KOMISIJAS LĒMUMS (ES, Euratom) 2018/559

(2018. gada 6. aprīlis)

par Lēmuma (ES, Euratom) 2017/46 par komunikācijas un informācijas sistēmu drošību Eiropas Komisijā 6. panta īstenošanas noteikumu paredzēšanu

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 249. pantu,

ņemot vērā Eiropas Atomenerģijas kopienas dibināšanas līgumu,

ņemot vērā Komisijas 2017. gada 10. janvāra Lēmumu (ES, Euratom) 2017/46 par komunikācijas un informācijas sistēmu drošību Eiropas Komisijā ([1]) un jo īpaši tā 6. pantu,

tā kā:

(1) Lēmuma (ES, Euratom) 2017/46 pieņemšanas rezultātā ir vajadzīgs, lai Komisija pārskatītu, atjauninātu un konsolidētu īstenošanas noteikumus, kas saistīti ar atcelto Komisijas Lēmumu C(2006) 3602 par Komisijas lietoto komunikāciju un informācijas sistēmu drošību.

(2) Par drošību atbildīgais Komisijas loceklis, pilnībā ievērojot iekšējos noteikumus un procedūras, ir ticis pilnvarots noteikt īstenošanas noteikumus saskaņā ar Lēmuma (ES, Euratom) 2017/46 13. pantu ([2]).

(3) Tādēļ Lēmuma C(2006) 3602 īstenošanas noteikumi būtu jāatceļ,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. NODAĻA

VISPĀRĪGI NOTEIKUMI

1. pants

Priekšmets un darbības joma

1. Šā lēmuma priekšmets un darbības joma ir paredzēti Lēmuma (ES, Euratom) 2017/46 1. pantā.

2. Šā lēmuma noteikumi attiecas uz visām komunikācijas un informācijas sistēmām (KIS). Tomēr šajā lēmumā noteiktie pienākumi neattiecas uz KIS, kurās rīkojas ar ES klasificēto informāciju. Saskaņā ar Komisijas Lēmumu (ES, Euratom) 2015/444 ([3]) attiecīgos pienākumus saistībā ar minētajām sistēmām nosaka sistēmas īpašnieks un Komisijas Drošības iestāde.

3. Šā lēmuma 2. nodaļā ir sniegts pārskats par tās organizācijas un pienākumu praktisko īstenošanu, kas ir saistīti ar IT drošību. Šā lēmuma 3. nodaļā ir sniegts pārskats par procesiem, kas saistīti ar Lēmuma (ES, Euratom) 2017/46 6. pantu.

2. pants

Definīcijas

Šajā lēmumā piemēro Lēmuma (ES, Euratom) 2017/46 2. pantā noteiktās definīcijas. Šajā lēmumā izmanto arī šādas definīcijas:

1) "kriptogrāfijas apstiprinājuma iestāde" (KAI) ir funkcija, ko uzņemas Komisijas Drošības iestāde, kura darbojas Cilvēkresursu un drošības ģenerāldirektora pakļautībā;

([1]) OV L 6, 11.1.2017., 40. lpp.
([2]) Komisijas 2017. gada 8. novembra Lēmums C(2017) 7428 final, ar kuru piešķir pilnvaras pieņemt īstenošanas noteikumus, standartus un pamatnostādnes saistībā ar komunikācijas un informācijas sistēmu drošību Eiropas Komisijā.
([3]) Komisijas 2015. gada 13. marta Lēmums (ES, Euratom) 2015/444 par drošības noteikumiem ES klasificētas informācijas aizsardzībai (OV L 72, 17.3.2015., 53. lpp.).

2) "ārējais tīkla savienojums" ir elektronisko sakaru savienojums starp Komisijas iekšējo tīklu un jebkādu citu tīklu, tostarp internetu. Šī definīcija neattiecas uz trešo personu tīkliem, kurus nodrošina saskaņā ar līgumu un kuri ir daļa no Komisijas iekšējā tīkla;

3) "šifratslēgas uzticējumglabāšana" ir šifratslēgu, kuras sastāv no vienas vai vairākām atsevišķām daļām, kopiju glabāšanas procedūra, kas nodrošina pienākumu nošķiršanu, lai darba kopijas zaudēšanas gadījumā tās varētu atgūt. Šifratslēgas var būt sadalītas divās vai vairākās daļās, katru no kurām glabā cita puse, lai nodrošinātu, ka nevienas puses rīcībā nav visas šifratslēgas;

4) "*RASCI*" ir saīsinājums, ar ko apzīmē atbildības sadalījumu, balstoties uz šādiem indikatoriem:

   a) "*responsible*" (R, atbildīgs) ir tāds, kam ir pienākums rīkoties un pieņemt lēmumus vajadzīgā iznākuma sasniegšanai;

   b) "*accountable*" (A, saucams pie atbildības) ir tāds, kas ir atbildīgs par darbībām, lēmumiem un rezultātiem;

   c) "*supports*" (S, sniedz atbalstu) ir tāds, kam ir pienākums sadarboties ar personu, kura ir atbildīga par uzdevuma paveikšanu;

   d) "*consulted*" (C, tiek uzklausīts) ir tāds, kam lūdz ieteikumu vai atzinumu;

   e) "*informed*" (I, ir informēts) ir tāds, kuram regulāri tiek sniegta aktuāla attiecīgā informācija.

2. NODAĻA

ORGANIZĀCIJA UN PIENĀKUMI

3. pants

Lomas un pienākumi

Lomas un pienākumi saistībā ar šā lēmuma 4. līdz 8. pantu ir definētas pielikumā atbilstoši *RASCI* modelim.

4. pants

Salāgošana ar Komisijas informācijas drošības politiku

1. Cilvēkresursu un drošības ģenerāldirektorāts pārskata Komisijas IT drošības politiku un ar to saistītos standartus un pamatnostādnes, lai nodrošinātu, ka tie atbilst Komisijas vispārējās drošības politikai, jo īpaši Komisijas Lēmumam (ES, Euratom) 2015/443 ([1]) un Lēmumam (ES, Euratom) 2015/444.

2. Pēc citu Komisijas struktūrvienību pieprasījuma Cilvēkresursu un drošības ģenerāldirektorāts var pārskatīt to IT drošības politiku vai citus IT drošības dokumentus, lai nodrošinātu to saskanību ar Komisijas informācijas drošības politiku. Attiecīgās Komisijas struktūrvienības vadītājs nodrošina, ka tiek novērstas visas neatbilstības.

3. Par informācijas drošību atbildīgais Cilvēkresursu un drošības ģenerāldirektorāts sadarbojas ar Informātikas ģenerāldirektorātu, lai nodrošinātu, ka IT drošības procesos tiek pilnībā ņemta vērā Lēmumā (ES, Euratom) 2015/443 un jo īpaši tā 3. un 9. pantā paredzētā drošības klasifikācija un principi.

3. NODAĻA

IT DROŠĪBAS PROCESI

5. pants

Šifrēšanas tehnoloģijas

1. Izmantojot šifrēšanas tehnoloģijas ES klasificētās informācijas ("ESKI") aizsardzībai, ievēro Lēmuma (ES, Euratom) 2015/444 noteikumus.

2. Lēmumus par šifrēšanas tehnoloģiju izmantošanu tādu datu aizsardzībai, kas nav ESKI, pieņem katras KIS sistēmas īpašnieks, ņemot vērā gan riskus, kurus paredzēts mazināt, izmantojot šifrēšanu, gan šifrēšanas radītos riskus.

3. Jebkādai šifrēšanas tehnoloģiju izmantošanai ir vajadzīgs KAI iepriekšējs apstiprinājums, izņemot gadījumus, kad šifrēšana tiek izmantota vienīgi tādu tranzītā esošu datu konfidencialitātes aizsardzībai, kas nav ESKI, un tiek izmantoti standarta tīkla sakaru protokoli.

([1]) Komisijas 2015. gada 13. marta Lēmums (ES, Euratom) 2015/443 par drošību Komisijā (OV L 72, 17.3.2015., 41. lpp.).

4. Izņemot šā panta 3. punktā minēto izņēmuma gadījumu, Komisijas struktūrvienības nodrošina, ka visu atšifrēšanas atslēgu rezerves kopijas tiek glabātas atbilstoši šifratslēgas uzticējumglabāšanai, lai gadījumā, ja atšifrēšanas atslēga nav pieejama, noglabātos datus varētu atgūt. Šifrētu datu atgūšanu, izmantojot atšifrēšanas atslēgu rezerves kopijas, veic tikai tad, kad ir saņemta atļauja saskaņā ar KAI definēto standartu.

5. Šifrēšanas tehnoloģiju izmantošanas apstiprinājumu pieprasījumus oficiāli dokumentē, un tajos norāda ziņas par KIS un aizsargājamajiem datiem, tehnoloģijām, kuras paredzēts izmantot, un saistītajām drošības darba procedūrām. Šādus apstiprinājumu pieprasījumus paraksta sistēmas īpašnieks.

6. Šifrēšanas tehnoloģiju izmantošanas apstiprinājumu pieprasījumus KAI izvērtē atbilstoši publicētajiem standartiem un prasībām.

6. pants

IT drošības inspekcijas

1. Cilvēkresursu un drošības ģenerāldirektorāts inspicē IT drošību, lai pārliecinātos, vai IT drošības pasākumi atbilst Komisijas IT drošības politikai, un pārbaudītu šo kontroles pasākumu integritāti.

2. Cilvēkresursu un drošības ģenerāldirektorāts var veikt IT drošības inspekciju:

a) pēc savas iniciatīvas;

b) pēc Informācijas drošības koordinācijas padomes ("IDKP") pieprasījuma;

c) pēc sistēmas īpašnieka pieprasījuma;

d) pēc drošības incidenta; vai

e) pēc tam, kad tika konstatēts augsts risks konkrētai sistēmai.

3. Datu īpašnieki var pieprasīt IT drošības inspekciju pirms informācijas saglabāšanas kādā no KIS.

4. Inspekciju rezultātus dokumentē oficiālā ziņojumā sistēmas īpašniekam un tajā ietver atzinumus un ieteikumus par to, kā uzlabot KIS atbilstību IT drošības politikai; ziņojuma kopiju nosūta vietējam informātikas drošības speciālistam ("*LISO*"). Cilvēkresursu un drošības ģenerāldirektorāts par būtiskām problēmām un ieteikumiem ziņo IDKP.

5. Cilvēkresursu un drošības ģenerāldirektorāts uzrauga ieteikumu īstenošanu.

6. Attiecīgā gadījumā IT drošības inspekcijas ietver to pakalpojumu, telpu un iekārtu inspicēšanu, ko gan iekšēji, gan ārēji pakalpojumu sniedzēji nodrošina sistēmas īpašniekam.

7. pants

Piekļuve no ārējiem tīkliem

1. Cilvēkresursu un drošības ģenerāldirektorāts paredz noteikumus šajā jautājumā, nosakot standartu, atbilstoši kuram piešķir atļauju piekļuvei starp Komisijas KIS un ārējiem tīkliem.

2. Noteikumos nošķir dažādus ārējo tīklu savienojumu veidus un paredz pienācīgus drošības noteikumus katram savienojuma veidam, tostarp to, vai savienojumam ir nepieciešama iepriekšēja atļauja no attiecīgās iestādes, kā tas paredzēts šā panta 4. punktā.

3. Vajadzības gadījumā atļauju piešķir oficiālā pieprasījuma un apstiprinājuma procedūrā. Apstiprinājums ir derīgs konkrētu laiku, un to iegūst pirms savienojuma aktivizēšanas.

4. Cilvēkresursu un drošības ģenerāldirektorātam ir vispārēja atbildība par pieprasījumu apstiprināšanu, taču tas pēc saviem ieskatiem var deleģēt atbildību par dažu savienojumu veidu atļaušanu atbilstoši Lēmuma (ES, Euratom) 2015/443 17. panta 3. punktam, ja ir izpildīti 8. punktā paredzētie nosacījumi.

5. Lai aizsargātu Komisijas KIS un tīklus pret riskiem saistībā ar neatļautu piekļuvi vai citiem drošības prasību pārkāpumiem, atļaujas piešķīrēja struktūra var noteikt papildu drošības prasības kā priekšnoteikumu apstiprinājuma saņemšanai.

6. Informātikas ģenerāldirektorāts ir tīklu pakalpojumu standarta nodrošinātājs Komisijā. Jebkurai citai Komisijas struktūrvienībai, kas ekspluatē tādu tīklu, kuru nenodrošina Informātikas ģenerāldirektorāts, vispirms ir jāsaņem IDKP piekrišana. Šī Komisijas struktūrvienība dokumentē pieprasījuma ekonomisko pamatojumu un pierāda, ka tīkla kontroles pasākumi ir pietiekami, lai izpildītu prasības attiecībā uz ienākošo un izejošo informācijas plūsmu kontroli.

7. KIS sistēmas īpašnieks nosaka drošības prasības ārējai piekļuvei konkrētajai KIS un ar *LISO* atbalstu nodrošina, ka tiek īstenoti pienācīgi pasākumi tās drošības aizsardzībai.

8. Attiecībā uz ārējo tīklu savienojumiem īstenojamie drošības pasākumi balstās uz vajadzības pēc informācijas un mazāko privilēģiju principu, kas nodrošina, ka personas saņem tikai to informāciju un piekļuves tiesības, kuras tām ir vajadzīgas, lai pildītu savus dienesta pienākumus Komisijā.

9. Visus ārējo tīklu savienojumus filtrē un uzrauga nolūkā atklāt iespējamus drošības prasību pārkāpumus.

10. Ja savienojumi ir izveidoti, lai KIS nodotu ārpakalpojumā, atļauju piešķir tikai tad, ja ir veiksmīgi pabeigta 8. pantā noteiktā procedūra.

8. pants

KIS nodošana ārpakalpojumā

1. Šajā lēmumā KIS uzskata par nodotu ārpakalpojumā, ja to nodrošina, pamatojoties uz tādu līgumu ar trešo personu, saskaņā ar kuru KIS izvieto ārpus Komisijas telpām. Tas ietver atsevišķu vai vairāku KIS vai citu IT pakalpojumu, datu centru nodošanu ārpakalpojumā ārpus Komisijas telpām un rīkošanos ar Komisijas datu kopumiem, ko veic ārpakalpojumu sniedzēji.

2. Nododot KIS ārpakalpojumā, ņem vērā informācijas, ar kuru rīkojas, sensitivitāti vai klasifikāciju, proti:

a) KIS, kurās rīkojas ar ESKI, ir jābūt akreditētām atbilstoši Lēmumam (ES, Euratom) 2015/444, un pirms tam ir jākonsultējas ar Komisijas Drošības akreditācijas iestādi (DAI). Sistēmas, kurās rīkojas ar ESKI, nedrīkst nodot ārpakalpojumā;

b) tādas KIS sistēmas īpašnieks, kurā rīkojas ar informāciju, kas nav ESKI, īsteno samērīgus pasākumus, lai risinātu drošības vajadzības atbilstoši attiecīgajiem juridiskajiem pienākumiem un informācijas sensitivitātei, ņemot vērā ar nodošanu ārpakalpojumā saistītos riskus. Cilvēkresursu un drošības ģenerāldirektorāts var noteikt papildu prasības;

c) nododot ārpakalpojumā izstrādes projektus, ņem vērā izstrādātā koda un izstrādes laikā izmantoto testdatu sensitivitāti.

3. Ārpakalpojumā nodotām KIS papildus Lēmuma (ES, Euratom) 2017/46 3. pantā paredzētajiem principiem piemēro arī šādus principus:

a) kārtību nodošanai ārpakalpojumā izstrādā tā, lai novērstu atkarību no konkrētiem pakalpojumu sniedzējiem;

b) drošības pasākumi attiecībā uz nodošanu ārpakalpojumā minimizē trešo personu darbinieku iespējas piekļūt Komisijas informācijai vai pārveidot to;

c) trešo personu darbiniekiem, kam ir piekļuve ārpakalpojumā nodotām KIS, ir jāparaksta vienošanās par konfidencialitāti;

d) KIS nodošana ārpakalpojumā ir jānorāda KIS inventarizācijas dokumentos.

4. Sistēmas īpašnieks kopā ar datu īpašnieku:

a) novērtē un dokumentē ar nodošanu ārpakalpojumā saistītos riskus;

b) nosaka attiecīgas drošības prasības;

c) apspriežas ar visu pārējo saistīto KIS sistēmu īpašniekiem, lai nodrošinātu, ka ir ietvertas viņu drošības prasības;

d) nodrošina, ka ārpakalpojuma līgumā ir ietvertas pienācīgas drošības prasības un tiesības;

e) izpilda citas prasības, kas noteiktas šā panta 8. punktā minētajā sīki izstrādātajā procedūrā.

Minētās darbības ir jāpabeidz, pirms tiek parakstīts līgums vai citas vienošanās par vienas vai vairāku KIS nodošanu ārpakalpojumā.

5. Sistēmu īpašnieki pārvalda ar nodošanu ārpakalpojumā saistītos riskus visā KIS darbības laikā, lai izpildītu noteiktās drošības prasības.

6. Sistēmu īpašnieki nodrošina, ka trešām personām, kas ir līgumslēdzējas, ir pienākums nekavējoties ziņot Komisijai par visiem IT drošības incidentiem, kas ietekmē Komisijas ārpakalpojumā nodotās KIS.

7. Sistēmas īpašnieks ir atbildīgs par to, lai nodrošinātu, ka KIS, ārpakalpojuma līgums un drošības pasākumi atbilst Komisijas noteikumiem par informācijas drošību un IT drošību.

8. Cilvēkresursu un drošības ģenerāldirektorāts atbilstoši 10. pantam nosaka sīki izstrādātu standartu saistībā ar 1.–7. punktā izklāstītajiem pienākumiem un darbībām.

4. NODAĻA

DAŽĀDI NOTEIKUMI UN NOBEIGUMA NOTEIKUMI

9. pants

Pārredzamība

Šo lēmumu dara zināmu Komisijas darbiniekiem un visām personām, uz ko tas attiecas, un publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

10. pants

Standarti

1. Vajadzības gadījumā šā lēmuma noteikumus sīkāk izstrādā standartos un/vai pamatnostādnēs, kas jāpieņem atbilstoši Lēmumam (ES, Euratom) 2017/46 un Lēmumam C(2017) 7428. IT drošības standartos un pamatnostādnēs paredz sīkāku informāciju par šiem īstenošanas noteikumiem un Lēmumu (ES, Euratom) 2017/46 attiecībā uz specifiskām drošības jomām saskaņā ar ISO 27001:2013 A pielikumu. Minētie standarti un pamatnostādnes balstās uz nozares paraugpraksi, un tiek atlasīti tie, kas ir piemēroti Komisijas IT videi.

2. Vajadzības gadījumā standartus izstrādā atbilstoši ISO 27001:2013 A pielikumam šādās jomās:

1) informācijas drošības organizācija;

2) cilvēkresursu drošība;

3) aktīvu pārvaldība;

4) piekļuves kontrole;

5) kriptogrāfija;

6) fiziskā un vides drošība;

7) darbības drošība;

8) komunikāciju drošība;

9) sistēmas iegāde, attīstība un uzturēšana;

10) attiecības ar piegādātājiem;

11) informācijas drošības incidentu pārvaldība;

12) darbības nepārtrauktības pārvaldības informācijas drošības aspekti;

13) atbilstība.

3. IDKP apstiprina šā panta 1. un 2. punktā minētos standartus pirms to pieņemšanas.

4. Ar šo atceļ Lēmuma C(2006) 3602 īstenošanas noteikumus, kas saistīti ar šā lēmuma darbības jomu.

5. Saskaņā ar 2006. gada 16. augusta Lēmumu C(2006) 3602 pieņemtie standarti un pamatnostādnes paliek spēkā, ciktāl tie nav pretrunā šiem īstenošanas noteikumiem, līdz tos atceļ vai aizstāj ar standartiem vai pamatnostādnēm, kas jāpieņem saskaņā ar Lēmuma (ES, Euratom) 2017/46 13. pantu.

11. pants

Stāšanās spēkā

Šis lēmums stājas spēkā divdesmitajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī.*

Briselē, 2018. gada 6. aprīlī

Komisijas
un tās priekšsēdētāja vārdā –
Komisijas loceklis
Günther OETTINGER

PIELIKUMS

LOMAS UN PIENĀKUMI (*RASCI*)

Atbilstoši *RASCI* modelim lomas struktūrvienībām tiek piešķirtas, izmantojot šādus saīsinājumus:

a) R – *Responsible* (atbildīgs);

b) A – *Accountable* (saucams pie atbildības);

c) S – *Supporting* (atbalstu sniedzošs);

d) C – *Consulted* (uzklausīts);

e) I – *Informed* (informēts).

Process \ Loma	IDKP	Cilvēkresursu un drošības ĢD (Drošības direktorāts)	Komisijas departamenti	Sistēmas īpašnieks	Datu īpašnieks	LISO	Informātikas ĢD	Līgumslēdzēji
Salāgošana ar Komisijas informācijas drošības politiku		**R/A**	**S**				**S**	
Šifrēšanas tehnoloģijas		**C**	**A**	**R**	**I**	**C**		
IT drošības inspekcijas	**I**	**A/R**		**S**	**I**	**I**	**S**	
Piekļuve no ārējiem tīkliem	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
KIS nodošana ārpakalpojumā		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] Visām Komisijas struktūrvienībām, izņemot Informātikas ģenerāldirektorātu, ir jākonsultējas ar IDKP saistībā ar iekšējo tīklu darbību.

[2] Ārpakalpojumā nododamās KIS sistēmas īpašnieks ir atbildīgais, un ir jākonsultējas ar visu to KIS sistēmu īpašniekiem, ar kuriem ir starpsavienota ārpakalpojumā nododamā KIS.