiklos vykdymas;

32) bendro naudojimo IT paslauga – su informacijos tvarkymu susijusi paslauga, kurią RIS teikia kitoms RIS;

33) sistemos savininkas – asmuo, bendrai atsakingas už RIS viešąjį pirkimą, kūrimą, integravimą, keitimą, naudojimą, techninę priežiūrą ir nurašymą;

34) naudotojas – asmuo, besinaudojantis RIS funkcijomis Komisijoje arba išorėje.

3 straipsnis

Komisijos IT saugumo principai

1. IT saugumas Komisijoje grindžiamas teisėtumo, skaidrumo, proporcingumo ir atskaitomybės principais.

2. Į IT saugumo klausimus turi būti atsižvelgiama nuo pat Komisijos RIS kūrimo ir įgyvendinimo pradžios. Tuo tikslu Informatikos generalinis direktoratas ir Žmogiškųjų išteklių ir saugumo generalinis direktoratas dalyvauja kuriant ir įgyvendinant RIS atitinkamose savo atsakomybės srityse.

3. Veiksmingu IT saugumu užtikrinamos šios tinkamo lygio savybės:

a) autentiškumas – užtikrinimas, kad informacija yra tikra ir gauta iš *bona fide* šaltinių;

b) prieinamumas – savybė, kuri reiškia, kad leidimą turintis subjektas, pateikęs prašymą, gali gauti informaciją ir ja naudotis;

c) konfidencialumas – savybė, kuri reiškia, kad informacija neatskleidžiama neturintiems leidimo asmenims, subjektams ar procesams;

d) vientisumas – savybė, kuri reiškia, kad apsaugomas išteklių ir informacijos tikslumas ir visuma;

e) nepaneigiamumas – galimybė įrodyti, kad veiksmas buvo atliktas ar įvykis įvyko, taigi to įvykio ar veiksmo negalima vėliau užginčyti;

f) asmens duomenų apsauga – tinkamų asmens duomenų apsaugos priemonių teikimas visapusiškai laikantis Reglamento (EB) Nr. 45/2001;

g) profesinė paslaptis – informacijos, kuriai taikomas profesinės paslapties įpareigojimas, visų pirma informacijos apie įmones, jų verslo ryšius ar išlaidų sudedamąsias dalis, kaip nustatyta SESV 339 straipsnyje, apsauga.

4. IT saugumas grindžiamas rizikos valdymo procesu. Šio proceso tikslas – nustatyti IT saugumo rizikos lygius ir saugumo priemones, kad tokia rizika proporcingomis sąnaudomis būtų sumažinta iki priimtino lygio.

5. Visos RIS turi būti identifikuotos, priskirtos sistemos savininkui ir inventorizuotos.

6. Visų RIS saugumo reikalavimai nustatomi remiantis jų saugumo poreikiais ir jose tvarkomos informacijos saugumo poreikiais. RIS, teikiančios paslaugas kitoms RIS, gali būti suprojektuotos taip, kad užtikrintų nustatytus saugumo poreikių lygius.

7. IT saugumo planai ir IT saugumo priemonės turi būti proporcingi RIS saugumo poreikiams.

Su šiais principais susiję procesai ir veikla išsamiau nustatomi įgyvendinimo taisyklėse.

2 SKYRIUS

ORGANIZAVIMAS IR PAREIGOS

4 straipsnis

Organizacinio valdymo taryba

Organizacinio valdymo taryba prisiima bendrą atsakomybę už visą IT saugumo valdymą visoje Komisijoje.

5 straipsnis

Informacijos saugumo valdyba (ISV)

1. Informacijos saugumo valdybai pirmininkauja Generalinio sekretoriaus pavaduotojas, atsakingas už Komisijos IT saugumo valdymą. ISV nariai yra Informatikos generalinio direktorato, Žmogiškųjų išteklių ir saugumo generalinio direktorato, Biudžeto generalinio direktorato ir, dvejų metų rotacijos principu, kitų keturių Komisijos padalinių, kuriems IT saugumas yra itin svarbus jų veiklos aspektas, atstovai, atstovaujantys įvairių Komisijos padalinių veiklos, technologijų ir saugumo interesams. Nariai yra vyresniosios vadovybės lygmens atstovai.

2. ISV padeda organizacinio valdymo tarybai vykdyti užduotis, susijusias su IT saugumu. ISV prisiima viso IT saugumo valdymo Komisijoje veiklos atsakomybę.

3. ISV rekomenduoja Komisijos tvirtintiną Komisijos IT saugumo politiką.

4. ISV du kartus per metus peržiūri valdymo ir IT saugumo klausimus, įskaitant didelius IT saugumo incidentus, ir pateikia ataskaitą organizacinio valdymo tarybai.

5. ISV stebi, kaip bendrai įgyvendinamas šis sprendimas, ir apžvalgos ataskaitą pateikia organizacinio valdymo tarybai.

6. Informatikos generalinio direktorato siūlymu ISV peržiūri ir tvirtina tęstinę IT saugumo strategiją ir stebi jos įgyvendinimą. Įgyvendinimo ataskaitą ISV pateikia organizacinio valdymo tarybai.

7. ISV stebi, vertina ir kontroliuoja organizacinio informacijos rizikos valdymo padėtį ir turi teisę prireikus nustatyti oficialius jo gerinimo reikalavimus.

Su šiomis pareigomis ir veikla susiję procesai išsamiau nustatomi įgyvendinimo taisyklėse.

6 straipsnis

Žmogiškųjų išteklių ir saugumo generalinis direktoratas

Žmogiškųjų išteklių ir saugumo generalinis direktoratas atlieka toliau išvardytas pareigas, susijusias su IT saugumu. Jis:

1) užtikrina IT saugumo politikos ir Komisijos informacijos saugumo politikos darną;

2) nustato leidimų saugant ir perduodant informaciją ryšių ir informacinėse sistemose naudoti šifravimo technologijas sistemą;

3) informuoja Informatikos generalinį direktoratą apie konkrečias grėsmes, kurios galėtų labai paveikti RIS ir jose tvarkomų duomenų rinkinių saugumą;

4) atlieka IT saugumo patikrinimus siekdamas įvertinti, ar Komisijos RIS atitinka saugumo politikos reikalavimus, ir praneša rezultatus ISV;

5) nustato prieigos prie Komisijos RIS iš išorės tinklų leidimų sistemą bei susijusias tinkamas saugumo taisykles ir glaudžiai bendradarbiaudamas su Informatikos generaliniu direktoratu parengia susijusius IT saugumo standartus ir gaires;

6) pasiūlo RIS paslaugų užsakymo principus ir taisykles, kuriais siekiama išlaikyti tinkamą informacijos saugumo kontrolę;

7) glaudžiai bendradarbiaudamas su Informatikos generaliniu direktoratu parengia su 6 straipsniu susijusius IT saugumo standartus ir gaires.

Su šiomis pareigomis ir veikla susiję procesai išsamiau nustatomi įgyvendinimo taisyklėse.

7 straipsnis

Informatikos generalinis direktoratas

Informatikos generalinis direktoratas atlieka toliau išvardytas pareigas, bendrai susijusias su IT saugumu Komisijoje. Jis:

1) glaudžiai bendradarbiaudamas su Žmogiškųjų išteklių ir saugumo generaliniu direktoratu, kad būtų užtikrintas IT saugumo politikos ir Komisijos informacijos saugumo politikos nuoseklumas, parengia IT saugumo standartus ir gaires, išskyrus numatytus 6 straipsnyje, ir pasiūlo juos ISV;

2) vertina visų Komisijos padalinių IT saugumo rizikos valdymo metodus, procesus ir rezultatus ir reguliariai teikia ataskaitas Informacijos saugumo valdybai;

3) pasiūlo tęstinę IT saugumo strategiją, kurią peržiūri ir patvirtina ISV, o vėliau tvirtina organizacinio valdymo taryba, ir programą, apimančią IT saugumo strategijos įgyvendinimo projektų planus ir veiklą;

4) stebi, kaip įgyvendinama Komisijos IT saugumo strategija, ir reguliariai teikia ataskaitas Informacijos saugumo valdybai;

5) stebi IT saugumo riziką bei ryšių ir informacinėse sistemose įgyvendinamas IT saugumo priemones ir reguliariai teikia ataskaitas Informacijos saugumo valdybai;

(6) Informacijos saugumo valdybai reguliariai teikia bendro šio sprendimo įgyvendinimo ir jo nuostatų laikymosi ataskaitas;

7) pasikonsultavęs su Žmogiškųjų išteklių ir saugumo generaliniu direktoratu, pareikalauja, kad sistemos savininkai imtųsi konkrečių IT saugumo priemonių, siekdami sumažinti IT saugumo riziką Komisijos ryšių ir informacinėms sistemoms;

8) užtikrina tinkamą Informatikos generalinio direktorato IT saugumo paslaugų katalogą, prieinamą sistemų ir duomenų savininkams, kad šie galėtų vykdyti su IT saugumu susijusias savo pareigas ir laikytis IT saugumo politikos ir standartų;

9) sistemų ir duomenų savininkams pateikia tinkamus dokumentus ir prireikus su jais konsultuojasi dėl pastarųjų teikiamų IT paslaugų IT saugumo priemonių įgyvendinimo, kad sudarytų sąlygas laikytis IT saugumo politikos ir padėtų sistemų savininkams valdyti IT saugumo riziką;

10) rengia reguliarius VISP tinklo posėdžius ir padeda VISP atlikti savo pareigas;

11) bendradarbiaudamas su Komisijos padaliniais nustato IT saugumo mokymo poreikius, koordinuoja mokymo programas ir glaudžiai bendradarbiaudamas su Žmogiškųjų išteklių generaliniu direktoratu rengia, įgyvendina ir koordinuoja informuotumo apie IT saugumą didinimo kampanijas;

12) užtikrina, kad sistemų savininkai, duomenų savininkai ir kiti IT saugumo funkcijų Komisijos padaliniuose vykdytojai būtų informuoti apie IT saugumo politiką;

13) informuoja Žmogiškųjų išteklių ir saugumo generalinį direktoratą apie konkrečias grėsmes IT saugumui, incidentus ir Komisijos IT saugumo politikos išimtis, apie kuriuos pranešė sistemos savininkai ir kurie gali labai paveikti saugumą Komisijoje;

14) vykdydamas savo IT paslaugų teikėjo funkciją pateikia Komisijai katalogą bendro naudojimo IT paslaugų, kurios užtikrina nustatytą saugumo lygį. Tai atliekama sistemingai vertinant, valdant ir stebint IT saugumo riziką, kad būtų įgyvendinamos saugumo priemonės, užtikrinančios galimybę pasiekti nustatytą saugumo lygį.

Susiję procesai ir pareigos išsamiau nustatomi įgyvendinimo taisyklėse.

8 straipsnis

Komisijos padaliniai

Dėl IT saugumo savo padalinyje kiekvienas Komisijos padalinio vadovas:

1) oficialiai paskiria kiekvienos RIS savininką, kuris yra pareigūnas arba laikinasis darbuotojas ir kuris bus atsakingas už tos RIS IT saugumą, ir oficialiai paskiria kiekvieno RIS tvarkomo duomenų rinkinio savininką, kuris turėtų priklausyti tam pačiam administraciniam vienetui, kuris yra duomenų rinkinių, kuriems taikomas Reglamentas (EB) Nr. 45/2001, duomenų valdytojas;

2) oficialiai paskiria VISP, kuris gali vykdyti pareigas nepriklausomai nuo sistemų savininkų ir duomenų savininkų. Gali būti paskirtas vieno arba kelių Komisijos padalinių VISP;

3) užtikrina, kad būtų atlikti tinkami IT saugumo rizikos vertinimai bei parengti ir įgyvendinti IT apsaugos planai;

4) užtikrina, kad Informatikos generaliniam direktoratui būtų reguliariai pateikiama IT saugumo rizikos ir priemonių santrauka;

5) padedamas Informatikos generalinio direktorato užtikrina, kad būtų įgyvendinti tinkami procesai, procedūros ir sprendimai, užtikrinantys efektyvų su savo RIS susijusių IT saugumo incidentų aptikimą, pranešimą apie juos ir jų pašalinimą;

6) susidarius IT saugumo ekstremaliajai situacijai pradeda skubos procedūrą;

7) yra labiausiai atskaitingas už IT saugumą, įskaitant sistemos valdytojo ir duomenų savininko pareigas;

8) prisiima riziką, susijusią su savo RIS ir duomenų rinkiniais;

9) sprendžia visus duomenų savininkų ir sistemos savininkų nesutarimus, o jei nesutarimai išlieka, perduoda klausimą spręsti ISV;

10) užtikrina, kad būtų įgyvendinti IT saugumo planai ir IT saugumo priemonės ir tinkamai išspręsti rizikos klausimai.

Su šiomis pareigomis ir veikla susiję procesai išsamiau nustatomi įgyvendinimo taisyklėse.

9 straipsnis

Sistemų savininkai

1. Sistemos savininkas atsako už RIS IT saugumą ir teikia ataskaitas Komisijos padalinio vadovui.

2. Dėl IT saugumo sistemos savininkas:

a) užtikrina, kad RIS būtų suderinama su IT saugumo politika;

b) užtikrina, kad RIS būtų tiksliai užregistruota atitinkamame inventoriaus apraše;

c) bendradarbiaudamas su duomenų savininkais ir konsultuodamasis su Informatikos generaliniu direktoratu įvertina kiekvienos RIS IT saugumo riziką ir nustato IT saugumo poreikius;

d) parengia saugumo planą, į kurį, kai tinkama, įtraukia išsamius įvertintos rizikos duomenis ir visas būtinas papildomas saugumo priemones;

e) įgyvendina atitinkamas IT saugumo priemones, proporcingas nustatytai IT saugumo rizikai, ir laikosi ISV patvirtintų rekomendacijų;

f) nustato visus priklausomybės nuo kitų RIS ir bendro naudojimo IT paslaugų atvejus ir, kai tinkama, įgyvendina saugumo priemones, remdamasis pasiūlytais tų RIS arba bendro naudojimo IT paslaugų saugumo lygiais;

g) valdo ir stebi IT saugumo riziką;

h) Komisijos padalinio vadovui reguliariai teikia savo RIS IT saugumo rizikos profilio ataskaitas ir Informatikos generaliniam direktoratui susijusios rizikos, rizikos valdymo veiklos ir saugumo priemonių, kurių buvo imtasi, ataskaitas;

i) konsultuojasi su atitinkamo Komisijos padalinio (-ių) VISP dėl IT saugumo aspektų;

j) naudotojams duoda nurodymus dėl RIS ir susijusių duomenų naudojimo, taip pat dėl jų pareigų, susijusių su RIS;

k) dėl kiekvienos RIS, kurioje naudojama šifravimo technologija, prašo Žmogiškųjų išteklių ir saugumo generalinio direktorato, veikiančio kaip šifravimo institucija, leidimo;

l) iš anksto konsultuojasi su Komisijos saugumo institucija dėl kiekvienos ES įslaptintos informacijos tvarkymo sistemos;

m) užtikrina, kad visų iššifravimo raktų atsarginės kopijos būtų laikomos sąlyginio deponavimo paskyroje. Užšifruoti duomenys iššifruojami tik gavus leidimą Žmogiškųjų išteklių ir saugumo generalinio direktorato nustatyta tvarka;

n) laikosi atitinkamų duomenų valdytojo (-ų) nurodymų dėl asmens duomenų apsaugos ir duomenų apsaugos taisyklių taikymo duomenų tvarkymo saugumui;

o) Informatikos generaliniam direktoratui praneša apie visas Komisijos IT saugumo politikos išimtis ir jas tinkamai pagrindžia;

p) Komisijos padalinio vadovui praneša apie visus neišsprendžiamus duomenų savininko ir sistemos savininko nesutarimus, prireikus atitinkamoms suinteresuotosioms šalims laiku praneša apie IT saugumo incidentus, atsižvelgdamas į jų sunkumą, kaip nustatyta 15 straipsnyje;

q) užtikrina, kad, kai sistemas teikia trečiosios šalys, į užsakomųjų paslaugų sutartis būtų įtrauktos tinkamos IT saugumo nuostatos ir kad apie trečiųjų šalių teikiamose RIS įvykusius IT saugumo incidentus būtų pranešama pagal 15 straipsnį;

r) užtikrina nustatytą ir dokumentais aiškiai pagrįstą RIS, kurios naudojamos teikiant bendro naudojimo IT paslaugas, saugumo lygį ir saugumo priemonių, kuriomis toje RIS užtikrinamas nustatytas saugumo lygis, įgyvendinimą.

3. Sistemos savininkai gali oficialiai perduoti kai kurias arba visas savo IT saugumo užduotis, tačiau išlieka atsakingi už savo RIS IT saugumą.

Su šiomis pareigomis ir veikla susiję procesai išsamiau nustatomi įgyvendinimo taisyklėse.

10 straipsnis

Duomenų savininkai

1. Duomenų savininkas už konkretaus duomenų rinkinio IT saugumą atsako Komisijos padalinio vadovui ir yra atskaitingas už duomenų rinkinio konfidencialumą, vientisumą ir prieinamumą.

2. Dėl to duomenų rinkinio duomenų savininkas:

a) užtikrina, kad visi duomenų rinkiniai, už kuriuos jis atsakingas, būtų tinkamai klasifikuoti pagal sprendimus (ES, Euratomas) 2015/443 ir (ES, Euratomas) 2015/444;

b) nustato informacijos saugumo poreikius ir apie juos informuoja atitinkamus sistemų savininkus;

c) dalyvauja atliekant RIS rizikos vertinimą;

d) Komisijos padalinio vadovui praneša apie visus neišsprendžiamus duomenų savininko ir sistemos savininko nesutarimus;

e) praneša apie IT saugumo incidentus, kaip numatyta 15 straipsnyje.

3. Duomenų savininkai gali oficialiai perduoti kai kurias arba visas savo IT saugumo užduotis, tačiau išlaiko šiame straipsnyje nustatytas savo pareigas.

Su šiomis pareigomis ir veikla susiję procesai išsamiau nustatomi įgyvendinimo taisyklėse.

11 straipsnis

Vietos informatikos saugumo pareigūnai (VISP)

Dėl IT saugumo VISP:

a) savo iniciatyva nustato ir informuoja sistemų savininkus, duomenų savininkus ir kitų IT saugumo pareigų vykdytojus Komisijos padalinyje (-iuose) apie IT saugumo politiką;

b) dalyvaudamas VISP tinklo veikloje palaiko ryšius su Informatikos generaliniu direktoratu su IT saugumu susijusiais klausimais Komisijos padalinyje (-iuose);

c) dalyvauja reguliariuose VISP susirinkimuose;

d) bendrai stebi informacijos saugumo rizikos valdymo procesą ir informacijos sistemos saugumo planų rengimą ir įgyvendinimą;

e) pataria duomenų savininkams, sistemos savininkams ir Komisijos padalinių vadovams su IT saugumu susijusiais klausimais;

f) bendradarbiauja su Informatikos generaliniu direktoratu skleidžiant geriausią IT saugumo praktiką ir siūlo specialias informuotumo didinimo ir mokymo programas;

g) Komisijos padalinio (-ių) vadovui (-ams) atsiskaito IT saugumo klausimais, nustato trūkumus ir tobulinimo priemones.

Su šiomis pareigomis ir veikla susiję procesai išsamiau nustatomi įgyvendinimo taisyklėse.

12 straipsnis

Naudotojai

1. Dėl IT saugumo naudotojai:

a) laikosi IT saugumo politikos ir sistemos savininko duotų kiekvienos RIS naudojimo nurodymų;

b) praneša apie IT saugumo incidentus, kaip numatyta 15 straipsnyje.

2. Jei Komisijos RIS naudojama pažeidžiant IT saugumo politiką ar nesilaikant sistemos savininko nurodymų, gali būti pradėta drausminė procedūra.

Su šiomis pareigomis ir veikla susiję procesai išsamiau nustatomi įgyvendinimo taisyklėse.

3 SKYRIUS

SAUGUMO REIKALAVIMAI IR ĮPAREIGOJIMAI

13 straipsnis

Šio sprendimo įgyvendinimas

1. Įgyvendinimo taisyklių ir susijusių standartų ir gairių priėmimas pagal 6 straipsnį priklausys nuo Komisijos sprendimo, kuriuo ji suteiks įgaliojimus už saugumo klausimus atsakingam Komisijos nariui.

2. Kitų su šiuo sprendimu susijusių įgyvendinimo taisyklių bei standartų ir gairių priėmimas priklausys nuo Komisijos sprendimo, kuriuo ji suteiks įgaliojimus už informatikos klausimus atsakingam Komisijos nariui.

3. Prieš priimant 1 ir 2 dalyse minėtas įgyvendinimo taisykles, standartus ir gaires, juos tvirtina ISV.

14 straipsnis

Įpareigojimas laikytis reikalavimų

1. IT saugumo politikoje išdėstytų nuostatų ir standartų laikytis privaloma.

2. Dėl IT saugumo politikos nuostatų ir standartų nesilaikymo gali būti taikomos drausminės priemonės pagal Sutartis, Tarnybos nuostatus ir Įdarbinimo sąlygas, taip pat darbo sutartyse numatytos sankcijos ir (arba) atliekami teisiniai veiksmai pagal nacionalinės teisės aktus.

3. Informatikos generaliniam direktoratui pranešama apie visas IT saugumo politikos išimtis.

4. Jeigu ISV nusprendžia, kad nuolat kyla nepriimtinas pavojus Komisijos RIS, Informatikos generalinis direktoratas, bendradarbiaudamas su sistemos savininku, pasiūlo ISV tvirtinti poveikio mažinimo priemones. Šios priemonės, be kita ko, gali būti sustiprintas stebėjimas ir pranešimas, paslaugų apribojimai ir atjungimas.

5. Prireikus ISV nustato privalomą patvirtintų poveikio mažinimo priemonių įgyvendinimą. ISV taip pat gali Žmogiškųjų išteklių ir saugumo generalinio direktorato generaliniam direktoriui rekomenduoti pradėti administracinį tyrimą. Informatikos generalinis direktoratas praneša ISV apie kiekvieną atvejį, kai nustatomas privalomas poveikio mažinimo priemonių taikymas.

Su šiomis pareigomis ir veikla susiję procesai išsamiau nustatomi įgyvendinimo taisyklėse.

15 straipsnis

IT saugumo incidentų valdymas

1. Informatikos generalinis direktoratas atsako už pagrindinį gebėjimą operatyviai reaguoti į IT saugumo incidentus Europos Komisijoje.

2. Žmogiškųjų išteklių ir saugumo generalinis direktoratas, kaip suinteresuotoji šalis, padedanti reaguoti į IT saugumo incidentus:

a) turi teisę gauti visų incidentų įrašų informacijos santrauką, o paprašęs – išsamius įrašus;

b) dalyvauja IT saugumo incidentų krizių valdymo grupės veikloje ir vykdant IT saugumo skubos procedūras;

c) atsako už ryšius su teisėsaugos ir žvalgybos tarnybomis;

d) atlieka kibernetinio saugumo teisminę ekspertizę pagal Sprendimo (ES, Euratomas) 2015/443 11 straipsnį;

e) sprendžia dėl poreikio pradėti oficialų tyrimą;

f) informuoja Informatikos generalinį direktoratą apie visus IT saugumo incidentus, kurie gali kelti pavojų kitoms RIS.

3. Informatikos generalinis direktoratas ir Žmogiškųjų išteklių ir saugumo generalinis direktoratas palaiko reguliarų ryšį, keičiasi informacija ir koordinuoja saugumo incidentų valdymą, ypač visų IT saugumo incidentų, dėl kurių gali reikėti atlikti oficialų tyrimą.

4. Kai tinkama, vykdant incidentų valdymo procesą ir dalijantis žiniomis su kitomis ES institucijomis ir agentūromis, kurioms gali būti daromas poveikis, gali būti panaudojamos Europos institucijų, įstaigų ir agentūrų Kompiuterinių incidentų tyrimo tarnybos (ES CERT) incidentų koordinavimo tarnybos.

5. Su IT saugumo incidentu susijusių sistemų savininkai:

a) nedelsdami praneša savo Komisijos padalinio vadovui, Informatikos generaliniam direktoratui ir Žmogiškųjų išteklių generaliniam direktoratui, VISP ir, kai tinkama, duomenų savininkui apie visus didelius IT saugumo incidentus, ypač tuos, kurie yra susiję su duomenų konfidencialumo pažeidimu;

b) bendradarbiauja su atitinkamomis Komisijos institucijomis dėl pranešimo apie incidentus, reagavimo į juos ir padėties ištaisymo ir vykdo tų institucijų nurodymus.

6. Naudotojai laiku praneša apie visus faktinius ir įtariamus IT saugumo incidentus atitinkamai IT pagalbos tarnybai.

7. Duomenų savininkai laiku praneša apie visus faktinius ir įtariamus IT saugumo incidentus atitinkamai reagavimo į IT saugumo incidentus tarnybai.

8. Informatikos generalinis direktoratas, padedamas kitų prisidedančių suinteresuotųjų šalių, atsako už kiekvieno Komisijos ryšių ir informacinėse sistemose, kurios nėra trečiųjų šalių teikiamos sistemos, nustatytų IT saugumo incidentų valdymą.

9. Informatikos generalinis direktoratas, vadovaudamasis principu „būtina žinoti“, apie IT saugumo incidentus informuoja paveiktus Komisijos padalinius, VISP ir, kai tinkama, ES CERT.

10. Informatikos generalinis direktoratas ISV reguliariai teikia didelių IT saugumo incidentų, paveikiančių Komisijos RIS, ataskaitas.

11. Atitinkamo VISP prašymu jam suteikiama prieiga prie IT saugumo incidentų registracijos įrašų, susijusių su Komisijos padalinio RIS.

12. Įvykus dideliam IT saugumo incidentui Informatikos generalinis direktoratas veikia kaip krizės valdymo kontaktinis punktas, koordinuojantis IT saugumo incidentų krizių valdymo grupes.

13. Susidarius ekstremaliajai situacijai Informatikos generalinio direktorato generalinis direktorius gali nuspręsti pradėti IT saugumo skubos procedūrą. Informatikos generalinis direktoratas parengia skubos procedūras, kurias po to tvirtina ISV.

14. Informatikos generalinis direktoratas teikia skubos procedūrų vykdymo ataskaitas ISV ir paveiktų Komisijos padalinių vadovams.

Su šiomis pareigomis ir veikla susiję procesai išsamiau nustatomi įgyvendinimo taisyklėse.

4 SKYRIUS

BAIGIAMOSIOS NUOSTATOS

16 straipsnis

Skaidrumas

Apie šį sprendimą informuojami Komisijos darbuotojai ir visi asmenys, kuriems jis taikomas, ir jis paskelbiamas *Europos Sąjungos oficialiajame leidinyje*.

17 straipsnis

Ryšys su kitais teisės aktais

Šio sprendimo nuostatos nedaro poveikio Sprendimo (ES, Euratomas) 2015/443, Sprendimo (ES, Euratomas) 2015/444, Reglamento (EB) Nr. 45/2001, Europos Parlamento ir Tarybos reglamento (EB) Nr. 1049/2001 ([1]), Komisijos sprendimo 2002/47/EB, EAPB, Euratomas ([2]), Europos Parlamento ir Tarybos reglamento (ES, Euratomas) Nr. 883/2013 ([3]) ir Sprendimo 1999/352/EB, EAPB, Euratomas taikymui.

18 straipsnis

Panaikinimas ir pereinamojo laikotarpio priemonės

2006 m. rugpjūčio 16 d. Sprendimas C(2006) 3602 panaikinamas.

Įgyvendinimo taisyklės ir saugumo standartai, priimti pagal Sprendimo C(2006) 3602 10 straipsnį, galioja tiek, kiek jie neprieštarauja šiam sprendimui, ir tol, kol nebus pakeisti įgyvendinimo taisyklėmis ir standartais, numatytais priimti pagal šio sprendimo 13 straipsnį. Visos nuorodos į Sprendimo C(2006) 3602 10 straipsnį laikomos nuorodomis į šio sprendimo 13 straipsnį.

19 straipsnis

Įsigaliojimas

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

Priimta Briuselyje 2017 m. sausio 10 d.

Komisijos vardu

Pirmininkas

Jean-Claude JUNCKER

([1]) 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).

([2]) 2002 m. sausio 23 d. Komisijos sprendimas 2002/47/EB, EAPB, Euratomas, iš dalies keičiantis jos darbo tvarkos taisykles (OL L 21, 2002 1 24, p. 23).

([3]) 2013 m. rugsėjo 11 d. Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) Nr. 883/2013 dėl Europos kovos su sukčiavimu tarnybos (OLAF) atliekamų tyrimų ir kuriuo panaikinami Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1073/1999 ir Tarybos reglamentas (Euratomas) Nr. 1074/1999 (OL L 248, 2013 9 18, p. 1).