OTSUSED

KOMISJONI OTSUS (EL, Euratom) 2017/46,

10. jaanuar 2017,

Euroopa Komisjoni side- ja infosüsteemide turvalisuse kohta

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 249,

võttes arvesse Euroopa Aatomienergiaühenduse asutamislepingut,

ning arvestades järgmist:

(1) Komisjoni side- ja infosüsteemid on komisjoni toimimise lahutamatu osa ning IT turvalisuse intsidentidel on rasked tagajärjed komisjoni tööle, aga ka kolmandatele isikutele, sh üksikisikutele, ettevõtjatele ja liikmesriikidele.

(2) Komisjoni side- ja infosüsteemide ja neis sisalduva teabe konfidentsiaalsust, terviklust ja käideldavust võivad kahjustada mitmesugused ohud, näiteks õnnetused, vead, tahtlikud ründed ja loodusnähtused, ning neid tuleks käsitada tööga seotud riskidena.

(3) Side- ja infosüsteemide kaitse tase peab olema vastavuses neid ähvardavate riskide tõenäosuse, mõju ja laadiga.

(4) Komisjoni IT turve peaks tagama, et komisjoni side- ja infosüsteemid kaitsevad neis töödeldavat teavet ning funktsioneerivad õiguspäraste kasutajate kontrolli all nii, nagu vaja, ja siis, kui vaja.

(5) Komisjoni IT turbe põhimõtteid tuleb rakendada viisil, mis on kooskõlas komisjoni turvalisuspõhimõtetega.

(6) Üldiselt vastutab komisjonis turvalisuse eest personalihalduse ja julgeoleku peadirektoraadi julgeoleku direktoraat, mis tegutseb julgeolekuküsimuste eest vastutava komisjoniliikme alluvuses ja vastutusalas.

(7) Komisjoni lähenemine peaks arvestama võrgu- ja infoturbe alaseid ELi poliitilisi algatusi ja õigusakte, tööstuse standardeid ja häid tavasid, järgima kõiki asjakohaseid õigusakte ning võimaldama koostalitlusvõimet ja ühilduvust.

(8) Side- ja infosüsteemide eest vastutavad komisjoni talitused peaksid välja töötama asjakohased meetmed ja neid rakendama ning tõhususe ja tulemuslikkuse huvides tuleks side- ja infosüsteemide kaitseks võetud IT turbe meetmeid koordineerida kogu komisjonis.

(9) IT turbe kontekstis, sh IT turbe intsidentide käsitlemise puhul, peaksid teabele juurdepääsu eeskirjad ja menetlused olema komisjoni või selle töötajaid ähvardava ohuga proportsionaalsed ja kooskõlas Euroopa Parlamendi ja nõukogu määruses (EÜ) nr 45/2001 [1] (üksikisikute kaitse kohta isikuandmete töötlemisel liidu institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta) kehtestatud põhimõtetega ning arvestama ELi toimimise lepingu artiklis 339 sätestatud ametisaladuse põhimõtet.

[1] Euroopa Parlamendi ja nõukogu 18. detsembri 2000. aasta määrus (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta (EÜT L 8, 12.1.2001, lk 1).

(10) ELi salastatud teabe, tundliku, kuid salastamata teabe, ja salastamata teabe töötlemiseks kasutatavate side- ja infosüsteemide suhtes kohaldatavad põhimõtted ja eeskirjad peavad olema täielikult vastavuses komisjoni otsustega (EL, Euratom) 2015/443 ([1]) ja (EL, Euratom) 2015/444 ([2]).

(11) Komisjonil on vaja oma side- ja infosüsteemide turvalisust käsitlevad sätted läbi vaadata ja neid ajakohastada.

(12) Seega tuleks komisjoni otsus C(2006) 3602 kehtetuks tunnistada,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

1. PEATÜKK

ÜLDSÄTTED

Artikkel 1

Reguleerimisese ja kohaldamisala

1. Käesolevat otsust kohaldatakse kõigi side- ja infosüsteemide suhtes, mis kuuluvad komisjonile, mille komisjon on hankinud, mida ta haldab või käitab või mis on hangitud, mida hallatakse või käitatakse tema nimel, ning selliste side- ja infosüsteemide igasuguse komisjonipoolse kasutamise suhtes.

2. Käesolevas otsuses sätestatakse selliste side- ja infosüsteemide turbega seotud peamised põhimõtted, eesmärgid, töökorraldus ja vastutusalad, mis kehtivad eeskätt komisjoni talituste suhtes, kellel on side- ja infosüsteeme või kes hangivad, haldavad või käitavad neid, kaasa arvatud komisjonisisese IT-teenuse osutaja pakutavate side- ja infosüsteemide suhtes. Kui side- ja infosüsteemi pakub, omab, haldab või käitab komisjoniväline isik kahepoolse kokkulepe või lepingu põhjal, peavad kokkuleppe või lepingu tingimused olema kooskõlas käesoleva otsusega.

3. Käesolevat otsust kohaldatakse kõigi komisjoni talituste ja rakendusametite suhtes. Kui muud asutused ja institutsioonid kasutavad komisjoni side- ja infosüsteemi komisjoniga sõlmitud kahepoolse kokkulepe põhjal, peavad kokkuleppe tingimused olema kooskõlas käesoleva otsusega.

4. Olenemata konkreetsetest viidetest teatavatele personali rühmadele kohaldatakse käesolevat otsust komisjoni liikmete, Euroopa Liidu ametnike personalieeskirjade (edaspidi „personalieeskirjad“) ning liidu muude teenistujate teenistustingimuste ([3]) kohaldamisalas oleva komisjoni personali, komisjoni lähetatud riikide ekspertide, ([4]) komisjoniväliste teenusepakkujate ja nende personali, praktikantide ning kõigi isikute suhtes, kellel on juurdepääs side- ja infosüsteemidele, mis kuuluvad käesoleva otsuse kohaldamisalasse.

5. Käesolevat otsust kohaldatakse Euroopa Pettustevastase Ameti (OLAF) suhtes, kuivõrd see on kokkusobiv liidu õigusaktidega ja komisjoni otsusega 1999/352/EÜ, ESTÜ, Euratom ([5]). Eeskätt ei pruugi käesolevas otsuses sätestatud meetmeid, sh juhiseid, inspekteerimisi, uurimisi ja samaväärseid meetmeid OLAFi suhtes kohaldada, kui see ei sobi kokku tema uurimisfunktsiooni sõltumatusega ja/või OLAFi poolt oma ülesannete täitmise käigus saadud teabe konfidentsiaalsusega.

Artikkel 2

Mõisted

Käesolevas otsuses kasutatakse järgmisi mõisteid:

1) „vastutusele võetav“ – st isik peab andma vastust toimingute, otsuste ja sooituse kohta;

([1]) Komisjoni 13. märtsi 2015. aasta otsus (EL, Euratom) 2015/443 komisjoni julgeoleku kohta (ELT L 72, 17.3.2015, lk 41).
([2]) Komisjoni 13. märtsi 2015. aasta otsus (EL, Euratom) 2015/444 ELi salastatud teabe kaitseks vajalike julgeolekunormide kohta (ELT L 72, 17.3.2015, lk 53).
([3]) Kehtestatud nõukogu 29. veebruari 1968. aasta määrusega (EMÜ, Euratom, ESTÜ) nr 259/68, millega kehtestatakse Euroopa ühenduste ametnike personalieeskirjad ja muude teenistujate teenistustingimused ning komisjoni ametnike suhtes ajutiselt kohaldatavad erimeetmed (EÜT L 56, 4.3.1968, lk 1).
([4]) Komisjoni 12. novembri 2008. aasta otsus, millega kehtestatakse komisjoni talituste juurde lähetatud riiklike ekspertide ja seal erialast koolitust saavate riiklike ekspertide suhtes kohaldatavad eeskirjad (C(2008) 6866 (final)).
([5]) Komisjoni 28. aprilli 1999. aasta otsus 1999/352/EÜ, ESTÜ, Euratom, millega asutatakse Euroopa Pettustevastane Amet (OLAF) (EÜT L 136, 31.5.1999, lk 20).

2) „CERT-EU“ – ELi institutsioonide ja ametite infoturbeintsidentidega tegelev rühm. Tema ülesanne on toetada Euroopa institutsioone ja aidata neil endid kaitsta sihilike ja pahatahtlike rünnete eest, mis võivad kahjustada nende IT-varade terviklust ja ELi huve. CERT-EU tegevuste hulka kuuluvad ennetustegevus, avastamine, reageerimine ja taastamine;

3) „komisjoni talitus“ – komisjoni mis tahes peadirektoraat või talitus või komisjoniliikme kabinet;

4) „komisjoni julgeolekuasutus“ – otsuses (EL, Euratom) 2015/444 sätestatud ülesannete täitja;

5) „side- ja infosüsteem“ – süsteem, mis võimaldab elektroonilises vormis oleva teabe töötlemist, kaasa arvatud süsteemi toimimiseks vajaliku vara ning infrastruktuuri, töökorralduse, töötajate ja teabega seotud ressursid. See määratlus hõlmab ärirakendusi, jagatud IT-teenuseid, sisseostetud süsteeme ja lõppkasutajate seadmeid;

6) „üldjuhatus“ – organ, mis teostab kõrgeimal tasandil asutuse juhatuse järelevalvet komisjoni töö ja halduskü simuste üle;

7) „andmete omanik“ – üksikisik, kes vastutab side- ja infosüsteemis käideldava konkreetse andmekogumi kaitsmise ja kasutamise tagamise eest;

8) „andmekogum“ – hulk teavet, mida kasutatakse komisjoni konkreetse äriprotsessi või toimingu jaoks;

9) „hädaolukorras tegutsemise kord“ – kiireloomulistele juhtudele reageerimiseks eelnevalt paika pandud meetodite ja vastutuse kord, et vältida komisjonile raskeid tagajärgi;

10) „infoturbepõhimõtted“ – infoturbe eesmärkide kogum, mis on kehtestatud, mida rakendatakse ja kontrollitakse või mis tuleb kehtestada, rakendada ja mida tuleb kontrollida. See hõlmab otsuseid (EL, Euratom) 2015/444 ja (EL, Euratom) 2015/443, kuid ei piirdu ainult nendega;

11) „infoturbe juhtnõukogu“ – juhtorgan, mis toetab üldjuhatust IT turbega seotud ülesannetes;

12) „komisjonisisene IT-teenuse osutaja“ – komisjoni talitus, kes osutab ühiseid IT-teenuseid;

13) „IT turve“ ehk „side- ja infosüsteemide turve“ – side- ja infosüsteemide ja neis töödeldavate andmekogumite konfidentsiaalsuse, tervikluse ja käideldavuse säilitamine;

14) „IT turbe suunised“ – soovituslikud, kuid vabatahtlikud meetmed, mis aitavad toetada IT standardeid või millele saab toetuda kohaldatavate standardite puudumise korral;

15) „IT turbe intsident“ – juhtum, mis võib kahjustada side- ja infosüsteemi konfidentsiaalsust, terviklust või käideldavust;

16) „IT turbe meede“ – tehniline või organisatsiooniline meede, mille eesmärk on leevendada IT turbe riske;

17) „IT turbega seotud vajadus“ – teabe või IT-süsteemi konfidentsiaalsuse, tervikluse ja käideldavuse tasemete täpne ja ühemõtteline määratlus, et teha kindlaks vajaliku kaitse tase;

18) „IT turbe eesmärk“ – kinnitatud kavatsus tõrjuda konkreetseid ohte ja/või täita konkreetsed organisatsioonilised turvalisusega seotud nõuded või eeldused;

19) „IT turbe kava“ – side- ja infosüsteemi IT turbe vajaduste täitmiseks vajalikke IT turbe meetmeid käsitlev dokumentatsioon;

20) „IT turbe põhimõtted“ – IT turbe eesmärkide kogum, mis on kehtestatud, mida rakendatakse ja kontrollitakse või mis tuleb kehtestada, rakendada ja mida tuleb kontrollida. See hõlmab käesolevat otsust ja selle rakenduseeskirju;

21) „IT turbe nõue“ – eelnevalt kindlaks määratud korras ametliku kuju saanud IT turbe vajadus;

22) „IT turbe risk“ – mõju, mida IT turbe oht võib side- ja infosüsteemi nõrkust ära kasutades sellele avaldada. Selles plaanis iseloomustavad IT turbe riske kaks tegurit: 1) määramatus, st tõenäosus, et IT turbe oht põhjustab soovimatu juhtumi, ja 2) mõju, st sellise soovimatu juhtumi võimalikud tagajärjed side- ja infosüsteemi jaoks;

23) „IT turbe standardid“ – konkreetsed kohustuslikud IT turbe meetmed, mis aitavad tagada IT turbe põhimõtete täitmise ja toetavad seda;

24) „IT turbe strateegia“ – hulk komisjoni eesmärkide saavutamiseks väljatöötatud projekte ja toiminguid, mis tuleb kehtestada ning mida tuleb rakendada ja kontrollida;

25) „IT turbe oht“ – tegur, mis võib põhjustada soovimatu juhtumi, mille tulemusena saab side- ja infosüsteem kahjustatud. Selline oht võib olla juhuslik või tahtlik ning seda iseloomustavad ohtlikud elemendid, võimalikud sihtmärgid ja ründemeetodid;

26) „kohalik informaatika turvalisuse ametnik“ ehk „LISO“ – ametnik, kes vastutab komisjoni talituse IT turbe alase teabevahetuse eest;

27) terminid „isikuandmed“, „isikuandmete töötlemine“, „vastutav töötleja“ ja „isikuandmete kataloog“ tähendavad sama, kui on sätestatud määruses (EÜ) nr 45/2001, eeskätt selle artiklis 2;

28) „teabe töötlemine“ – side- ja infosüsteemi kõik funktsioonid, mis on seotud andmekogumitega, sh teabe loomine, muutmine, kuvamine, salvestamine, edastamine, kustutamine ja arhiveerimine. Side- ja infosüsteem võib pakkuda teabe töötlemist kasutajatele mõeldud funktsioonide kogumina või teistele side- ja infosüsteemidele mõeldud IT-teenusena;

29) „ametisaladus“ – ametisaladuse hoidmise kohustusega hõlmatud äriandmetega seotud teabe kaitsmine, eeskätt sellise teabe, mis puudutab ettevõtjaid, nende ärisuhteid või nende kulukomponente vastavalt ELi toimimise lepingu artiklile 339;

30) „vastutama“ – olema kohustatud tegutsema ja võtma vastu otsuseid, et saavutada vajalikud tulemused;

31) „komisjoni turvalisus“ komisjoni isikute, vara ja teabe turvalisus, eelkõige isikute füüsiline puutumatus, vara füüsiline terviklikkus, teabe ning side- ja infosüsteemide terviklus, konfidentsiaalsus ja käideldavus ning komisjoni tööülesannete takistusteta täitmine;

32) „jagatud IT-teenus“ – teenus, mida üks side- ja infosüsteem osutab teisele side- ja infosüsteemile teabe töötlemiseks;

33) „süsteemi omanik“ – üksikisik, kes vastutab side- ja infosüsteemiga seotud hangete ning nende süsteemide arendamise, integreerimise, muutmise, käitamise, hooldamise ja käibelt kõrvaldamise eest;

34) „kasutaja“ – iga üksikisik, kes kasutab side- ja infosüsteemi funktsioone komisjoni sees või väljaspool komisjoni.

Artikkel 3

Komisjoni IT turbe põhimõtted

1. Komisjoni IT turve põhineb seaduslikkuse, läbipaistvuse, proportsionaalsuse ja vastutusele võetavuse põhimõttel.

2. Komisjoni side- ja infosüsteemide arendamisel ja teostamisel võetakse IT turbega seotud küsimusi arvesse algusest peale. Et see oleks võimalik, kaasatakse oma vastutusalades informaatika peadirektoraat ning personalihalduse ja julgeoleku peadirektoraat.

3. Tulemuslik IT turve tagab asjakohasel tasemel järgmised omadused:

a) autentsus: tagatis, et teave on ehtne ja pärineb heausksest allikast;

b) käideldavus: teave on volitatud isiku taotluse korral kättesaadav ja kasutatav;

c) konfidentsiaalsus: teavet ei avalikustata volitamata isikutele, üksustele või töötlemiseks;

d) terviklus: vara ja teabe täpsuse ja täielikkuse tagamine;

e) salgamatus: võime tõendada toimingu või sündmuse toimumist selliselt, et kõnealuse sündmuse või toimingu toimumist ei saa hiljem eitada;

f) isikuandmete kaitse: asjakohaste kaitsemeetmete pakkumine isikuandmete puhul täielikus vastavuses määrusega (EÜ) nr 45/2001;

g) ametisaladus: ametisaladuse hoidmise kohustusega hõlmatud teabe kaitsmine, eeskätt sellise teabe, mis puudutab ettevõtjaid, nende ärisuhteid või nende kulukomponente vastavalt ELi toimimise lepingu artiklile 339.

4. IT turbe aluseks on riskihalduse protsess. Selle protsessi eesmärk on teha kindlaks IT turbe riskide tasemed ja määrata kindlaks turbemeetmed, mille abil vähendada need riskid sobiva tasemeni ja seda proportsionaalsete kuludega.

5. Kõik side- ja infosüsteemid peavad olema identifitseeritud, omistatud süsteemi omanikule ja inventeeritud.

6. Kõigi side- ja infosüsteemide turbe nõuded määratakse kindlaks nende turbevajadustest ja neis töödeldava teabe turbevajadustest lähtudes. Teistele side- ja infosüsteemidele teenuseid pakkuvad side- ja infosüsteemid tuleb projekteerida selliselt, et nad toetaksid konkreetsel tasemel turbevajadusi.

7. IT turbe kavad ja IT turbe meetmed peavad olema asjaomase side- ja infosüsteemi turbevajadustega proportsionaalsed.

Nende põhimõtete ja toimingutega seotud protsesse kirjeldatakse üksikasjalikumalt rakenduseeskirjades.

2. PEATÜKK

TÖÖKORRALDUS JA VASTUTUSALAD

Artikkel 4

Üldjuhatus

Üldjuhatus vastutab üldiselt komisjoni IT turbe kui terviku juhtimise eest.

Artikkel 5

Infoturbe juhtnõukogu

1. Infoturbe juhtnõukogu (edaspidi „juhtnõukogu“) esimeheks on komisjonis IT turbe juhtimise eest vastutav asepeasekretär. Juhtnõukogu liikmed esindavad komisjoni eri talituste äripoole, tehnoloogia ja turbega seotud huve ning nende hulka kuuluvad informaatika peadirektoraadi, personalihalduse ja julgeoleku peadirektoraadi ja eelarve peadirektoraadi esindajad ning kahe aasta kaupa roteeruvalt nelja muu asjaomase komisjoni talituse esindajad, kui IT turve on nende töö seisukohast väga oluline. Juhtnõukogu liikmed on kõrgema juhtkonna hulgast.

2. Juhtnõukogu toetab üldjuhatust IT turbega seotud ülesannete täitmisel. Juhtnõukogu vastutab praktiliselt komisjoni IT turbe kui terviku juhtimise eest.

3. Juhtnõukogu soovitab komisjonil võtta vastu oma IT turbe põhimõtted.

4. Juhtnõukogu vaatab kaks korda aastas üle juhtimist puudutavad küsimused ja IT turbega seotud küsimused, sh tõsised IT turbe intsidendid, ja annab üldjuhatusele selle kohta aru.

5. Juhtnõukogu jälgib käesoleva otsuse üldist rakendamist ning vaatab selle läbi ja annab üldjuhatusele selle kohta aru.

6. Informaatika peadirektoraadi ettepanekul vaatab juhtnõukogu läbi kehtiva IT turbe perioodiliselt uuendatava strateegia ning kiidab selle heaks ja jälgib selle rakendamist. Juhtnõukogu annab selle kohta aru üldjuhatusele.

7. Juhtnõukogu jälgib, hindab ja kontrollib komisjoni teavet puudutavate riskide käsitlemise olukorda ning tal on õigus teha vajaduse korral ametlikke ettepanekuid olukorra parandamiseks.

Nende vastutusalade ja toimingutega seotud protsesse kirjeldatakse üksikasjalikumalt rakenduseeskirjades.

Artikkel 6

Personalihalduse ja julgeoleku peadirektoraat

IT turbe puhul vastutab personalihalduse ja julgeoleku peadirektoraat järgmiste teemade eest. Ta

1) tagab, et IT turbe põhimõtted ja komisjoni infoturbepõhimõtted on omavahel vastavuses;

2) loob raamistiku krüpteerimistehnoloogiate kasutamise volitamiseks side- ja infosüsteemides teabe salvestamise ja edastamise jaoks;

3) teavitab informaatika peadirektoraati konkreetsetest ohtudest, millel võib olla oluline mõju side- ja infosüsteemide turbele ja neis süsteemides töödeldavatele andmekogumitele;

4) inspekteerib IT turvet, et hinnata komisjoni side- ja infosüsteemide vastavust turbepõhimõtetele, ning annab inspekteerimise tulemuste kohta aru juhtnõukogule;

5) loob komisjoni side- ja infosüsteemidele välisvõrkudest juurdepääsu õiguste volitamise raamistiku ja sellega seotud asjakohased turbe-eeskirjad ning arendab asjakohaseid IT turbe standardeid ja suuniseid tihedas koostöös informaatika peadirektoraadiga;

6) teeb ettepanekud side- ja infosüsteemide hangete põhimõtete ja eeskirjade kohta, et säiliks piisav kontroll teabe turvalisuse üle;

7) arendab artikliga 6 seotud asjakohaseid IT turbe standardeid ja suuniseid tihedas koostöös informaatika peadirektoraadiga.

Nende vastutusalade ja toimingutega seotud protsesse kirjeldatakse üksikasjalikumalt rakenduseeskirjades.

Artikkel 7

Informaatika peadirektoraat

Komisjoni üldise IT turbe puhul vastutab informaatika peadirektoraat järgmiste teemade eest. Ta

1) arendab tihedas koostöös personalihalduse ja julgeoleku peadirektoraadiga IT turbe standardeid ja suuniseid, välja arvatud artiklis 6 osutatud juhtudel, et tagada IT turbe põhimõtete kooskõla komisjoni infoturbepõhimõtetega, ning esitab sellekohase ettepaneku juhtnõukogule;

2) hindab kõigi komisjoni talituste IT turbe riskihalduse meetodeid, protsesse ja tulemusi ja annab juhtnõukogule selle kohta regulaarselt aru;

3) esitab IT turbe perioodiliselt uuendatava strateegia ettepaneku läbivaatamiseks ja heakskiitmiseks juhtnõukogule, et üldjuhatus saaks selle hiljem vastu võtta, ning esitab programmiettepaneku, milles käsitletakse muu hulgas IT turbe strateegia projektide kavandamist ja toimingute elluviimist;

4) teostab komisjoni IT turbe strateegia seiret ja annab selle kohta regulaarselt aru juhtnõukogule;

5) teostab IT turbe riskide ning side- ja infosüsteemide IT turbe meetmete seiret ja annab selle kohta regulaarselt aru juhtnõukogule;

6) annab juhtnõukogule regulaarselt aru käesoleva otsuse üldise rakendamise ja täitmise kohta;

7) nõuab süsteemide omanikelt pärast personalihalduse ja julgeoleku peadirektoraadiga konsulteerimist konkreetsete IT turbe meetmete võtmist, et leevendada komisjoni side- ja infosüsteemide IT turbe riske;

8) tagab, et süsteemide omanikele ja andmete omanikele on kättesaadav piisav valik informaatika peadirektoraadi IT turbe teenuseid, et nad saaksid täita oma vastutusalasse kuuluvaid IT turbega seotud ülesandeid ning järgida IT turbe põhimõtteid ja standardeid;

9) pakub süsteemide ja andmete omanikele piisavat dokumentatsiooni ning nõustab neid vajaduse korral nende IT teenuste suhtes rakendatavate IT turbe meetmete kohta, et hõlbustada IT turbe põhimõtete järgimist ning toetada süsteemi omanikke IT riskide haldamisel;

10) korraldab LISOde võrgu regulaarseid kohtumisi ja toetab LISOsid nende tööülesannete täitmisel;

11) määrab kindlaks koolitusvajadused ja koordineerib IT turbe alaseid koolitusprogramme koostöös komisjoni talitustega ning arendab, rakendab ja koordineerib tihedas koostöös personaliüsimuste peadirektoraadiga kampaaniaid, et suurendada teadlikkust IT turbest;

12) tagab, et süsteemide omanikud, andmete omanikud ja muud IT turbe valdkonnas vastutavat rolli kandvad isikud komisjoni talitustes on IT turbe põhimõtetest teadlikud;

13) teavitab personalihalduse ja julgeoleku peadirektoraati konkreetsetest IT turbe ohtudest, intsidentidest ja komisjoni IT turbe põhimõtetest tehtavatest eranditest, millest süsteemide omanikud on teada andnud ja millel võib olla oluline mõju komisjoni turvalisusele;

14) pakub komisjonile komisjonisisese IT-teenuse osutajana valikut kindlaksmääratud turvalisuse tasemeid pakkuvaid jagatud IT-teenuseid. Sel otstarbel hinnatakse, hallatakse ja jälgitakse IT turbe riske süsteemselt, et rakendada kindlaksmääratud turvalisuse taseme saavutamiseks turbemeetmeid.

Seotud protsesse ja täpsemalt määratletud vastutusalasid kirjeldatakse üksikasjalikumalt rakenduseeskirjades.

Artikkel 8

Komisjoni talitused

Iga komisjoni talituse juhataja teeb oma talituses IT turbe valdkonnas järgmist:

1) määrab ametlikult igale side- ja infosüsteemile süsteemi omaniku, kelleks on ametnik või ajutine teenistuja, kes vastutab selle side- ja infosüsteemi IT turbe eest, ning samuti määrab ta igale side- ja infosüsteemis töödeldavale andmekogumile andmete omaniku, kes peaks kuuluma samasse haldusüksusesse kui määruse (EÜ) nr 45/2001 ko-haldamisalasse kuuluva andmekogumi vastutav töötleja;

2) määrab ametlikult kohaliku informaatika turvalisuse ametniku (LISO), kes saab oma ülesandeid täita süsteemi ja andmete omanikest sõltumatult. LISO võib määrata ühe või mitme komisjoni talituse jaoks;

3) tagab, et tehtud on asjakohased IT turbe riskide hindamised ja koostatud on IT turbe kavad ning et neid rakendatakse;

4) tagab, et informaatika peadirektoraadile esitatakse regulaarselt IT turbe riskide ja meetmete kokkuvõttev aruanne;

5) tagab informaatika peadirektoraadi toel, et kehtestatud on asjakohased protsessid, menetlused ja lahendused, mis võimaldaksid nende side- ja infosüsteeme puudutavaid IT turbe intsidente tõhusalt avastada, neist aru anda ja need lahendada;

6) käivitab IT turbe hädaolukorra tekkides hädaolukorras tegutsemise korra;

7) on lõppinstantsina vastutusele võetav IT turbe eest, see hõlmab ka süsteemi omaniku ja andmete omaniku vastutust;

8) omab side- ja infosüsteemide ja andmekogumitega seotud riske;

9) lahendab võimalikud lahkarvamused andmete omanike ja süsteemide omanike vahel ning esitab pikaleveninud vaidlused lahendamiseks juhtnõukogule;

10) tagab, et IT turbe kavad ja IT turbe meetmed viiakse ellu ja et riskid on piisavalt kaetud.

Nende vastutusalade ja toimingutega seotud protsesse kirjeldatakse üksikasjalikumalt rakenduseeskirjades.

Artikkel 9

Süsteemide omanikud

1. Süsteemi omanik vastutab side- ja infosüsteemi IT turbe eest ja annab aru komisjoni talituse juhile.

2. Seoses IT turbega teeb süsteemi omanik järgmist:

a) tagab side- ja infosüsteemi vastavuse IT turbe põhimõtetele;

b) tagab, et side- ja infosüsteem on kantud asjakohasesse registrisse;

c) hindab IT turbe riske ja teeb kindlaks iga side- ja infosüsteemi IT turbega seotud vajadused koostöös andmete omanikega ja konsulteerides informaatika peadirektoraadiga;

d) koostab turbekava, mis hõlmab muu hulgas üksikasju hinnatud riskide ja vajalike täiendavate turbemeetmete kohta;

e) rakendab asjakohaseid IT turbe meetmeid, mis on kindlaks tehtud IT turbe riskide seisukohast proportsionaalsed ning järgivad juhtnõukogu heaks kiidetud soovitusi;

f) teeb kindlaks võimalikud sõltuvused teistest side- ja infosüsteemidest või jagatud IT-teenustest ning rakendab vastavalt vajadusele turbemeetmeid, lähtudes nende side- ja infosüsteemide või jagatud IT-teenuste pakutud turvalisuse tasemetest;

g) haldab ja jälgib IT turbe riske;

h) annab komisjoni talituse juhile regulaarselt aru nende side- ja infosüsteemi IT turbe riskide profiili kohta ning informaatika peadirektoraadile seotud riskide, riskihaldusmeetmete ja turbemeetmete kohta;

i) konsulteerib asjaomaste komisjoni talituste LISOga IT turvet puudutavates küsimustes;

j) annab kasutajatele juhtnööre side- ja infosüsteemi ja sellega seotud andmete kasutamise ning kohustuste kohta, mis kasutajatel seoses side- ja infosüsteemiga on;

k) taotleb krüpteerimisvolitaja ülesannetes personalihalduse ja julgeoleku peadirektoraadilt volitusi kõigi side- ja infosüsteemide jaoks, mis kasutavad krüpteerimist;

l) konsulteerib ennetavalt komisjoni julgeolekuasutusega iga süsteemi puhul, mis töötleb ELi salastatud teavet;

m) tagab, et dekrüpteerimisvõtmete varukoopiaid hoitakse hoiustuskontol. Krüpteeritud andmete taastamine toimub ainult siis, kui selleks on antud personalihalduse ja julgeoleku peadirektoraadi määratletud raamistiku kohane luba;

n) järgib asjaomaste vastutavate töötlejate juhiseid isikuandmete kaitse kohta ja selle kohta, kuidas kohaldatakse andmekaitse-eeskirju töötlemise turvalisuse suhtes;

o) teavitab informaatika peadirektoraati kõigist eranditest, mis tehakse komisjoni IT turbe põhimõtetest, ja nende põhjustest;

p) annab andmete omaniku ja süsteemi omaniku vahelistest lahendamatutest vaidlustest aru komisjoni talituse juhile, teatab IT turbe intsidentidest asjaomastele sidusrühmadele aegsasti ja otstarbekalt vastavalt nende raskusastmele nii, nagu on sätestatud artiklis 15;

q) tagab, et sisseostetud süsteemide puhul sisaldavad hankelepingud asjakohaseid IT turvet käsitlevaid sätteid ning et sisseostetud side- ja infosüsteemide IT turbe intsidentidest antakse aru vastavalt artiklile 15;

r) tagab jagatud IT-teenuseid pakkuvate side- ja infosüsteemide puhul, et pakutakse kindlaksmääratud turvalisuse taset, see on selgelt dokumenteeritud ja selle side- ja infosüsteemi puhul rakendatakse kindlaks määratud turvalisuse taseme saavutamiseks vajalikke turbemeetmeid.

3. Süsteemide omanikud võivad ametlikult delegeerida kõik oma IT turbega seotud ülesanded või osa neist, kuid nemad jäävad vastutama oma side- ja infosüsteemi IT turbe eest.

Nende vastutusalade ja toimingutega seotud protsesse kirjeldatakse üksikasjalikumalt rakenduseeskirjades.

Artikkel 10

Andmete omanikud

1. Andmete omanik vastutab konkreetse andmekogumi IT turbe eest komisjoni talituse juhi ees ja on vastutusele võetav selle andmekogumi konfidentsiaalsuse, tervikluse ja käideldavuse eest.

2. Seoses sellise andmekogumiga teeb andmete omanik järgmist:

a) tagab, et kõik tema vastutusalas olevad andmekogumid on asjakohaselt liigitatud vastavalt otsustele (EL, Euratom) 2015/443 ja (EL, Euratom) 2015/444;

b) määrab kindlaks infoturbealased vajadused ning teavitab asjaomaseid süsteemide omanikke neist vajadustest;

c) osaleb side- ja infosüsteemide riskide hindamisel;

d) annab andmete omaniku ja süsteemi omaniku vahelistest lahendamatutest vaidlustest aru komisjoni talituse juhile;

e) teatab IT turbe intsidentidest nii, nagu on sätestatud artiklis 15.

3. Andmete omanikud võivad ametlikult delegeerida kõik oma IT turbega seotud ülesanded või osa neist, kuid nemad jäävad vastutama käesolevas artiklis sätestatud küsimuste eest.

Nende vastutusalade ja toimingutega seotud protsesse kirjeldatakse üksikasjalikumalt rakenduseeskirjades.

Artikkel 11

Kohalikud informaatika turvalisuse ametnikud (LISOd)

Seoses IT turbega teeb LISO järgmist:

a) teeb proaktiivselt kindlaks süsteemide omanikud, andmete omanikud ja muud IT turbe valdkonnas vastutavat rolli kandvad isikud komisjoni talitustes ja teavitab neid IT turbe põhimõtetest;

b) suhtleb komisjoni talitus(t)e IT turbega seotud küsimustes informaatika peadirektoraadiga LISO võrgustiku raames;

c) osaleb regulaarselt LISOde kohtumistel;

d) omab ülevaadet infoturbe riski halduse protsessist ning infosüsteemi turbekavade arendamisest ja rakendamisest;

e) nõustab andmete omanikke, süsteemide omanikke ja komisjoni talituste juhte IT turbega seotud küsimustes;

f) teeb koostööd informaatika peadirektoraadiga, et levitada IT turbe häid tavasid ning teeb ettepanekuid konkreetsete teadlikkuse suurendamise ja koolitusprogrammide kohta;

g) annab komisjoni talitus(t)e juhile aru IT turbe, tuvastatud puudujääkide ja parenduste kohta.

Nende vastutusalade ja toimingutega seotud protsesse kirjeldatakse üksikasjalikumalt rakenduseeskirjades.

Artikkel 12

Kasutajad

1. Seoses IT turbega teevad kasutajad järgmist:

a) järgivad IT turbe põhimõtteid ja süsteemi omaniku antud juhtnööre iga side- ja infosüsteemi kasutamise kohta;

b) teatavad IT turbe intsidentidest nii, nagu on sätestatud artiklis 15.

2. Kui komisjoni side- ja infosüsteemi kasutatakse viisil, mis on vastuolus IT turbe põhimõtete või süsteemi omaniku juhtnööridega, võib see tuua kaasa distsiplinaarmenetluse.

Nende vastutusalade ja toimingutega seotud protsesse kirjeldatakse üksikasjalikumalt rakenduseeskirjades.

3. PEATÜKK

TURBENÕUDED JA -KOHUSTUSED

Artikkel 13

Käesoleva otsuse rakendamine

1. Artikli 6 rakenduseeskirjade ning seotud standardite ja suuniste vastuvõtmiseks on vaja, et komisjon otsustaks anda volitused turvalisusküsimuste eest vastutavale komisjoni liikmele.

2. Kõigi muude käesoleva otsusega seotud rakenduseeskirjade ning seotud IT turbe standardite ja suuniste vastuvõtmiseks on vaja, et komisjon otsustaks anda volitused informaatika eest vastutavale komisjoni liikmele.

3. Enne lõigetes 1 ja 2 osutatud rakenduseeskirjade, standardite ja suuniste vastuvõtmist peab need heaks kiitma juhtnõukogu.

Artikkel 14

Järgimiskohustus

1. IT turbe põhimõtetes ja standardites sätestatu järgimine on kohustuslik.

2. Kui IT turbe põhimõtteid ja standardeid ei järgita, võib see kaasa tuua aluslepingute, personalieeskirjade ja liidu muude teenistujate teenistustingimuste kohase distsiplinaarmeetme, lepingulised sanktsioonid ja/või riiklike õigusnormide kohase kohtumenetluse.

3. Informaatika peadirektoraati teavitatakse kõigist eranditest, mis komisjoni IT turbe põhimõtetest tehakse.

4. Kui juhtnõukogu otsustab, et komisjoni side- ja infosüsteeme ähvardab pidev ja vastuvõetamatu risk, esitab informaatika peadirektoraat koostöös süsteemi omanikuga juhtnõukogule vastuvõtmiseks ettepaneku leevendavate meetmete kohta. Muu hulgas võivad need meetmed hõlmata tugevdatud seiret ja aruandlust, teenuste piiramist ja ühenduse lahutamist.

5. Vajaduse korral annab juhtnõukogu korralduse heakskiidetud leevendusmeetmete rakendamiseks. Samuti võib juhtnõukogu soovitada personalihalduse ja julgeoleku peadirektoraadil alustada haldusuurimist. Informaatika peadirektoraat annab juhtnõukogule aru igast olukorrast, mille puhul kohaldati leevendusmeetmeid.

Nende vastutusalade ja toimingutega seotud protsesse kirjeldatakse üksikasjalikumalt rakenduseeskirjades.

Artikkel 15

IT turbe intsidentide käsitlemine

1. Euroopa Komisjonis vastutab IT turbe intsidentidele operatiivse reageerimise peamise suutlikkuse eest informaatika peadirektoraat.

2. Personalihalduse ja julgeoleku peadirektoraat teeb IT turbe intsidentidele reageerimisse panustava sidusrühmana järgmist:

a) tal on taotluse alusel õigus pääseda juurde kõigi intsidentide kannete kokkuvõtvale teabele ja täielikele kannetele;

b) osaleb IT turbe intsidentide kriisihalduse rühmades ja IT turbe hädaolukorras tegutsemise korras;

c) veab suhteid õiguskaitseasutuste ja luureteenistustega;

d) tegeleb küberjulgeoleku alase kohtuekspertiisiga vastavalt otsuse (EL, Euratom) 2015/443 artiklile 11;

e) otsustab, kas on vaja alustada ametlikku uurimist;

f) teavitab informaatika peadirektoraati kõigist IT turbe intsidentidest, mis võivad kujutada ohtu teistele side- ja infosüsteemidele.

3. Informaatika peadirektoraat ning personalihalduse ja julgeoleku peadirektoraat suhtlevad omavahel regulaarselt, et vahetada infot ja koordineerida ametlikku uurimist vajavate turbeintsidentide, eeskätt IT turbe intsidentide käsitlemist.

4. Vajaduse korral võib Euroopa institutsioonide, organite ja asutuste infoturbeintsidentidega tegeleva rühma („CERT-EU“) intsidentide koordineerimise teenuseid kasutada intsidentide käsitlemise protsessi toetamiseks ja teadmiste jagamiseks teiste mõjutatud ELi institutsioonide ja asutustega.

5. IT turbe intsidendiga seotud süsteemi omanikud teevad järgmist:

a) teavitavad oma talituste juhte, informaatika peadirektoraati, personaliküsimuste peadirektoraati, LISOt ja vajaduse korral ka andmete omanikku viivitamata igast olulisemast IT turbe intsidendist, eeskätt juhul, kui sellega kaasneb andmete konfidentsiaalsuse rikkumine;

b) teeb intsidente käsitleva teabevahetuse, intsidentidele reageerimise ja nende heastamise vallas koostööd asjaomaste komisjoni ametivõimudega ja järgib nende juhiseid.

6. Kasutajad teatavad kõigist tegelikest või kahtlustatavatest IT turbe intsidentidest aegsasti asjaomasele IT kasutajatoele.

7. Andmete omanikud teatavad kõigist tegelikest või kahtlustatavatest IT turbe intsidentidest aegsasti asjaomasele IT turbe intsidentidele reageerimise rühmale.

8. Informaatika peadirektoraat, keda toetavad muud panustavad sidusrühmad, vastutab selliste avastatud IT turbe intsidentide käsitlemise eest, mis puudutavad komisjoni side- ja infosüsteeme, välja arvatud sisseostetavaid süsteeme.

9. Informaatika peadirektoraat teavitab IT turbe intsidentidest komisjoni talitusi, keda need puudutavad, asjaomaseid LISOsid ja vajaduse korral ka CERT-EUd, lähtudes teadmisvajaduse põhimõttest.

10. Informaatika peadirektoraat annab juhtnõukogule regulaarselt aru olulisematest komisjoni side- ja infosüsteeme mõjutanud IT turbe intsidentidest.

11. Asjaomasel LISO-l on taotluse põhjal juurdepääs komisjoni talituse side- ja infosüsteeme puudutavate IT turbe intsidentide andmetele.

12. Olulise IT turbe intsidendi korral on informaatika peadirektoraat kriisiolukorra ohjamise kontaktpunkt, kes koordineerib IT turbe intsidentide kriisiohje rühmi.

13. Hädaolukorras võib informaatika peadirektoraat otsustada käivitada IT turbe hädaolukorras tegutsemise korra. Informaatika peadirektoraat töötab välja hädaolukorras tegutsemise korra, mille peab heaks kiitma juhtnõukogu.

14. Informaatika peadirektoraat annab hädaolukorras tegutsemise korra järgimisest aru juhtnõukogule ja mõjutatud komisjoni talituste juhtidele.

Nende vastutusalade ja toimingutega seotud protsesse kirjeldatakse üksikasjalikumalt rakenduseeskirjades.

4. PEATÜKK

LÕPPSÄTTED

Artikkel 16

Läbipaistvus

Käesolevast otsusest antakse teada komisjoni töötajatele ja kõigile teistele isikutele, kelle suhtes see kehtib, ning otsus avaldatakse *Euroopa Liidu Teatajas*.

Artikkel 17

Seos muude õigusaktidega

Käesoleva otsuse sätted ei piira otsuse (EL, Euratom) 2015/443, otsuse (EL, Euratom) 2015/444, määruse (EÜ) nr 45/2001, Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 1049/2001, ([1]) komisjoni otsuse 2002/47/EÜ, ESTÜ, Euratom, ([2]) Euroopa Parlamendi ja nõukogu määruse (EL, Euratom) nr 883/2013 ([3]) ja otsuse 1999/352/EÜ, ESTÜ, Euratom kohaldamist.

Artikkel 18

Kehtetuks tunnistamine ja üleminekumeetmed

16. augusti 2006. aasta otsus C(2006) 3602 tunnistatakse kehtetuks.

Otsuse C(2006) 3602 artikli 10 alusel vastu võetud rakenduseeskirjad ja IT turbe standardid jäävad jõusse, kui nad ei ole vastuolus käesoleva otsusega, kuni nad asendatakse käesoleva otsuse artikli 13 alusel vastu võetavate rakenduseeskirjade ja standarditega. Kõiki viiteid otsuse C(2006) 3602 artiklile 10 loetakse viidetena käesoleva otsuse artiklile 13.

Artikkel 19

Jõustumine

Käesolev otsus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Brüssel, 10. jaanuar 2017

Komisjoni nimel

president

Jean-Claude JUNCKER

([1]) Euroopa Parlamendi ja nõukogu 30. mai 2001. aasta määrus (EÜ) nr 1049/2001 üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele (EÜT L 145, 31.5.2001, lk 43).

([2]) Komisjoni 23. jaanuari 2002. aasta otsus 2002/47/EÜ, ESTÜ, Euratom, millega muudetakse komisjoni töökorda (EÜT L 21, 24.1.2002, p. 23).

([3]) Euroopa Parlamendi ja nõukogu 11. septembri 2013. aasta määrus (EL, Euratom) nr 883/2013, mis käsitleb Euroopa Pettustevastase Ameti (OLAF) juurdlusi ning millega tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1073/1999 ja nõukogu määrus (Euratom) nr 1074/1999 (ELT L 248, 18.9.2013, lk 1).