LĒMUMI

KOMISIJAS LĒMUMS (ES, Euratom) 2017/46

(2017. gada 10. janvāris)

par komunikācijas un informācijas sistēmu drošību Eiropas Komisijā

EIROPAS KOMISIJA,

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

ņemot vērā Eiropas Atomenerģijas kopienas dibināšanas līgumu,

tā kā:

(1) Komisijas komunikācijas un informācijas sistēmas ir Komisijas funkcionēšanas sastāvdaļa, un IT drošības incidenti var nopietni ietekmēt Komisijas darbību, kā arī trešās personas, ieskaitot privātpersonas, uzņēmumus un dalībvalstis.

(2) Komisijas komunikācijas un informācijas sistēmu konfidencialitātei, veselumam un pieejamībai un tajās apstrādātajai informācijai draud visdažādākās briesmas. Starp tām minami negadījumi, kļūdas, tīši uzbrukumi un dabas parādības, un tas viss uzskatāms par risku darbībai.

(3) Komunikācijas un informācijas sistēmām jāsaņem tādas pakāpes aizsardzība, kādu prasa draudošā riska iespējamība, ietekme un raksturs.

(4) IT drošībai Komisijā jānodrošina, lai Komisijas KIS aizsargā tajās apstrādāto informāciju un leģitīmo lietotāju kontrolē vajadzības gadījumā darbojas, kā pienākas.

(5) Komisijas IT drošības politika būtu jāīsteno saskanīgi ar Komisijas politiku drošības jomā.

(6) Cilvēkresursu un drošības ģenerāldirektorāta Drošības direktorāts vispārīgi atbild par drošību Komisijā, ko pārzina un par ko atbild par drošību atbildīgais Komisijas loceklis.

(7) Komisijas pieejā būtu jāņem vērā ES politiskās iniciatīvas un tiesību normas par tīklu un informācijas drošību, rūpniecības standartiem un labāko praksi, lai ievērotu visus attiecīgos tiesību aktus un dotu vietu sadarbspējai un saderībai.

(8) Komisijas struktūrvienībām, kas atbild par komunikācijas un informācijas sistēmām, būtu jāizstrādā un jāīsteno piemēroti pasākumi, un visā Komisijā būtu koordinējami IT drošības pasākumi, kas aizsargā komunikācijas un informācijas sistēmas.

(9) Informācijas piekļuves noteikumiem un procedūrām IT drošības sakarā, ieskaitot rīcību IT drošības incidentos, būtu jābūt proporcionāliem Komisijai un tās personālam draudošajām briesmām un jāatbilst Eiropas Parlamenta un Padomes Regulas (EK) Nr. 45/2001 [1] principiem, kas attiecas uz privātpersonu aizsardzību Savienības iestādēs un struktūrās notiekošās personas datu apstrādes aspektā un šādu datu brīvu apriti, un jārēķinās ar LESD 339. pantā noteikto dienesta noslēpuma glabāšanas principu.

[1] Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regula (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti (OV L 8, 12.1.2001., 1. lpp.).

(10) Politikai un normām, kas attiecas uz komunikāciju un informācijas sistēmām, kuras apstrādā ES klasificētu informāciju, sensitīvu neklasificētu informāciju un neklasificētu informāciju, ir pilnīgi jāsaskan ar Komisijas Lēmumiem (ES, Euratom) 2015/443 ([1]) un (ES, Euratom) 2015/444 ([2]).

(11) Ir vajadzīgs, lai Komisija pārskata un atjaunina noteikumus par Komisijas lietoto komunikāciju un informācijas sistēmu drošību.

(12) Tāpēc Komisijas Lēmums C(2006) 3602 būtu jāatceļ,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. NODAĻA

VISPĀRĪGI NOTEIKUMI

1. pants

Priekšmets un darbības joma

1. Šis lēmums attiecas uz visām komunikācijas un informācijas sistēmām (KIS), kas pieder vai ir iegādātas Komisijai, tiek apsaimniekotas un darbinātas Komisijā vai tās uzdevumā, un minēto KIS jebkādu Komisijas izmantojumu.

2. Šajā lēmumā ir noteikti pamatprincipi, mērķi, organizācija un pienākumi, kas attiecas uz minēto KIS drošību, galvenokārt Komisijas struktūrvienībās, kam pieder vai ir iegādātas, tiek apsaimniekotas vai darbinātas KIS, ieskaitot KIS, ko piegādā ārējs IT pakalpojumu sniedzējs. Ja KIS piegādā, apsaimnieko vai darbina ārēja persona vai KIS tai pieder saskaņā ar divpusēju vienošanos vai līgumu ar Komisiju, vienošanās vai līguma noteikumiem ir jāatbilst šim lēmumam.

3. Šis lēmums attiecas uz visām Komisijas struktūrvienībām un izpildaģentūrām. Ja Komisijas KIS izmanto citas struktūras un iestādes saskaņā ar divpusēju vienošanos ar Komisiju, vienošanās noteikumiem ir jāatbilst šim lēmumam.

4. Neatkarīgi no īpašiem apzīmējumiem attiecīgām personāla grupām, šis lēmums attiecas uz Komisijas locekļiem, Komisijas darbiniekiem, kuriem piemēro Eiropas Savienības Civildienesta noteikumus ("Civildienesta noteikumi") un Savienības Pārējo darbinieku nodarbināšanas kārtību ("PDNK") ([3]), uz Komisiju norīkotiem valstu ekspertiem ("NVE") ([4]), ārējiem pakalpojumu sniedzējiem un to personālu, stažieriem un ikvienu privātpersonu, kam ir piekļuve KIS šā lēmuma darbības jomā.

5. Šis lēmums attiecas uz Eiropas Biroju krāpšanas apkarošanai (*OLAF*), cik tas ir saderīgi ar Savienības tiesību aktiem un Komisijas Lēmumu 1999/352/EK, EOTK, Euratom ([5]). Konkrēti, šajā lēmumā noteiktie pasākumi, iekaitot norādījumus, pārbaudes, pieprasījumus u. tml., var neattiekties uz Biroja KIS, kas tas nav saderīgs ar Biroja izmeklēšanas funkcijas neatkarību un/vai Biroja funkcijas izpildē savāktās informācijas konfidencialitāti.

2. pants

Definīcijas

Šajā lēmumā lietoti šādi jēdzieni:

1) "saucams pie atbildības" nozīmē būt atbildīgam par darbībām, lēmumiem un rezultātiem;

([1]) Komisijas 2015. gada 13. marta Lēmums (ES, Euratom) 2015/443 par drošību Komisijā (OV L 72, 17.3.2015., 41. lpp.).
([2]) 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.).
([3]) Noteikts ar Padomes 1968. gada 29. februāra Regulu (EEK, Euratom, EOTK) Nr. 259/68, ar ko nosaka Eiropas Kopienu Civildienesta noteikumus un Pārējo darbinieku nodarbināšanas kārtību, kā arī paredz īpašus Komisijas ierēdņiem uz laiku piemērojamus pasākumus (Pārējo darbinieku nodarbināšanas kārtība) (OV L 56, 4.3.1968., 1. lpp.).
([4]) Komisijas 2008. gada 12. novembra Lēmums, ar ko nosaka valsts ekspertu norīkošanu uz Komisiju un valsts ekspertu profesionālās apmācības noteikumus (C(2008) 6866 galīgā redakcija).
([5]) Komisijas 1999. gada 28. aprīļa Lēmums 1999/352/EK, EOTK, Euratom, ar ko izveido Eiropas Biroju krāpšanas apkarošanai (*OLAF*) (OV L 136, 31.5.1999., 20. lpp.).

2) "*CERT-EU*" ir ES iestāžu un aģentūru datorapdraudējumu reaģēšanas vienība. Tās uzdevums ir atbalstīt Eiropas iestādes aizsargāties pret tīšiem un ļaunprātīgiem uzbrukumiem, kuri var iedragāt IT aktīvu veselumu un kaitēt ES interesēm. *CERT-EU* darbībās ietilpst profilakse, atklāšana, reaģēšana un atkope;

3) "Komisijas struktūrvienība" ir Komisijas ģenerāldirektorāts vai dienests vai Komisijas locekļa kabinets;

4) "Komisijas drošības iestāde" norāda uz Lēmumā (ES, Euratom) 2015/444 noteikto lomu;

5) "Komunikācijas un informācijas sistēma" jeb "KIS" ir katra sistēma, kas ļauj rīkoties ar informāciju elektroniskā formā, ieskaitot visus aktīvus, kas vajadzīgi tās darbībai, kā arī infrastruktūras, organizācijas, personāla un informācijas resursus. Šis jēdziens aptver darba lietotnes, kopīgotus IT pakalpojumus, ārpakalpojumā nodotās sistēmas un galalietotāju ierīces;

6) "iestādes valde" (IV) veic pārraudzību iestādes vadības pašā augstākajā līmenī saistībā ar Komisijas darbības un administratīvajiem jautājumiem;

7) "datu īpašnieks" ir privātpersona, kas atbild par KIS apstrādātu specifisku datu kopumu aizsardzības un lietošanas nodrošināšanu;

8) "datu kopa" ir informācijas kopums, kas kalpo noteiktam Komisijas darba procesam vai darbībai;

9) "ārkārtas procedūra" ir iepriekš noteiktu metožu un pienākumu kopums reaģēšanai ārkārtas situācijās ar nolūku novērst lielāku ietekmi uz Komisiju;

10) "informācijas drošības politika" ir informācijas drošības mērķu kopums, kuri tiek noteikti, īstenoti un pārbaudīti vai kuriem tas ir jādara. Tā aptver Lēmumus (ES, Euratom) 2015/444 un (ES, Euratom) 2015/443, bet ne tikai tos;

11) "Informācijas drošības koordinācijas padome" (IDKP) ir pārvaldības struktūra, kas atbalsta iestādes valdi ar IT drošību saistītajos uzdevumos;

12) "iekšējs IT pakalpojumu sniedzējs" ir Komisijas struktūrvienība, kas sniedz koplietojamus IT pakalpojumus;

13) "IT drošība" jeb "KIS drošība" ir KIS un to apstrādājamo datu kopu konfidencialitātes, veseluma un pieejamības saglabāšana;

14) "IT drošības vadlīnijas" ir ieteicamie, bet brīvprātīgi veicamie pasākumi, kas palīdz atbalstīt IT drošības standartus vai kalpo par atsauci, kad trūkst piemērojama standarta;

15) "IT drošības incidents" ir atgadījums, kas varētu negatīvi ietekmēt KIS konfidencialitāti, veselumu vai pieejamību;

16) "IT drošības pasākums" ir tehnisks vai organizatorisks pasākums, kas domāts IT drošības riska mazināšanai;

17) "IT drošības vajadzības" ir precīzi, nepārprotami definētas konfidencialitātes, veselumu un pieejamības pakāpes, ko saista ar informāciju vai IT sistēmu ar mērķi noteikt vajadzīgās aizsardzības pakāpi;

18) "IT drošības mērķis" ir deklarēts nodoms pretoties noteiktiem apdraudējumiem un/vai apmierināt noteiktas organizatoriskas drošības prasības vai pieņēmumus;

19) "IT drošības plāns" ir kādas KIS IT drošības vajadzību apmierināšanai vajadzīgie IT drošības pasākumu dokumenti;

20) "IT drošības politika" ir informācijas drošības mērķu kopums, kuri tiek noteikti, īstenoti un pārbaudīti vai ar kuriem tas ir jādara. Tā aptver šo lēmumu un tā īstenošanas noteikumus;

21) "IT drošības prasības" ir iepriekšēji noteiktā procesā formalizētas IT drošības vajadzības;

22) "IT drošības risks" nozīmē ietekmi uz KIS, ko neaizsargātības dēļ varētu atstāt apdraudējums IT drošībai. Pašu IT drošības risku raksturo divi elementi: 1) nenoteiktība, t. i., varbūtība, ka IT drošības apdraudējums izraisīs nevēlamu atgadījumu, 2) ietekme, t. i., sekas, ko tāds nevēlams atgadījums var atstāt KIS;

23) "IT drošības normas" ir īpaši obligāti IT drošības pasākumi, kas palīdz panākt IT drošības politikas izpildi un to atbalsta;

24) "IT drošības stratēģija" ir Komisijas mērķu sasniegšanai plānoto nosakāmo, īstenojamo un pārbaudāmo projektu un darbību kopums;

25) "apdraudējums IT drošībai" ir faktors, kas spēj izraisīt nevēlamu atgadījumu, kurš var beigties ar nodarījumu KIS. Apdraudējumi var būt netīši vai tīši, un tiem ir raksturīgi dažādi apdraudējuma elementi, iespējamie mērķi un uzbrukuma metodes;

26) "vietējais informātikas drošības speciālists" jeb *LISO* ir ierēdnis, kura pienākumos ir Komisijas struktūrvienības saziņa sakarā ar IT drošību;

27) "personas dati", "personas datu apstrāde", "datu pārzinis" un "personas datu kartotēka" nozīmē to pašu, ko Regulā (EK) Nr. 45/2001, sevišķi tās 2. pantā;

28) "informācijas apstrāde" ir visas KIS funkcijas, kas attiecas uz datu kopām, ieskaitot informācijas radīšanu, pārveidošanu, parādīšanu, glabāšanu, pārraidīšanu, dzēšanu un arhivēšanu. Informācijas apstrādi KIS var sniegt kā funkciju kopu lietotājiem un kā IT pakalpojumus citām KIS;

29) "dienesta noslēpums" ir tādu darba datu informācijas aizsardzība, uz kuriem attiecas pienākums glabāt dienesta noslēpumu, it īpaši informācija par uzņēmumiem, to darījumsakariem vai izmaksu komponentēm, kā noteikts LESD 339. pantā;

30) "atbildīgs" ir tāds, kam ir pienākums rīkoties un pieņemt lēmumus vajadzīgā iznākuma sasniegšanai;

31) "drošība Komisijā" ir cilvēku, aktīvu un informācijas drošība Komisijā, it īpaši cilvēku un aktīvu fiziskais veselums, informācijas un komunikācijas un informācijas sistēmu veselums, konfidencialitāte un pieejamība, kā arī Komisijas darbību netraucēta norise;

32) "kopīgots IT pakalpojums" ir pakalpojums, ko informācijas apstrādē KIS sniedz citām KIS;

33) "sistēmas īpašnieks" ir fiziska persona, kas atbild par kopējo KIS iepirkumu, izstrādi, integrēšanu, pārveidošanu, darbināšanu, uzturēšanu un norakstīšanu;

34) "lietotājs" ir fiziska persona, kas izmanto KIS sniegtās funkcijas Komisijā vai ārpus tās.

3. pants

IT drošības principi Komisijā

1. IT drošība Komisijā pamatojas uz likumības, pārredzamības, proporcionalitātes un pārskatatbildības principu.

2. IT drošības jautājumi tiek ņemti vērā, sākot izstrādāt un īstenot Komisijas KIS. Šim nolūkam Informātikas ģenerāldirektorāts un Cilvēkresursu un drošības ģenerāldirektorāts iesaistās savā attiecīgajā atbildības sfērā.

3. Ar efektīvu IT drošību piemērotā līmenī tiek nodrošināti:

a) autentiskums – garantija, ka informācija ir īsta un saņemta no labticīgiem avotiem;

b) pieejamība – tai var piekļūt un to var izmantot pēc pilnvarotas iestādes pieprasījuma;

c) konfidencialitāte – informāciju neatklāj nesankcionētām personām, iestādēm vai procesiem;

d) veselums – spēja nosargāt informācijas un aktīvu precizitāti un pilnīgumu;

e) neapstrīdamība – spēja pierādīt, ka darbība vai atgadījums ir noticis, lai vēlāk nevarētu notikumu noliegt;

f) personas datu aizsardzība – piemērotu aizsardzības pasākumu nodrošināšana personas datiem pilnīgā atbilstībā Regulai (EK) Nr. 45/2001;

g) dienesta noslēpums – tādu darba datu informācijas aizsardzība, uz kuriem attiecas pienākums glabāt dienesta noslēpumu, it īpaši informācija par uzņēmumiem, to darījumsakariem vai izmaksu komponentēm, kā noteikts LESD 339. pantā.

4. IT drošība balstās uz riska pārzināšanas procesu. Šis procesa mērķis ir noteikt IT drošības risku pakāpi un drošības pasākumus, kas tādu risku samazinātu līdz pieņemamai pakāpei un ar samērīgām izmaksām.

5. Visas KIS identificē, piešķir sistēmas īpašniekam un iekļauj inventāra sarakstā.

6. Visu KIS drošības prasības nosaka pēc to drošības vajadzībām un pēc to apstrādātās informācijas drošības vajadzībām. KIS, kuras sniedz pakalpojumus citām KIS, var veidot tā, lai tās atbalstītu noteiktas pakāpes drošības vajadzības.

7. IT drošības plāniem un IT drošības pasākumiem jābūt proporcionāliem KIS drošības vajadzībām.

Ar šiem principiem un darbībām saistītie procesi sīkāk nosakāmi īstenošanas noteikumos.

2. NODAĻA

ORGANIZĀCIJA UN PIENĀKUMI

4. pants

Iestādes valde

Iestādes valde Komisijā uzņemas vispārēju atbildību par IT drošību kopumā.

5. pants

Informācijas drošības koordinācijas padome (IDKP)

1. IDKP vada ģenerālsekretāra vietnieks, kurš atbild par IT drošības pārvaldību Komisijā. Tās locekļi pārstāv darba, tehnoloģijas un drošības intereses visās Komisijas struktūrvienībās, un viņu vidū ir Informātikas ģenerāldirektorāta, Cilvēkresursu un drošības ģenerāldirektorāta, Budžeta ģenerāldirektorāta un rotācijas kārtā četru citu Komisijas struktūrvienību pārstāvji, kurus iesaista, kad IT drošībai ir svarīga nozīme to darbībās. Locekļi ir no augstākās vadības.

2. IDKP atbalsta iestādes valdi ar IT saistīto uzdevumu izpildē. IDKP Komisijā uzņemas operatīvo atbildību par IT drošību kopumā.

3. IDKP iesaka, kādu Komisijas IT drošības politiku Komisijai pieņemt.

4. IDKP pārskata pārvaldības jautājumus un divas reizes gadā iestādes valdei ziņo par minētajiem jautājumiem, kā arī par IT drošības problēmām, tostarp par nopietniem IT drošības incidentiem.

5. IDKP pārrauga un pārskata šā lēmuma vispārējo īstenošanu un par to ziņo iestādes valdei.

6. Pēc Informātikas ģenerāldirektorāta priekšlikuma IDKP izskata un apstiprina aktuālo IT drošības stratēģiju un pārrauga tās īstenošanu. IDKP par to ziņo iestādes valdei.

7. IDKP pārrauga, izvērtē un kontrolē iestādes informācijas risku novēršanas kopainu, un tai attiecīgā gadījumā ir pilnvaras izteikt formālas prasības izdarīt uzlabojumus.

Ar šiem pienākumiem un darbībām saistītie procesi sīkāk nosakāmi īstenošanas noteikumos.

6. pants

Cilvēkresursu un drošības ģenerāldirektorāts

Saistībā ar IT drošību Cilvēkresursu un drošības ģenerāldirektorātam ir šādi pienākumi. Tas:

1) salāgo IT drošības politiku ar Komisijas informācijas drošības politiku;

2) iedibina kārtību šifrēšanas tehnoloģiju izmantošanas atļaušanai KIS informācijas glabāšanā un sniegšanā;

3) informē Informātikas ģenerāldirektorātu par īpašu apdraudējumu, kas var ievērojami iespaidot KIS un to apstrādājamo datu kopu drošību;

4) inspicē IT drošību, lai varētu novērtēt, kā Komisijas KIS ievēro drošības politiku, un par rezultātiem ziņo IDKP;

5) iedibina kārtību un attiecīgus pienācīgus drošības noteikumus par atļaujām piekļūt Komisijas KIS no ārējiem tīkliem un ciešā sadarbībā ar Informātikas ģenerāldirektorātu izstrādā attiecīgās IT drošības normas un vadlīnijas;

6) KIS nodošanai ārpakalpojumos ierosina principus un noteikumus, lai informācijas drošību paturētu pienācīgā kontrolē;

7) ciešā sadarbībā ar Informātikas ģenerāldirektorātu izstrādā saistītās IT drošības normas un vadlīnijas sakarā ar 6. pantu.

Ar šiem pienākumiem un darbībām saistītie procesi sīkāk nosakāmi īstenošanas noteikumos.

7. pants

Informātikas ģenerāldirektorāts

Informātikas ģenerāldirektorātam ir šādi pienākumi saistībā ar Komisijas vispārējo IT drošību. Tas:

1) izstrādā IT drošības normas un vadlīnijas, izņemot 6. pantā noteiktās, ciešā sadarbībā ar Cilvēkresursu un drošības ģenerāldirektorātu, lai nodrošinātu IT drošības politikas un Komisijas informācijas drošības politikas konsekventu saskanību, un iesniedz to priekšlikumu IDKP;

2) novērtē visu Komisijas struktūrvienību IT drošības risku pārzināšanas metodes, procesus un rezultātus un par to regulāri ziņo IDKP;

3) aktuālo IT drošības stratēģiju iesniedz IDKP pārskatīt un apstiprināt un pēc tam iestādes valdei apstiprināt un liek priekšā programmu, kurā iekļauj IT drošības stratēģijas īstenošanas projektu un darbību plānošanu;

4) pārrauga Komisijas IT drošības stratēģijas izpildi un par to regulāri ziņo IDKP;

5) pārrauga IT drošības riskus un KIS īstenotos IT drošības pasākumus un par to regulāri ziņo IDKP;

6) regulāri ziņo IDKP par vispārējo īstenošanu un atbilstību šim lēmumam;

7) apspriedies ar Cilvēkresursu un drošības ģenerāldirektorātu, pieprasa sistēmu īpašniekiem veikt īpašus IT drošības pasākumus, lai mazinātu Komisijas KIS IT drošības riskus;

8) nodrošina, lai sistēmas īpašniekiem un datu īpašniekiem būtu pieejami adekvāti Informātikas ģenerāldirektorāta IT drošības pakalpojumi, lai tie varētu izpildīt savus pienākumus IT drošības jomā un panākt atbilstību IT drošības politikai un normām;

9) piegādā sistēmu un datu īpašniekiem adekvātu dokumentāciju un ar tiem pienācīgi apspriežas par to IT pakalpojumiem piemērojamajiem IT drošības pasākumiem, lai atvieglinātu atbilstību IT drošības politikai un atbalstītu sistēmu īpašniekus IT riska pārzināšanā;

10) rīko regulāras sanāksmes ar *LISO* tīklu un atbalstu *LISO* viņu pienākumu izpildē;

11) sadarbībā ar Komisijas struktūrvienībām nosaka apmācības vajadzības un koordinē apmācības programmas IT drošības jautājumos un ciešā sadarbībā ar Cilvēkresursu ģenerāldirektorātu izstrādā, īsteno un koordinē izpratnes veicināšanas kampaņas IT drošības jautājumos;

12) nodrošina, ka sistēmas īpašniekiem, datu īpašnieku un citu IT drošības pienākumu pildītājiem Komisijas struktūrvienībās tiek darīts zināms par IT drošības politiku;

13) informē Cilvēkresursu un drošības ģenerāldirektorātu par konkrētiem apdraudējumiem IT drošībai, incidentiem un sistēmas īpašnieku paziņotiem izņēmumiem Komisijas IT drošības politikā, kuriem varētu būt ievērojama ietekme uz drošību Komisijā;

14) savā iekšēja IT pakalpojumu sniedzēja funkcijā piegādā Komisijai katalogu, kurā ir koplietotie IT pakalpojumi, kas nodrošina noteiktas pakāpes drošību. To dara, sistemātiski novērtējot, pārvaldot un pārraugot IT drošības riskus, lai varētu īstenot drošības pasākumus ar nolūku panākt noteiktu drošuma pakāpi.

Ar šo saistītie procesi un detalizētāki pienākumi sīkāk nosakāmi īstenošanas noteikumos.

8. pants

Komisijas struktūrvienības

Savas struktūrvienības IT drošības dēļ katrs Komisijas struktūrvienības vadītājs:

1) oficiāli katrai KIS ieceļ sistēmas īpašnieku no ierēdņiem vai pagaidu darbiniekiem, kurš atbild par minētās KIS IT drošību, un katrai KIS apstrādājamajai datu kopai oficiāli ieceļ datu īpašnieku, kurš pieder pie tās pašas administratīvās vienības, kura ir datu kopu datu pārzinis atbilstoši Regulai (EK) Nr. 45/2001;

2) oficiāli ieceļ vietējo informātikas drošības speciālistu (*LISO*), kurš spēj veikt pienākumus neatkarīgi no sistēmas īpašniekiem un datu īpašniekiem. Vienu *LISO* var iecelt vienai vai vairākām Komisijas struktūrvienībām;

3) nodrošina pienācīga IT drošības riska novērtējumu un IT drošības plānu sastādīšanu un īstenošanu;

4) gādā, lai Informātikas ģenerāldirektorātam regulāri tiktu iesniegts IT drošības risku un pasākumu kopsavilkums;

5) ar Informātikas ģenerāldirektorāta atbalstu nodrošina, ka ir ieviesti piemēroti procesi, procedūras un risinājumi, kas nodrošina ar viņa KIS saistītu IT drošības incidentu efektīvu atklāšanu, izziņošanu un atrisināšanu;

6) IT drošības ārkārtas situācijā sāk ārkārtas gadījuma procedūru;

7) ir pilnīgi atbildīgs par IT drošību, ieskaitot sistēmas īpašnieka un datu īpašnieka pienākumus;

8) atbild par risku, kas saistīts ar viņa KIS un datu kopām;

9) atrisina ikkatras domstarpības starp datu īpašniekiem un sistēmu īpašniekiem un ieilgušu domstarpību gadījumā nodod lieti izskatīšanai IDKP;

10) nodrošina IT drošības plānu un IT drošības pasākumu īstenošanu un risku adekvātu aptvērumu.

Ar šiem pienākumiem un darbībām saistītie procesi sīkāk nosakāmi īstenošanas noteikumos.

9. pants

Sistēmas īpašnieki

1. Sistēmas īpašnieks atbild par KIS IT drošību un ziņo Komisijas struktūrvienības vadītājam.

2. Saistībā ar IT drošību sistēmas īpašnieks:

a) gādā par KIS atbilstību IT drošības politikai;

b) gādā par KIS precīzu ierakstīšanu attiecīgajā reģistrā;

c) sadarbībā ar datu īpašniekiem, apspriežoties ar Informātikas ģenerāldirektorātu, novērtē katras KIS IT drošības risku un nosaka IT drošības vajadzības;

d) sastāda drošības plānu, attiecīgā gadījumā tajā iekļaujot ziņas par novērtēto risku un citiem vajadzīgiem drošības pasākumiem;

e) īsteno piemērotus IT drošības pasākumus, kas ir proporcionāli noskaidrotajam IT drošības riskam, un ievēro IDKP atbalstītos ieteikumus;

f) noskaidro atkarību no citām KIS vai koplietotiem IT pakalpojumiem un īsteno pienācīgus drošības pasākumus, balstoties uz minēto KIS vai koplietoto IT pakalpojumu ierosinātajām drošības pakāpēm;

g) pārzina un pārrauga IT drošības riskus;

h) regulāri ziņo Komisijas struktūrvienības vadītājam par savas KIS IT drošības riska profilu un Informātikas ģenerāldirektorātam par attiecīgo risku, riska pārzināšanas darbībām un veiktajiem drošības pasākumiem;

i) konsultējas ar attiecīgo Komisijas struktūrvienību *LISO* par IT drošības aspektiem;

j) dod norādījumus lietotājiem par KIS un ar to saistīto datu lietošanu, kā arī par lietotāju pienākumiem KIS sakarā;

k) pieprasa Cilvēkresursu un drošības ģenerāldirektorātam, kas darbojas kā šifrēšanas iestāde, atļauju katrai KIS, kura izmanto šifrēšanas tehnoloģiju;

l) laikus konsultējas ar Komisijas Drošības iestādi par katru sistēmu, kura apstrādā ES klasificētu informāciju;

m) nodrošina visu šifra atslēgu dublējuma glabāšanos uzticējumglabāšanas kontā. Šifrētu datu atguvi izdara tikai tad, ja tas atļauts Cilvēkresursu un drošības ģenerāldirektorāta noteiktā kārtībā;

n) ievēro attiecīgo datu pārziņu norādījumus par personas datu aizsardzību un datu aizsardzības noteikumu par apstrādes drošību piemērošanu;

o) paziņo Informātikas ģenerāldirektorātam par izņēmumiem no Komisijas IT drošības politikas, pievienojot attiecīgu attaisnojumu;

p) ziņo Komisijas struktūrvienības vadītājam par visām neatrisinātām domstarpībām starp datu īpašnieku un sistēmas īpašnieku, IT drošības incidentus laicīgi dara zināmus attiecīgajām ieinteresētajām personām atbilstīgi to nopietnumam, kā noteikts 15. pantā;

q) ārpakalpojumā nodotām sistēmām nodrošina piemērotu IT drošības noteikumu iekļaušanu ārpakalpojuma līgumā un paziņošanu par ārpakalpojumā nodotās KIS IT drošības incidentiem saskaņā ar 15. pantu;

r) nodrošina KIS, kuras sniedz koplietojamus IT pakalpojumus, noteiktas drošības pakāpes nodrošinājumu, skaidru dokumentēšanu un drošības pasākumu īstenošanu minētajai KIS, lai panāktu noteikto drošības pakāpi.

3. Sistēmas īpašnieki var oficiāli deleģēt dažus vai visus savus IT drošības uzdevumus, bet paliek atbildīgi par savas KIS IT drošību.

Ar šiem pienākumiem un darbībām saistītie procesi sīkāk nosakāmi īstenošanas noteikumos.

10. pants

Datu īpašnieki

1. Datu īpašnieks atbild par konkrētas datu kopas IT drošību Komisijas struktūrvienības vadītājam un ir saucams pie atbildības par datu kopas konfidencialitāti, veselumu un pieejamību.

2. Sakarā ar šo datu īpašnieks:

a) gādā, lai visas viņā atbildībā esošās datu kopas tiktu pienācīgi klasificētas saskaņā ar Lēmumiem (ES, Euratom) 2015/443 un (ES, Euratom) 2015/444;

b) nosaka informācijas drošības vajadzības un par tām informē attiecīgos sistēmas īpašniekus;

c) piedalās KIS riska novērtēšanā;

d) ziņo Komisijas struktūrvienības vadītājam par visām neatrisināmām domstarpībām starp datu īpašnieku un sistēmas īpašnieku;

e) dara zināmus IT drošības incidentus, kā noteikts 15. pantā.

3. Datu īpašnieki var oficiāli deleģēt dažus vai visus savus IT drošības uzdevumus, bet viņiem paliek šajā pantā noteiktie pienākumi.

Ar šiem pienākumiem un darbībām saistītie procesi sīkāk nosakāmi īstenošanas noteikumos.

11. pants

Vietējie informātikas drošības speciālisti (*LISO*)

Saistībā ar IT drošību *LISO*:

a) proaktīvi nosaka IT drošības politiku un par to informē sistēmas īpašniekus, datu īpašniekus un citu IT drošības pienākumu pildītājus Komisijas struktūrvienībās;

b) uztur saziņu Komisijas struktūrvienībās IT drošības jautājumos ar Informātikas ģenerāldirektorātu *LISO* tīkla ietvaros;

c) piedalās regulārajās *LISO* sanāksmēs;

d) uztur pārskatu par informācijas drošības riska pārzināšanas procesu un informācijas sistēmas drošības plānu sastādīšanu un īstenošanu;

e) konsultē datu īpašniekus, sistēmu īpašniekus un Komisijas struktūrvienību vadītājus ar IT drošību saistītos jautājumos;

f) sadarbojas ar Informātikas ģenerāldirektorātu labas IT drošības prakses izplatīšanā un ierosina konkrētas izpratnes veicināšanas un apmācības programmas;

g) ziņo Komisijas struktūrvienību vadītājiem par IT drošību, konstatētiem trūkumiem un uzlabojumiem.

Ar šiem pienākumiem un darbībām saistītie procesi sīkāk nosakāmi īstenošanas noteikumos.

12. pants

Lietotāji

1. Saistībā ar IT drošību lietotāji:

a) ievēro IT drošības politiku un sistēmas īpašnieka dotos norādījumus par katras KIS lietošanu;

b) dara zināmus IT drošības incidentus, kā noteikts 15. pantā.

2. Komisijas KIS lietošana pretēji IT drošības politikai vai sistēmas īpašnieka dotajiem norādījumiem var būt pamats disciplinārai lietai.

Ar šiem pienākumiem un darbībām saistītie procesi sīkāk nosakāmi īstenošanas noteikumos.

3. NODAĻA

DROŠĪBAS PRASĪBAS UN PIENĀKUMI

13. pants

Lēmuma īstenošana

1. 6. panta īstenošanas noteikumu un attiecīgo normu un vadlīniju pieņemšanai būs vajadzīgs Komisijas pilnvarojošs lēmums par labu Komisijas loceklim, kurš atbild par drošības jautājumiem.

2. Lai pieņemtu visus pārējos īstenošanas noteikumus saistībā ar šo lēmumu un par saistītajām IT drošības normām un vadlīnijām, būs vajadzīgs Komisijas pilnvarojošs lēmums par labu Komisijas loceklim, kurš atbild par informātikas jautājumiem.

3. 1. un 2. punktā minētos īstenošanas noteikumus, normas un vadlīnijas pirms pieņemšanas apstiprina IDKP.

14. pants

Pienākums nodrošināt atbilstību

1. IT drošības politikā un normās izklāstītie noteikumi ir izpildāmi obligāti.

2. IT drošības politikas un normu neievērošana var būt par pamatu saukšanai pie disciplināratbildības saskaņā ar līgumiem, Civildienesta noteikumiem un Savienības Pārējo darbinieku nodarbināšanas kārtību, līgumiskām sankcijām un/vai tiesvedībai saskaņā ar valsts tiesību normām.

3. Par visiem izņēmumiem no IT drošības politikas paziņo Informātikas ģenerāldirektorātam.

4. Ja IDKP nolemj, ka pastāv pastāvīgs, nepieņemams risks attiecībā uz Komisijas KIS, Informātikas ģenerāldirektorāts sadarbībā ar sistēmas īpašnieku apstiprināšanai IDKP piedāvā risku mazinošus pasākumus. Šādi pasākumi cita starpā var būt pārraudzības un ziņošanas pastiprināšana, darbības ierobežošana un pārtraukšana.

5. IDKP apstiprinātos risku mazinošos pasākumus piemēro, kad tas ir nepieciešams. IDKP var arī ieteikt Cilvēkresursu un drošības ģenerāldirektorāta ģenerāldirektoram sākt administratīvu izmeklēšanu. Informātikas ģenerāldirektorāts ziņo IDKP par katru gadījumu, kad risku mazinošie pasākumi ir piemēroti.

Ar šiem pienākumiem un darbībām saistītie procesi sīkāk nosakāmi īstenošanas noteikumos.

15. pants

Rīcība IT drošības incidentos

1. Informātikas ģenerāldirektorāts ir atbildīgs par spēju nodrošināt reakciju uz operatīviem IT drošības incidentiem Eiropas Komisijā.

2. Cilvēkresursu un drošības ģenerāldirektorāts kā ieinteresētā persona, kas iesaistīta reaģēšanā uz IT drošības incidentiem:

a) ir tiesīgs piekļūt visu incidentu reģistru informatīviem kopsavilkumiem un pēc pieprasījuma arī reģistru pilnajai informācijai;

b) līdzdarbojas IT drošības incidentu krīzes pārvarēšanas grupās un ar IT drošību saistītajās ārkārtas procedūrās;

c) ir atbildīgs par attiecībām ar tiesībaizsardzības un izlūkošanas iestādēm;

d) veic kriminālistisko kiberdrošības ekspertīzi atbilstoši Lēmuma (ES, Euratom) 2015/443 11. pantam;

e) lemj par nepieciešamību uzsākt oficiālu izmeklēšanu;

f) informē Informātikas ģenerāldirektorātu par IT drošības incidentiem, kas var radīt risku citām KIS.

3. Informātikas ģenerāldirektorāts un Cilvēkresursu un drošības ģenerāldirektorāts savā starpā regulāri sazinās, lai apmainītos ar informāciju un koordinētu rīcību saistībā ar drošības incidentiem, jo īpaši saistībā ar IT drošības incidentiem, kam var būt vajadzīga oficiāla izmeklēšana.

4. Lai atbalstītu rīcību saistībā ar incidentiem, attiecīgos gadījumos var izmantot ES iestāžu un aģentūru datorapdraudējumu reaģēšanas vienības (*CERT-EU*) incidentu koordinācijas dienestus, lai apmainītos ar informāciju ar citām ES iestādēm un aģentūrām, kuras šādi incidenti varētu ietekmēt.

5. Tās sistēmas īpašnieki, kas ir iesaistīta IT drošības incidentā:

a) nekavējoties informē Komisijas struktūrvienību vadītājus, Informātikas ģenerāldirektorātu, Cilvēkresursu un drošības ģenerāldirektorātu, *LISO* un attiecīgā gadījumā datu īpašniekus par nozīmīgiem IT drošības incidentiem, jo īpaši par tādiem incidentiem, kas ir saistīti ar datu konfidencialitātes pārkāpumu;

b) sadarbojas un ievēro attiecīgo Komisijas iestāžu norādījumus par saziņas, reakcijas un koriģēšanas pasākumiem saistībā ar incidentu.

6. Lietotāji par visiem faktiskiem un iespējamiem IT drošības incidentiem laikus ziņo attiecīgajam IT palīdzības dienestam.

7. Datu īpašnieki par visiem faktiskiem un iespējamiem IT drošības incidentiem laikus ziņo attiecīgajai IT drošības reaģēšanas vienībai.

8. Informātikas ģenerāldirektorāts ar citu iesaistīto ieinteresēto personu atbalstu ir atbildīgs par rīcību saistībā ar katru konstatētu IT drošības incidentu Komisijas KIS, kas nav ārpakalpojumā nodotās sistēmas.

9. Informātikas ģenerāldirektorāts informē ietekmētās Komisijas struktūrvienības par IT drošības incidentiem, attiecīgos *LISO* un attiecīgā gadījumā arī *CERT-EU*, ja pastāv vajadzībā pēc informācijas.

10. Informātikas ģenerāldirektorāts regulāri ziņo IDKP par nozīmīgiem IT drošības incidentiem, kas ietekmē Komisijas KIS.

11. Attiecīgajam *LISO* pēc pieprasījuma ir pieeja IT drošības incidentu reģistru informācijai par Komisijas struktūrvienības KIS.

12. Nozīmīga IT drošības incidenta gadījumā Informātikas ģenerāldirektorāts ir krīzes situācijas pārvarēšanas kontaktpunkts, kurš koordinē IT drošības incidentu krīzes pārvarēšanas grupas.

13. Ārkārtas situācijā Informātikas ģenerāldirektorāta ģenerāldirektors var pieņemt lēmumu uzsākt ar IT drošību saistītu ārkārtas procedūru. Informātikas ģenerāldirektorāts izstrādā ārkārtas procedūras, kuras pastiprina IDKP.

14. Informātikas ģenerāldirektorāts ziņo IDKP un ietekmēto Komisijas struktūrvienību vadītājiem par ārkārtas procedūru izpildi.

Ar šiem pienākumiem un darbībām saistītie procesi sīkāk nosakāmi īstenošanas noteikumos.

4. NODAĻA

NOBEIGUMA NOTEIKUMI

16. pants

Pārredzamība

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

17. pants

Saistība ar citiem aktiem

Šā lēmuma noteikumi neskar Lēmumu (ES, Euratom) 2015/443, Lēmumu (ES, Euratom) 2015/444, Regulu (EK) Nr. 45/2001, Eiropas Parlamenta un Padomes Regulu (EK) Nr. 1049/2001 ([1]), Komisijas Lēmumu 2002/47/EK, EOTK, Euratom ([2]), Eiropas Parlamenta un Padomes Regulu (ES, Euratom) Nr. 883/2013 ([3]) un Lēmumu 1999/352/EK, EOTK, Euratom.

18. pants

Atcelšana un pārejas pasākumi

2006. gada 16. augusta Lēmums C(2006) 3602 tiek atcelts.

Atbilstoši Lēmumam C(2006) 3602 pieņemtie īstenošanas noteikumi un IT drošības standarti paliek spēkā, ciktāl tie nav pretrunā šim lēmumam, līdz tos aizstāj ar īstenošanas noteikumiem un standartiem, kas pieņemti atbilstoši šā lēmuma 13. pantam. Norādes uz Lēmuma C(2006) 3602 10. pantu jāsaprot kā norādes uz šā lēmuma 13. pantu.

19. pants

Stāšanās spēkā

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

Briselē, 2017. gada 10. janvārī

Komisijas vārdā –
priekšsēdētājs
Jean-Claude JUNCKER

([1]) Eiropas Parlamenta un Padomes 2001. gada 30. maija Regula (EK) Nr. 1049/2001 par publisku piekļuvi Eiropas Parlamenta, Padomes un Komisijas dokumentiem (OV L 145, 31.5.2001., 43. lpp.).
([2]) Komisijas 2002. gada 23. janvāra Lēmums 2002/47/EK, EOTK, Euratom, ar ko groza Komisijas reglamentu (OV L 21, 24.1.2002., 23. lpp.).
([3]) Eiropas Parlamenta un Padomes 2013. gada 11. septembra Regula (ES, Euratom) Nr. 883/2013 par izmeklēšanu, ko veic Eiropas Birojs krāpšanas apkarošanai (*OLAF*), un ar ko atceļ Eiropas Parlamenta un Padomes Regulu (EK) Nr. 1073/1999 un Padomes Regulu (Euratom) Nr. 1074/1999 (OV L 248, 18.9.2013., 1. lpp.).