KOMISIJOS SPRENDIMAS (ES, Euratomas) 2018/559

2018 m. balandžio 6 d.

dėl Sprendimo (ES, Euratomas) 2017/46 dėl Europos Komisijos ryšių ir informacinių sistemų saugumo 6 straipsnio įgyvendinimo taisyklių nustatymo

EUROPOS KOMISIJA,

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

atsižvelgdama į Europos atominės energijos bendrijos steigimo sutartį,

atsižvelgdama į 2017 m. sausio 10 d. Komisijos sprendimą (ES, Euratomas) 2017/46 dėl Europos Komisijos ryšių ir informacinių sistemų saugumo ([1]), ypač į jo 6 straipsnį,

kadangi:

(1) priėmus Sprendimą (ES, Euratomas) 2017/46 atsirado poreikis Komisijai peržiūrėti, atnaujinti ir konsoliduoti įgyvendinimo taisykles, susijusias su panaikintu Komisijos sprendimu C(2006) 3602 dėl Komisijos naudojamų ryšių ir informacinių sistemų saugumo;

(2) griežtai laikantis vidaus taisyklių ir procedūrų, už saugumą atsakingas Komisijos narys pagal Sprendimo (ES, Euratomas) 2017/46 ([2]) 13 straipsnį įgaliotas parengti įgyvendinimo taisykles;

(3) todėl Sprendimu C(2006) 3602 nustatytos įgyvendinimo taisyklės turėtų būti panaikintos,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas ir taikymo sritis

1. Šio sprendimo dalykas ir taikymo sritis nustatyti Sprendimo (ES, Euratomas) 2017/46 1 straipsnyje.

2. Šio sprendimo nuostatos taikomos visoms ryšių ir informacinėms sistemoms (RIS). Tačiau šiame sprendime apibrėžtos pareigos netaikomos RIS, kuriose tvarkoma ES įslaptinta informacija. Atitinkamas su tomis sistemomis susijusias pareigas pagal Komisijos sprendimą (ES, Euratomas) 2015/444 ([3]) nustato sistemos savininkas ir Komisijos saugumo institucija.

3. Šio sprendimo 2 skyriuje apžvelgiamas su IT saugumu susijusio organizavimo ir pareigų praktinis įgyvendinimas. Šio sprendimo 3 skyriuje apžvelgiami su Sprendimo (ES, Euratomas) 2017/46 6 straipsniu susiję procesai.

2 straipsnis

Apibrėžtys

Šiame sprendime vartojamų terminų apibrėžtys nustatytos Sprendimo (ES, Euratomas) 2017/46 2 straipsnyje. Kitų šiame sprendime vartojamų terminų apibrėžtys:

1. Kriptografijos patvirtinimo institucija (KPI) – institucija, kurios funkciją prisiima Žmogiškųjų išteklių ir saugumo generaliniam direktoratui pavaldi Komisijos saugumo institucija;

([1]) OL L 6, 2017 1 11, p. 40.
([2]) 2017 m. lapkričio 8 d. Komisijos sprendimas C(2017) 7428 *final*, kuriuo suteikiami įgaliojimai priimti įgyvendinimo taisykles, standartus ir gaires, susijusius su Europos Komisijos ryšių ir informacinių sistemų saugumu
([3]) 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).

2. jungtis su išorės tinklu – bet kokia Komisijos vidaus tinklo ir bet kurio kito tinklo, įskaitant internetą, elektroninių ryšių jungtis. Šis terminas neapima trečiųjų šalių tinklų, teikiamų pagal sutartį kaip Komisijos vidaus tinklo dalių;

3. raktų deponavimas – procedūra, pagal kurią, užtikrinant pareigų atskyrimą, kriptografijos raktų kopijas saugo viena ar daugiau atskirų šalių, kad būtų galima raktus atkurti, jei naudojama kopija būtų prarasta. Siekiant užtikrinti, kad nė viena šalis neturėtų viso rakto, jis gali būti padalytas į dvi ar daugiau dalių, kurias saugo skirtingos šalys;

4. RASCI – santrumpa, reiškianti atsakomybės priskyrimą pagal šiuos priskyrimo rodiklius:

a) atsakingas (R) – įpareigotas veikti ir priimti sprendimus, kad būtų pasiekti reikiami rezultatai;

b) atskaitingas (A) – atsakingas už veiksmus, sprendimus ir veiklos efektyvumą;

c) pagalbinis (S) – įpareigotas bendradarbiauti su atsakingu asmeniu, kad būtų įvykdyta užduotis;

d) (su kuriuo) konsultuojamasi (C) – jo prašoma patarimo ar nuomonės;

e) (kuris) informuojamas (I) – jam nuolat teikiama aktuali informacija.

2 SKYRIUS

ORGANIZAVIMAS IR PAREIGOS

3 straipsnis

Funkcijos ir pareigos

Su šio sprendimo 4–8 straipsniais susijusios funkcijos ir pareigos pagal RASCI modelį apibrėžtos 1 priede.

4 straipsnis

Derėjimas su Komisijos informacijos saugumo politika

1. Žmogiškųjų išteklių ir saugumo generalinis direktoratas peržiūri Komisijos IT saugumo politiką ir susijusius standartus bei gaires, siekdamas užtikrinti, kad jie atitiktų Komisijos bendrąją saugumo politiką, visų pirma Sprendimą (ES, Euratomas) 2015/443 ([1]) ir Komisijos sprendimą (ES, Euratomas) 2015/444.

2. Kitų Komisijos padalinių prašymu Žmogiškųjų išteklių ir saugumo generalinis direktoratas gali peržiūrėti jų IT saugumo politiką ar kitus IT saugumo dokumentus, kad būtų užtikrintas jų suderinamumas su Komisijos informacijos saugumo politika. Atitinkamo Komisijos padalinio vadovas užtikrina, kad visi nesuderinamumo klausimai būtų išspręsti.

3. Vykdydamas informacijos saugumo užtikrinimo pareigą, Žmogiškųjų išteklių ir saugumo generalinis direktoratas bendradarbiauja su Informatikos generaliniu direktoratu, siekdamas užtikrinti, kad IT saugumo procesuose būtų visiškai atsižvelgta į Sprendime (ES, Euratomas) 2015/443, visų pirma jo 3 ir 9 straipsniuose, nustatytą klasifikaciją ir saugumo principus.

3 SKYRIUS

IT SAUGUMO PROCESAI

5 straipsnis

Šifravimo technologijos

1. Šifravimo technologijos ES įslaptintai informacijai (ESĮI) apsaugoti naudojamos pagal Sprendimo (ES, Euratomas) 2015/444 nuostatas.

2. Sprendimus dėl šifravimo technologijų naudojimo ne ESĮI duomenims apsaugoti priima kiekvienos RIS savininkas, atsižvelgdamas į riziką, kuri turėtų būti sumažinta naudojant šifravimą, ir į riziką, kylančią dėl jo naudojimo.

3. Visus šifravimo technologijų naudojimo atvejus turi iš anksto patvirtinti KPI, nebent šifravimas naudojamas tik ne ESĮI duomenų konfidencialumui apsaugoti tranzito metu ir jam naudojami standartiniai tinklo ryšio protokolai.

([1]) 2015 m. kovo 13 d. Komisijos sprendimas (ES, Euratomas) 2015/443 dėl saugumo Komisijoje (OL L 72, 2015 3 17, p. 41).

4. Išskyrus šio straipsnio 3 dalyje nurodytą išimtį, Komisijos padaliniai užtikrina visų iššifravimo raktų atsarginių kopijų deponavimą, kad būtų galima atkurti saugomus duomenis, jei nebūtų galima pasinaudoti iššifravimo raktu. Šifruotų duomenų atkūrimas naudojant atsarginius iššifravimo raktus atliekamas tik gavus leidimą KPI nustatyta tvarka.

5. Prašymai leisti naudoti šifravimo technologijas oficialiai įforminami dokumentais ir juose nurodomi išsamūs RIS duomenys, duomenys, kuriuos reikia apsaugoti, numatomos naudoti technologijos ir susijusios saugumo veiklos procedūros. Šiuos prašymus pasirašo sistemos savininkas.

6. Prašymus leisti naudoti šifravimo technologijas pagal paskelbtus standartus ir dokumentus įvertina KPI.

6 straipsnis

IT saugumo patikrinimai

1. Žmogiškųjų išteklių ir saugumo generalinis direktoratas vykdo saugumo patikrinimus, kad nustatytų, ar IT saugumo priemonės atitinka Komisijos IT saugumo politiką, ir patikrintų šių kontrolės priemonių vientisumą.

2. Žmogiškųjų išteklių ir saugumo generalinis direktoratas IT saugumo patikrinimą gali atlikti:

a) savo iniciatyva;

b) Informacijos saugumo valdybos prašymu;

c) sistemos savininko prašymu;

d) po saugumo incidento arba

e) nustačius, kad esama didelės rizikos konkrečiai sistemai.

3. Duomenų savininkai, prieš pradėdami saugoti savo informaciją ryšių ir informacinėje sistemoje, gali prašyti atlikti IT saugumo patikrinimą.

4. Patikrinimo rezultatai dokumentuojami oficialioje ataskaitoje, kurioje nurodomi nustatyti faktai ir pateikiamos RIS suderinamumo su IT saugumo politika gerinimo rekomendacijos; ataskaita pateikiama sistemos savininkui, o jos kopija – vietos informatikos saugumo pareigūnui. Žmogiškųjų išteklių ir saugumo generalinis direktoratas Informacijos saugumo valdybai praneša apie svarbius klausimus ir teikia rekomendacijas.

5. Žmogiškųjų išteklių ir saugumo generalinis direktoratas stebi rekomendacijų įgyvendinimą.

6. Jei reikia, IT saugumo patikrinimai apima sistemos savininkui tiek vidaus, tiek išorės teikėjų teikiamų paslaugų, patalpų ir įrangos patikrinimą.

7 straipsnis

Prieiga iš išorės tinklų

1. Žmogiškųjų išteklių ir saugumo generalinis direktoratas nustato taisykles Komisijos RIS ir išorės tinklų tarpusavio prieigos leidimo standarte.

2. Taisyklėse skiriami įvairūs jungčių su išorės tinklais tipai ir nustatomos atitinkamos kiekvieno tipo jungties saugumo taisyklės, įskaitant tai, ar būtina gauti atitinkamos institucijos leidimą prisijungti, kaip nurodyta šio straipsnio 4 dalyje.

3. Jei reikia, leidimas išduodamas remiantis oficialiu prašymo ir leidimo procesu. Leidimas galioja tam tikrą laiką ir turi būti gautas iki jungties aktyvinimo.

4. Žmogiškųjų išteklių ir saugumo generalinis direktoratas bendrai atsakingas už prisijungimo prašymų tenkinimą, tačiau pagal Sprendimo (ES, Euratomas) 2015/443 17 straipsnio 3 dalį ir šio straipsnio 8 dalyje nurodytomis sąlygomis gali savo nuožiūra perduoti atsakomybę už tam tikrų tipų jungtis.

5. Leidimus suteikiantis subjektas gali nustatyti papildomus saugumo reikalavimus kaip būtiną leidimo prisijungti sąlygą, kad apsaugotų Komisijos RIS ir tinklus nuo neteisėtos prieigos ar kitų saugumo pažeidimų rizikos.

6. Pagrindinis tinklų paslaugų teikėjas Komisijai yra Informatikos generalinis direktoratas. Bet kuris kitas Komisijos padalinys, ketinantis naudoti tinklą, kurį teikia ne Informatikos generalinis direktoratas, pirmiausia turi gauti Informacijos saugumo valdybos sutikimą. Komisijos padalinys prašymą naudoti tokį tinklą pagrindžia dokumentais ir įrodo, jog tinklo kontrolė yra pakankama, kad atitiktų gaunamos ir siunčiamos informacijos srautų kontrolės reikalavimus.

7. RIS savininkas nustato tos RIS prieigos iš išorės saugumo reikalavimus ir, padedamas vietos informatikos saugumo pareigūno, užtikrina, kad būtų įgyvendintos tinkamos jos saugumo užtikrinimo priemonės.

8. Įgyvendinamos tinklo išorės jungčių saugumo priemonės grindžiamos būtinumo žinoti ir mažiausių teisių principais, kurie užtikrina, kad asmenys gautų tik savo oficialioms pareigoms Komisijoje vykdyti būtiną informaciją ir prieigos teises.

9. Visos tinklo išorės jungtys filtruojamos ir stebimos siekiant aptikti galimus saugumo pažeidimus.

10. Kai jungtys kuriamos siekiant užtikrinti galimybę naudoti RIS kaip užsakomąją paslaugą, leidimas duodamas su sąlyga, kad 8 straipsnyje aprašytos procedūros rezultatas bus teigiamas.

8 straipsnis

RIS kaip užsakomosios paslaugos

1. Taikant šį sprendimą laikoma, kad RIS teikiama kaip užsakomoji paslauga, kai ji teikiama pagal rangos sutartį su trečiąja šalimi, kurioje numatyta, kad RIS laikoma ne Komisijos patalpose. Tai apima atskiras arba daugybines RIS, taip pat kitas užsakomąsias IT paslaugas, duomenų centrus ne Komisijos patalpose ir Komisijos duomenų rinkinių tvarkymą išorės tarnybose.

2. Užsakant RIS kaip užsakomąją paslaugą į tvarkomos informacijos neskelbtinumą arba klasifikavimą atsižvelgiama taip:

a) RIS, kuriose tvarkoma ESĮI, akredituojamos pagal Sprendimą (ES, Euratomas) 2015/444 ir dėl jų iš anksto konsultuojamasi su Komisijos Saugumo akreditavimo institucija. Sistemos, kuriose tvarkoma ESĮI, negali būti teikiamos kaip užsakomoji paslauga;

b) RIS, kurioje tvarkoma ne ESĮI, savininkas įgyvendina proporcingas priemones, kuriomis sprendžiami saugumo užtikrinimo klausimai laikantis atitinkamų teisinių įpareigojimų arba informacijos neskelbtinumo reikalavimų ir atsižvelgiant į riziką, susijusią su užsakomosiomis paslaugomis. Žmogiškųjų išteklių ir saugumo generalinis direktoratas gali nustatyti papildomų reikalavimų;

c) užsakomuosiuose programinės įrangos kūrimo projektuose atsižvelgiama į kuriamo programinio kodo ir jį kuriant naudojamų bandomųjų duomenų neskelbtinumą.

3. Be Sprendimo (ES, Euratomas) 2017/46 3 straipsnyje nustatytų principų, RIS, teikiamoms kaip užsakomosioms paslaugoms, taikomi šie principai:

a) užsakomųjų paslaugų susitarimai turi būti tokie, kad būtų išvengta priklausomybės nuo konkrečių tiekėjų;

b) užsakomųjų paslaugų saugumo susitarimais turi būti kuo labiau sumažinta trečiosios šalies darbuotojų galimybė gauti arba keisti Komisijos informaciją;

c) trečiosios šalies darbuotojai, kurie turi prieigą prie RIS, teikiamos kaip užsakomosios paslaugos, pasirašo konfidencialumo susitarimą;

d) RIS kaip užsakomosios paslaugos teikimas nurodomas ryšių ir informacinių sistemų inventorizacijos apraše.

4. Sistemos savininkas, dalyvaujant duomenų savininkui:

a) įvertina riziką ir parengia jos dokumentus;

b) nustato atitinkamus saugumo reikalavimus;

c) konsultuojasi su visų kitų sujungtų RIS savininkais, siekdamas užtikrinti, kad būtų atsižvelgta į jų saugumo reikalavimus;

d) užtikrina, kad tinkami saugumo reikalavimai ir teisės būtų įtraukti į užsakomųjų paslaugų sutartį;

e) įvykdo visus kitus reikalavimus, nustatytus išsamioje procedūroje, kaip nurodyta šio straipsnio 8 dalyje.

Šie veiksmai turi būti užbaigti prieš pasirašant sutartį ar kitą susitarimą dėl vienos ar daugiau RIS teikimo kaip užsakomųjų paslaugų.

5. Sistemų savininkai valdo su užsakomosiomis paslaugomis susijusią riziką visą RIS gyvavimo ciklą, kad būtų užtikrinta atitiktis nustatytiems saugumo reikalavimams.

6. Sistemų savininkai užtikrina, kad trečiųjų šalių rangovai būtų įpareigoti nedelsiant pranešti Komisijai apie visus IT saugumo incidentus, turinčius poveikio RIS, teikiamai Komisijai kaip užsakomajai paslaugai.

7. Sistemos savininkas atsakingas už tai, kad RIS, užsakomųjų paslaugų sutartis ir saugumo susitarimai atitiktų Komisijos informacijos saugumo ir IT saugumo taisyklių reikalavimus.

8. Žmogiškųjų išteklių ir saugumo generalinis direktoratas pagal 10 straipsnį nustato išsamų standartą, susijusį su pareigomis ir veikla, nustatytomis 1–7 dalyse.

4 SKYRIUS

KITOS IR BAIGIAMOSIOS NUOSTATOS

9 straipsnis

Skaidrumas

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

10 straipsnis

Standartai

1. Šio sprendimo nuostatos prireikus išsamiau išdėstomos standartuose ir (arba) gairėse, priimamuose pagal Sprendimą (ES, Euratomas) 2017/46 ir pagal Sprendimą C(2017) 7428. IT saugumo standartuose ir gairėse pateikiama išsami informacija apie šias įgyvendinimo taisykles ir Sprendimą (ES, Euratomas) 2017/46 konkrečiose saugumo srityse pagal standarto ISO 27001:2013 A priedą. Tie standartai ir gairės grindžiami geriausia praktika ir parenkami taip, kad tiktų Komisijos IT aplinkai.

2. Prireikus standartai rengiami pagal standarto ISO 27001:2013 A priedą šiose srityse:

1) informacijos saugumo organizavimas;

2) žmogiškųjų išteklių saugumas;

3) turto valdymas;

4) prieigos kontrolė;

5) kriptografija;

6) fizinis ir aplinkos saugumas;

7) veiklos saugumas;

8) ryšių saugumas;

9) sistemų įsigijimas, plėtojimas ir techninė priežiūra;

10) santykiai su tiekėjais;

11) informacijos saugumo incidentų valdymas;

12) veiklos tęstinumo valdymo informacijos saugumo aspektai;

13) atitiktis reikalavimams.

3. Prieš priimant standartus, nurodytus šio straipsnio 1 ir 2 dalyje, juos tvirtina Informacijos saugumo valdyba.

4. Su šio sprendimo taikymo sritimi susijusios Sprendimo C(2006) 3602 įgyvendinimo taisyklės panaikinamos.

5. Pagal 2006 m. rugpjūčio 16 d. Sprendimą C(2006) 3602 priimti standartai ir gairės, jei jie neprieštarauja šioms įgyvendinimo taisyklėms, išlieka galioti tol, kol bus panaikinti arba pakeisti standartais ar gairėmis, kurie turi būti priimti pagal Sprendimo (ES, Euratomas) 2017/46 13 straipsnį.

11 straipsnis

Įsigaliojimas

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

Priimta Briuselyje 2018 m. balandžio 6 d.

Komisijos vardu
Pirmininko pavedimu
Günther OETTINGER
Komisijos narys

PRIEDAS

FUNKCIJOS IR PAREIGOS (RASCI)

Pagal RASCI modelį funkcijos subjektams priskiriamos pagal šias santrumpas:

a) R – atsakingas

b) A – atskaitingas

c) S – pagalbinis

d) C – (su kuriuo) konsultuojamasi

e) I – (kuris) informuojamas

Procesas / Funkcija	Informacijos saugumo valdyba	Žmogiškųjų išteklių ir saugumo generalinis direktoratas	Komisijos padaliniai	Sistemos savininkas	Duomenų savininkas	Vietos informatikos saugumo pareigūnas	Informatikos generalinis direktoratas	Rangovai
Derinimas su Komisijos informacijos saugumo politika		**R/A**	**S**				**S**	
Šifravimo technologijos		**C**	**A**	**R**	**I**	**C**		
IT saugumo patikrinimai	**I**	**A/R**		**S**	**I**	**I**	**S**	
Prieiga iš išorės tinklų	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Ryšių ir informacinių sistemų užsakomosios paslaugos		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] Visi Komisijos padaliniai, išskyrus Informatikos generalinį direktoratą, dėl vidaus tinklų naudojimo konsultuojasi su Informacijos saugumo valdyba.

[2] Ryšių ir informacinės sistemos, teikiamos kaip užsakomosios paslaugos, savininkas yra atsakingas, o su bet kurios kitos ryšių ir informacinės sistemos, su kuria ji jungiasi, savininku konsultuojamasi.