ODLUKE

ODLUKA KOMISIJE (EU, Euratom) 2017/46

od 10. siječnja 2017.

o sigurnosti komunikacijskih i informacijskih sustava u Europskoj komisiji

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 249.,

uzimajući u obzir Ugovor o osnivanju Europske zajednice za atomsku energiju,

budući da:

(1) Komunikacijski i informacijski sustavi Komisije sastavni su dio funkcioniranja Komisije te incidenti u području IT sigurnosti mogu ozbiljno utjecati na aktivnosti Komisije i na treće strane, uključujući građane, poduzeća i države članice.

(2) Postoje mnoge prijetnje koje mogu naštetiti povjerljivosti, cjelovitosti i dostupnosti komunikacijskih i informacijskih sustava Komisije i informacija koje se u njima obrađuju. Te prijetnje uključuju nezgode, pogreške, namjerne napade i prirodne događaje te se trebaju prepoznati kao operativni rizici.

(3) Komunikacijski i informacijski sustavi trebaju imati razinu zaštite koja je razmjerna vjerojatnosti, utjecaju i prirodi rizika kojima su izloženi.

(4) IT sigurnost u Komisiji trebala bi jamčiti da CIS-ovi (CIS – *communication and information system*) štite informacije koje se u njima obrađuju te da funkcioniraju kako i kada je potrebno pod nadzorom zakonitih korisnika.

(5) Komisijina politika IT sigurnosti trebala bi se provoditi dosljedno s politikama sigurnosti u Komisiji.

(6) Uprava za sigurnost Glavne uprave za ljudske resurse i sigurnost općenito je odgovorna za sigurnost u Komisiji u okviru nadležnosti i odgovornosti člana Komisije odgovornog za sigurnost.

(7) Pristup Komisije trebao bi uzeti u obzir političke inicijative EU-a i zakonodavstvo o mrežnoj i informacijskoj sigurnosti, industrijske standarde i dobre prakse, kako bi se poštovalo sve mjerodavno zakonodavstvo i omogućile interoperabilnost i kompatibilnost.

(8) Službe Komisije odgovorne za komunikacijske i informacijske sustave trebale bi razviti i provesti odgovarajuće mjere te bi se mjere IT sigurnosti za zaštitu komunikacijskih i informacijskih sustava trebale koordinirati unutar Komisije kako bi se osigurala učinkovitost i djelotvornost.

(9) Pravila i postupci za pristup informacijama u kontekstu IT sigurnosti, uključujući rješavanje incidenata u području IT sigurnosti, trebali bi biti razmjerni prijetnji Komisiji ili njezinu osoblju i u skladu s načelima Uredbe (EZ) br. 45/2001 Europskog parlamenta i Vijeća ([1]) o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Unije i o slobodnom kretanju takvih podataka te uzimati u obzir načelo poslovne tajne, kako je propisano člankom 339. UFEU-a.

([1]) Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka (SL L 8, 12.1.2001., str. 1.).

(10) Politike i pravila za komunikacijske i informacijske sustave pri obradi klasificiranih podataka EU-a (EUCI), osjetljivih neklasificiranih podataka i neklasificiranih podataka moraju u potpunosti biti u skladu s odlukama Komisije (EU, Euratom) 2015/443 ([1]) i (EU, Euratom) 2015/444 ([2]).

(11) Potrebno je da Komisija preispita i ažurira odredbe o sigurnosti komunikacijskih i informacijskih sustava kojima se Komisija koristi.

(12) Odluku Komisije C(2006) 3602 stoga treba staviti izvan snage,

DONIJELA JE OVU ODLUKU:

POGLAVLJE 1.

OPĆE ODREDBE

Članak 1.

Predmet i područje primjene

1. Ova se Odluka primjenjuje na sve komunikacijske i informacijske sustave (CIS-ove) koje Komisija posjeduje, nabavlja odnosno kojima upravlja ili rukuje ili koji se u ime Komisije posjeduju, nabavljaju odnosno kojima se u njezino ime upravlja ili rukuje te svako korištenje tim CIS-ovima od strane Komisije.

2. Ovom se Odlukom utvrđuju osnovna načela, ciljevi, organizacija i odgovornosti u pogledu sigurnosti tih CIS-ova, osobito za službe Komisije koje posjeduju i nabavljaju CIS-ove i koje njima upravljaju ili rukuju, uključujući i CIS-ove koje pruža unutarnji pružatelj usluga informatičke tehnologije. Kada CIS pruža, posjeduje ili kada njime upravlja ili rukuje vanjska strana na temelju bilateralnoga sporazuma ili ugovora s Komisijom, uvjeti sporazuma ili ugovora moraju biti u skladu s ovom Odlukom.

3. Ova se Odluka primjenjuje na sve službe i izvršne agencije Komisije. Kada se CIS-om Komisije služe druga tijela ili institucije na temelju bilateralnoga sporazuma s Komisijom, uvjeti sporazuma ili ugovora moraju biti u skladu s ovom Odlukom.

4. Bez obzira na posebne napomene koje se odnose na određene skupine osoblja, ova se Odluka primjenjuje na članove Komisije, na osoblje Komisije na koje se primjenjuje Pravilnik o osoblju za dužnosnike Europske unije („Pravilnik o osoblju") i Uvjeti zaposlenja ostalih službenika Europske unije („Uvjeti zaposlenja") ([3]), na nacionalne stručnjake upućene na rad u Komisiji („UNS-ovi") ([4]), na vanjske pružatelje usluga i njihovo osoblje, na pripravnike i sve osobe koje imaju pristup komunikacijskom i informacijskom sustavu koji je u području primjene ove Odluke.

5. Ova će se Odluka primjenjivati na Europski ured za borbu protiv prijevara (OLAF), u onoj mjeri u kojoj je to u skladu sa zakonodavstvom Unije i Odlukom Komisije 1999/352/EZ, EZUČ, Euratom ([5]). Konkretno, mjere predviđene ovom Odlukom, uključujući upute, inspekcije, istrage i istovrsne mjere, ne smiju se primjenjivati na CIS Ureda gdje to nije spojivo s neovisnošću istražne funkcije toga Ureda i/ili povjerljivošću podataka koje je Ured pribavio pri izvršavanju te funkcije.

Članak 2.

Definicije pojmova

Za potrebe ove Odluke primjenjuju se sljedeće definicije:

1. „Odgovoran" znači odgovarati za mjere, odluke i djelovanje.

([1]) Odluka Komisije (EU, Euratom) 2015/443 od 13. ožujka 2015. o sigurnosti u Komisiji (SL L 72, 17.3.2015., str. 41.).
([2]) Odluka Komisije (EU, Euratom) 2015/444 od 13. ožujka 2015. o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a (SL L 72, 17.3.2015., str. 53.).
([3]) Utvrđeno Uredbom Vijeća (EEZ, Euratom, EZUČ) br. 259/68 od 29. veljače 1968. kojom se utvrđuje Pravilnik o osoblju za dužnosnike i Uvjeti zaposlenja ostalih službenika Europskih zajednica i kojom se uvode posebne mjere koje se privremeno primjenjuju na dužnosnike Komisije (SL L 56, 4.3.1968., str. 1.).
([4]) Odluka Komisije od 12. studenoga 2008. o upućivanju nacionalnih stručnjaka i nacionalnih stručnjaka na stručnom osposobljavanje u Komisiju (C(2008) 6866 final).
([5]) Odluka Komisije 1999/352/EZ, EZUČ, Euratom od 28. travnja 1999. o osnivanju Europskog ureda za borbu protiv prijevara (OLAF) (SL L 136, 31.5.1999., str. 20.).

2. „CERT-EU” je tim za hitne računalne intervencije institucija i agencija EU-a. Njegova je misija pomoći europskim institucijama da se zaštite od namjernih i zlonamjernih napada koji bi ugrozili cjelovitost njihovih sredstava informacijske tehnologije i ugrozili interese EU-a. Opseg aktivnost CERT-EU-a obuhvaća prevenciju, otkrivanje, odgovor i oporavak.

3. „Služba Komisije” znači bilo koja glavna uprava ili služba Komisije ili kabinet člana Komisije.

4. „Sigurnosno tijelo Komisije” odnosi se na ulogu utvrđenu u Odluci (EU, Euratom) 2015/444.

5. „Komunikacijski i informacijski sustav” ili „CIS” znači svaki sustav koji omogućuje postupanje s podacima u elektroničkom obliku, uključujući sva sredstva potrebna za njegovo funkcioniranje, kao i infrastrukturu, organizaciju, osoblje i informacijske resurse. Ta definicija uključuje poslovne aplikacije, zajedničke IT usluge, izdvojene sustave i uređaje krajnjih korisnika.

6. „Korporativni upravni odbor” (*Corporate Management Board,* CMB) pruža najvišu razinu korporativnog upravnog nadzora nad operativnim i administrativnim pitanjima u Komisiji.

7. „Vlasnik podataka” znači pojedinac odgovoran za osiguravanje zaštite i korištenje određenim skupom podataka kojim rukuje CIS.

8. „Skup podataka” znači skup informacija koji se upotrebljava u određenom poslovnom procesu ili aktivnosti Komisije.

9. „Postupak u slučaju nužde” znači unaprijed utvrđeni skup metoda i odgovornosti za djelovanje u hitnim situacijama kako bi se spriječile velike posljedice za Komisiju.

10. „Politika informacijske sigurnosti” znači skup ciljeva u području informacijske sigurnosti koji su utvrđeni, ostvareni i provjereni ili koje treba utvrditi, ostvariti i provjeriti. Obuhvaća, no nije ograničena na, odluke (EU, Euratom) 2015/444 i (EU, Euratom) 2015/443.

11. „Upravljački odbor za informacijsku sigurnost” (ISSB) znači upravljačko tijelo koje podupire korporativni upravni odbor u njegovim zadacima koji se odnose na IT sigurnost.

12. „Unutarnji pružatelj IT usluge” znači služba Komisije koja pruža zajedničke IT usluge.

13. „IT sigurnost” ili „sigurnost CIS-a” znači očuvanje povjerljivosti, cjelovitosti i dostupnosti CIS-ova i skupova podataka koje obrađuju.

14. „Smjernice za IT sigurnost” sastoje se od preporučenih, no dobrovoljnih mjera koje se provode za potporu standardima IT sigurnosti ili služe kao referenca kada ne postoji primjenljivi standard.

15. „Incident povezan s IT sigurnosti” znači događaj koji bi mogao nepovoljno utjecati na povjerljivost, cjelovitost ili dostupnost CIS-a.

16. „Mjera IT sigurnosti” znači tehnička ili organizacijska mjera kojoj je cilj ublažiti rizike IT sigurnosti.

17. „Potreba u pogledu IT sigurnosti” znači precizna i nedvosmislena definicija razina povjerljivosti, cjelovitosti i dostupnosti povezana s pojedinom informacijom ili IT sustavom radi utvrđivanja potrebne razine zaštite.

18. „Cilj u području IT sigurnosti” znači izjava o namjeri sprječavanja određenih prijetnji i/ili zadovoljavanja određenih organizacijskih sigurnosnih zahtjeva ili pretpostavki.

19. „Plan IT sigurnosti” znači dokumentacija o mjerama IT sigurnosti koje su potrebne za ispunjavanje potreba u pogledu IT sigurnosti CIS-a.

20. „Politika IT sigurnosti” znači skup ciljeva u području IT sigurnosti, koji su utvrđeni, ostvareni i provjereni ili koje treba utvrditi, ostvariti i provjeriti. Obuhvaća ovu Odluku i njezina provedbena pravila.

21. „Zahtjev u pogledu IT sigurnosti” znači potreba u pogledu IT sigurnosti formalizirana u prethodno definiranom postupku.

22. „Rizik za IT sigurnost” znači učinak koji bi prijetnja IT sigurnosti mogla imati na CIS ako bi se iskoristila slaba točka. Kao takav, rizik za IT sigurnost karakteriziraju dva čimbenika: 1. nesigurnost, tj. vjerojatnost da će prijetnja IT sigurnosti prouzročiti neželjeni događaj, i 2. utjecaj, tj. posljedice koje bi takav neželjeni događaj mogao imati za CIS.

23. „Standardi IT sigurnosti” znače određene obvezne mjere IT sigurnosti koje olakšavaju izvršenje i podupiru politiku IT sigurnosti.

24. „Strategija IT sigurnosti” znači skup projekata i aktivnosti koje su namijenjene postizanju ciljeva Komisije i koje treba uspostaviti, provesti i provjeriti.

25. „Prijetnja IT sigurnosti” znači čimbenik koji bi mogao dovesti do neželjenog događaja koji bi CIS-u mogao nanijeti štetu. Takve prijetnje mogu biti slučajne ili namjerne, a karakteriziraju ih prijeteći elementi, mogući ciljevi i načini napada.

26. „Lokalni službenik za informacijsku sigurnost” ili „LISO” znači odgovorni službenik za vezu u području IT sigurnosti u službi Komisije.

27. „Osobni podaci”, „obrada osobnih podataka”, „voditelj obrade” i „sustav datoteka osobnih podataka” imaju isto značenje kao u Uredbi (EZ) br. 45/2001, a posebno kao u članku 2.

28. „Obrada informacija” znači sve funkcije CIS-a u pogledu skupova podataka, uključujući stvaranje, izmjene, prikazivanje, pohranjivanje, prijenos, brisanje ili arhiviranje informacija. Obrada informacija korisnicima se može pružiti preko CIS-a kao skup funkcionalnosti i kao IT usluge drugim CIS-ovima.

29. „Poslovna tajna” znači zaštita poslovnih podataka koji su obuhvaćeni obvezom čuvanja poslovne tajne, osobito podataka o poduzećima, njihovim poslovnim odnosima ili troškovima, kako je utvrđeno u članku 339. UFEU-a.

30. „Odgovoran” znači biti obvezan postupati i odlučivati kako bi se postigli potrebni ciljevi.

31. „Sigurnost u Komisiji” znači sigurnost osoba, imovine i podataka u Komisiji, a osobito fizička cjelovitost osoba i imovine, cjelovitost, povjerljivost i dostupnost podataka i komunikacijskih i informacijskih sustava te nesmetan rad Komisije.

32. „Zajednička IT usluga” znači usluga koja se CIS-om pruža drugim CIS-ovima pri obradi informacija.

33. „Vlasnik sustava” znači pojedinac odgovoran za sveukupnu nabavu, razvoj, integraciju, izmjene, rad, održavanje i povlačenje CIS-a.

34. „Korisnik” znači pojedinac koji se koristi funkcionalnostima koje pruža CIS, unutar ili izvan Komisije.

Članak 3.

Načela IT sigurnosti u Komisiji

1. IT sigurnost u Komisiji zasniva se na načelima zakonitosti, transparentnosti, razmjernosti i odgovornosti.

2. Pitanja IT sigurnosti uzimaju se u obzir od početka razvoja i provedbe CIS-ova Komisije. U tu su svrhu uključene Glavna uprava za informatiku i Glavna uprava za ljudske resurse, svaka u svojim područjima nadležnosti.

3. Učinkovitom IT sigurnošću osigurava se primjerena razina:

(a) autentičnosti: jamstvo da su podaci točni i da potječu iz dobronamjernih (*bona fide*) izvora;

(b) raspoloživosti: podaci su dostupni i mogu se upotrebljavati na zahtjev ovlaštenog subjekta;

(c) povjerljivosti: podaci se ne otkrivaju neovlaštenim osobama, subjektima ni procesima;

(d) cjelovitosti: štiti se točnost i cjelovitost sredstava i podataka;

(e) nepobitnosti: može se dokazati da se dogodila određena radnja ili da je nastupio određeni događaj tako da se to kasnije ne može poreći;

(f) zaštite osobnih podataka: pruža se primjerena zaštita mjera u pogledu osobnih podataka u potpunosti u skladu s Uredbom (EZ) br. 45/2001;

(g) čuvanja poslovne tajne: štite se vrste informacija koje su obuhvaćene obvezom čuvanja poslovne tajne, osobito informacije o poduzećima, njihovim poslovnim odnosima ili troškovima, kako je utvrđeno u članku 339. UFEU-a.

4. IT sigurnost temelji se na postupku upravljanja rizikom. Taj je postupak usmjeren na utvrđivanje razine rizika za IT sigurnost i definiranje sigurnosnih mjera kako bi se takvi rizici smanjili na primjerenu razinu te uz razmjeran trošak.

5. Svi se CIS-ovi identificiraju, dodjeljuju vlasniku sustava i evidentiraju u inventaru.

6. Sigurnosni zahtjevi CIS-ova utvrđuju se na temelju njihovih sigurnosnih potreba te sigurnosnih potreba informacija koje obrađuju. CIS koji pruža usluge drugim CIS-ovima može biti namijenjen podupiranju određene razine sigurnosnih potreba.

7. Planovi IT sigurnosti i mjere IT sigurnosti moraju biti razmjerni sigurnosnim potrebama CIS-a.

Postupci koji se odnose na ta načela i aktivnosti detaljnije se utvrđuju u provedbenim pravilima.

POGLAVLJE 2.

ORGANIZACIJA I NADLEŽNOSTI

Članak 4.

Korporativni upravni odbor

Korporativni upravni odbor ima cjelokupnu nadležnost za upravljanje IT sigurnošću kao cjelinom unutar Komisije.

Članak 5.

Upravljački odbor za informacijsku sigurnost (ISSB)

1. ISSB-om predsjeda zamjenik glavnog tajnika nadležnog za upravljanje IT sigurnošću u Komisiji. Njegovi članovi predstavljaju poslovne, tehnološke i sigurnosne interese u odjelima Komisije i uključuju predstavnike Glavne uprave za informatiku, Glavne uprave za ljudske resurse i sigurnost, Glavne uprave za proračun i, prema načelu rotacije svake dvije godine, predstavnike četiriju drugih uključenih odjela Komisije u čijem radu IT sigurnost ima veliku važnost. Članovi su osobe na višim rukovodećim položajima.

2. ISSB podupire korporativni upravni odbor u njegovim zadacima koji se odnose na IT sigurnost. ISSB ima operativnu nadležnost za upravljanje IT sigurnošću kao cjelinom unutar Komisije.

3. ISSB preporučuje Komisijinu politiku IT sigurnosti koju donosi Komisija.

4. ISSB svake dvije godine preispituje upravljačka pitanja i pitanja povezana sa sigurnošću, uključujući ozbiljne incidente u području IT sigurnosti, i o tome izvješćuje korporativni upravni odbor.

5. ISSB prati i preispituje sveukupnu provedbu ove Odluke i o njoj izvješćuje korporativni upravni odbor.

6. ISSB na prijedlog Glavne uprave za informatiku preispituje, odobrava i prati provedbu postojeće strategije IT sigurnosti. ISSB o tome izvješćuje korporativni upravni odbor.

7. ISSB prati, ocjenjuje i kontrolira stanje u području upravljanja rizikom u pogledu korporativnih informacija i ima ovlast izdati formalne zahtjeve za poboljšanja kad god je to potrebno.

Postupci koji se odnose na te odgovornosti i aktivnosti detaljnije se utvrđuju u provedbenim pravilima.

Članak 6.

Glavna uprava za ljudske resurse i sigurnost

Kad je riječ o IT sigurnosti, Glavna uprava za ljudske resurse i sigurnost ima sljedeće odgovornosti:

1. osigurava usklađivanje politike IT sigurnosti i Komisijine politike informacijske sigurnosti;

2. uspostavlja okvir za izdavanje odobrenja za upotrebu tehnologija šifriranja za pohranu i razmjenu informacija preko CIS-ova;

3. obavješćuje Glavnu upravu za informatiku o posebnim prijetnjama koje bi mogle imati značajan utjecaj na sigurnost CIS-ova i skupove podataka koje obrađuju;

4. provodi inspekcije IT sigurnosti kako bi se ocijenila sukladnost Komisijinih CIS-ova s politikom sigurnosti te izvješćuje ISSB o rezultatima;

5. uspostavlja okvir za odobrenje pristupa CIS-ovima Komisije iz vanjskih mreža i za povezana primjerena sigurnosna pravila te u bliskoj suradnji s Glavnom upravom za informatiku razvija standarde i smjernice koje se odnose na IT sigurnost;

6. predlaže načela i pravila za eksternalizaciju CIS-ova kako bi se zadržala primjerena kontrola nad sigurnošću informacija;

7. razvija povezane standarde i smjernice za IT sigurnost u vezi s člankom 6. u bliskoj suradnji s Glavnom upravom za informatiku.

Postupci koji se odnose na te odgovornosti i aktivnosti detaljnije se utvrđuju u provedbenim pravilima.

Članak 7.

Glavna uprava za informatiku

Kad je riječ o sveukupnoj IT sigurnosti Komisije, Glavna uprava za informatiku ima sljedeće odgovornosti:

1. razvija standarde i smjernice za IT sigurnost, osim kako je predviđeno člankom 6., u bliskoj suradnji s Glavnom upravom za ljudske resurse i sigurnost, kako bi se osigurala dosljednost između politike IT sigurnosti i Komisijine politike informacijske sigurnosti te ih predlaže ISSB-u;

2. ocjenjuje metode, postupke i ishode u pogledu upravljanja rizicima IT sigurnosti svih službi Komisije i o tome redovito izvješćuje ISSB;

3. predlaže kontinuiranu strategiju IT sigurnosti koju pregledava i odobrava ISSB i zatim donosi korporativni upravni odbor te predlaže program, uključujući planiranje projekata i aktivnosti za provedbu strategije IT sigurnosti;

4. prati izvršavanje Komisijine strategije IT sigurnosti i o tome redovito izvješćuje ISSB;

5. prati rizike u području IT sigurnosti i mjere IT sigurnosti provedene u CIS-ovima i o tome redovito izvješćuje ISSB;

6. redovito izvješćuje ISSB o sveukupnoj provedbi i usklađenosti s ovom Odlukom;

7. nakon savjetovanja s Glavnom upravom za ljudske resurse i sigurnost zahtijeva od vlasnika sustava da poduzmu određene mjere IT sigurnosti kako bi se za CIS-ove Komisije ublažili rizici u području IT sigurnosti;

8. osigurava postojanje odgovarajućeg kataloga usluga IT sigurnosti Glavne uprave za informatiku koje su dostupne vlasnicima sustava i vlasnicima podataka kako bi ispunili svoje odgovornosti u pogledu IT sigurnosti i poštovali politike i standarde IT sigurnosti;

9. vlasnicima sustava i podataka osigurava odgovarajuću dokumentaciju te se po potrebi savjetuje s njima o mjerama IT sigurnosti koje su provedene za njihove IT usluge kako bi se olakšalo usklađivanje s politikom IT sigurnosti i pružila podrška vlasnicima sustava pri upravljanju IT rizicima;

10. organizira redovite sastanke lokalnih službenika za informacijsku sigurnost i podupire ih u izvršavanju njihovih zadataka;

11. utvrđuje potrebe izobrazbe i koordinira programe izobrazbe o IT sigurnosti u suradnji sa službama Komisije te razvija, provodi i koordinira kampanje za podizanje razine svijesti o IT sigurnosti u bliskoj suradnji s Glavnom upravom za ljudske resurse;

12. osigurava da su vlasnici sustava, vlasnici podataka i nositelji drugih funkcija s odgovornostima u području IT sigurnosti u službama Komisije upoznati s politikom IT sigurnosti;

13. obavješćuje Glavnu upravu za ljudske resurse i sigurnost o određenim prijetnjama IT sigurnosti, incidentima i iznimkama od Komisijine politike IT sigurnosti koje su prijavili vlasnici sustava, a koji bi mogli imati znatan utjecaj na sigurnost u Komisiji;

14. u pogledu svoje uloge kao unutarnjeg pružatelja IT usluge, Komisiji dostavlja katalog zajedničkih IT usluga kojima se pružaju utvrđene razine sigurnosti. To se izvršava sustavnom procjenom, upravljanjem i praćenjem rizika u području IT sigurnosti kako bi se provele sigurnosne mjere radi dostizanja utvrđene sigurnosne razine.

Povezani postupci i detaljnije odgovornosti dodatno će se definirati u provedbenim pravilima.

Članak 8.

Službe Komisije

U pogledu IT sigurnosti u svojoj službi svaki načelnik službe ima sljedeće dužnosti:

1. službeno imenuje vlasnika sustava za svaki CIS, koji je dužnosnik ili član privremenog osoblja i koji će biti nadležan za IT sigurnost dotičnog CIS-a, i službeno imenuje vlasnika podataka za svaki skup podataka kojim upravlja CIS, a koji mora pripadati administrativnom subjektu koji ima ulogu voditelja obrade podataka za skupove podataka koji podliježu Uredbi (EZ) br. 45/2001;

2. službeno imenuje lokalnog službenika za informacijsku sigurnost koji može izvršavati odgovornosti neovisno o vlasniku sustava i vlasniku podataka. Lokalni službenik za informacijsku sigurnost može biti imenovan za jednu službu Komisije ili više njih;

3. osigurava izradu i provedbu odgovarajućih procjena rizika u području IT sigurnosti i planova IT sigurnosti;

4. osigurava da se Glavnoj upravi za informatiku redovito dostavlja sažetak rizika i mjera u području IT-a;

5. osigurava, uz potporu Glavne uprave za informatiku, uspostavljanje odgovarajućih procesa, postupaka i rješenja kako bi se osiguralo učinkovito otkrivanje i rješavanje incidenata povezanih s IT sigurnosti koji se odnose na CIS-ove i izvješćivanje o njima;

6. u kriznim situacijama povezanima s IT sigurnosti pokreće postupak u slučaju nužde;

7. ima krajnju odgovornost za IT sigurnost, uključujući odgovornosti vlasnika sustava i vlasnika podataka;

8. preuzima rizike koji se odnose na vlastiti CIS i skupove podataka;

9. rješava sve nesporazume između vlasnika podataka i vlasnika sustava te u slučaju daljnjeg nesporazuma rješavanje tog pitanja prepušta ISSB-u;

10. osigurava provedbu planova IT sigurnosti i mjera IT sigurnosti te prikladno upravljanje rizicima.

Postupci koji se odnose na te odgovornosti i aktivnosti detaljnije se utvrđuju u provedbenim pravilima.

Članak 9.

Vlasnici sustava

1. Vlasnik sustava odgovoran je za IT sigurnost CIS-a te podnosi izvješća načelniku službe Komisije.

2. Vlasnik sustava u pogledu IT sigurnosti ima sljedeće obveze:

(a) osigurava usklađenost CIS-a s politikom IT sigurnosti;

(b) osigurava točno evidentiranje CIS-a u relevantnom inventaru;

(c) procjenjuje rizike u području IT sigurnosti i utvrđuje potrebe u pogledu IT sigurnosti za svaki CIS u suradnji s vlasnicima podataka te u dogovoru s Glavnom upravom za informatiku;

(d) izrađuje plan sigurnosti, uključujući, prema potrebi, pojedinosti o procijenjenim rizicima i sve dodatne sigurnosne mjere koje su potrebne;

(e) provodi odgovarajuće mjere IT sigurnosti razmjerne utvrđenim rizicima u području IT sigurnosti i prati preporuke koje je potvrdio ISSB;

(f) utvrđuje sve zavisnosti o drugim CIS-ovima ili zajedničkim IT uslugama i prema potrebi provodi sigurnosne mjere na temelju razina sigurnosti koje su predložene tim CIS-ovima ili zajedničkim IT uslugama;

(g) upravlja rizicima u području IT sigurnosti i prati ih;

(h) redovito izvješćuje načelnika službe Komisije o profilu rizičnosti u pogledu IT sigurnosti svojeg CIS-a te izvješćuje Glavnu upravu za informatiku o povezanim rizicima, aktivnostima upravljanja rizikom i poduzetim sigurnosnim mjerama;

(i) savjetuje se o aspektima IT sigurnosti s lokalnim službenikom za informacijsku sigurnost u relevantnim službama Komisije;

(j) izdaje upute korisnicima o uporabi CIS-a i povezanim podacima te o odgovornostima korisnika povezanima s CIS-om;

(k) traži odobrenje Glavne uprave za ljudske resurse i sigurnost, koja djeluje kao tijelo za šifriranje (*Crypto Authority*), za svaki CIS koji upotrebljava tehnologije šifriranja;

(l) unaprijed se savjetuje sa sigurnosnim tijelom Komisije u vezi sa svim sustavima koji obrađuju klasificirane informacije EU-a;

(m) osigurava pohranjivanje sigurnosnih kopija svih ključeva za dešifriranje na pričuvnom računu. Oporavak šifriranih podataka provodi se samo kada je odobren u skladu s okvirom koji je utvrdila Glavna uprava za ljudske resurse i sigurnost;

(n) poštuje sve upute relevantnih voditelja obrade podataka povezane sa zaštitom osobnih podataka i primjenom pravila o zaštiti podataka na sigurnost obrade;

(o) obavješćuje Glavnu upravu za informatiku o svim iznimkama od Komisijine politike IT sigurnosti, uključujući relevantna obrazloženja;

(p) izvješćuje načelnika Komisijine službe o svim nerješivim nesporazumima između vlasnika podataka i vlasnika sustava i prema potrebi relevantnim dionicima pravodobno prenosi informacije o incidentima u području IT sigurnosti, kako je primjereno s obzirom na njihovu težinu u skladu s člankom 15.;

(q) osigurava da se u ugovore o eksternalizaciji za eksternalizirane sustave uključe primjerene odredbe o IT sigurnosti te da se o incidentima u području IT sigurnosti koji se događaju u eksternaliziranim CIS-ovima izvješćuje u skladu s člankom 15.;

(r) za CIS-ove koji pružaju zajedničke IT usluge osigurava da se pruža i jasno dokumentira utvrđena razina sigurnosti te da se za taj CIS provode sigurnosne mjere radi dostizanja utvrđene razine sigurnosti.

3. Vlasnici sustava mogu formalno delegirati neke ili sve svoje zadatke u vezi s IT sigurnošću, no ostaju odgovorni za IT sigurnost svojega CIS-a.

Postupci koji se odnose na te odgovornosti i aktivnosti detaljnije se utvrđuju u provedbenim pravilima.

Članak 10.

Vlasnici podataka

1. Vlasnik podataka odgovara za IT sigurnost određenog skupa podataka načelniku Komisijine službe te je odgovoran za povjerljivost, cjelovitost i dostupnost skupa podataka.

2. Vlasnik sustava u pogledu skupa podataka ima sljedeće obveze:

(a) osigurava da se svi skupovi podataka koji su u njegovoj ili njezinoj nadležnosti klasificiraju na primjeren način u skladu s odlukama (EU, Euratom) 2015/443 i (EU, Euratom) 2015/444;

(b) utvrđuje potrebe u pogledu informacijske sigurnosti i obavješćuje relevantne vlasnike sustava o tim potrebama;

(c) sudjeluje u procjeni rizika u CIS-u;

(d) izvješćuje načelnika Komisijine službe o svim nerješivim nesporazumima između vlasnika podataka i vlasnika sustava;

(e) prenosi informacije o incidentima u području IT sigurnosti kako je predviđeno člankom 15.

3. Vlasnici sustava mogu formalno delegirati neke ili sve svoje zadatke u vezi s IT sigurnošću, no zadržavaju svoje odgovornosti u skladu s ovim člankom.

Postupci koji se odnose na te odgovornosti i aktivnosti detaljnije se utvrđuju u provedbenim pravilima.

Članak 11.

Lokalni službenici za sigurnost

Lokalni službenik za sigurnost u pogledu IT sigurnosti ima sljedeće obveze:

(a) proaktivno utvrđuje politiku IT sigurnosti i o njoj obavješćuje vlasnike sustava, vlasnike podataka i druge nositelje funkcija s odgovornostima u pogledu IT sigurnosti u službama Komisije;

(b) povezuje se s Glavnom upravom za informatiku u sklopu mreže lokalnih službenika za sigurnost u vezi s pitanjima povezanima s IT sigurnosti u službama Komisije;

(c) prisustvuje redovitim sastancima lokalnih službenika za sigurnost;

(d) održava pregled procesa upravljanja rizikom u području informacijske sigurnosti te razvoja i provedbe sigurnosnih planova za informacijski sustav;

(e) savjetuje vlasnike podataka, vlasnike sustava i načelnika Komisijine službe o pitanjima u vezi s IT sigurnošću;

(f) surađuje s Glavnom upravom za informatiku pri širenju dobrih IT praksi i predlaže određene programe podizanja razine svijesti i izobrazbe;

(g) izvješćuje načelnika Komisijine službe o IT sigurnosti, utvrđuje nedostatke i poboljšanja.

Postupci koji se odnose na te odgovornosti i aktivnosti detaljnije se utvrđuju u provedbenim pravilima.

Članak 12.

Korisnici

1. Korisnici u pogledu IT sigurnosti imaju sljedeće obveze:

(a) poštuju politiku IT sigurnosti i upute koje je izdao vlasnik sustava o upotrebi svakog CIS-a;

(b) prenose informacije o incidentima u području IT sigurnosti kako je predviđeno člankom 15.

2. Upotreba Komisijina CIS-a kojom se krše politika IT sigurnosti ili upute koje je izdao vlasnik sustava može dovesti do stegovnog postupka.

Postupci koji se odnose na te odgovornosti i aktivnosti detaljnije se utvrđuju u provedbenim pravilima.

POGLAVLJE 3.

SIGURNOSNI ZAHTJEVI I OBVEZE

Članak 13.

Provedba ove Odluke

1. Donošenje provedbenih pravila koja se odnose na članak 6. i povezanih standarda i smjernica podliježe odluci Komisije o ovlaštenju člana Komisije nadležnog za pitanja sigurnosti.

2. Donošenje svih ostalih provedbenih pravila povezanih s ovom Odlukom i povezanih standarda i smjernica za IT podliježe odluci Komisije o ovlaštenju člana Komisije nadležnog za informatiku.

3. ISSB odobrava provedbena pravila, standarde i smjernice iz stavaka 1. i 2. prije njihova donošenja.

Članak 14.

Obveza u pogledu usklađenosti

1. Poštovanje odredaba iz politike i standarda IT sigurnosti obvezno je.

2. U slučaju nepoštovanja politike i standarda IT sigurnosti može se pokrenuti stegovni postupak u skladu s Ugovorima, Pravilnikom o osoblju i Uvjetima zaposlenja ostalih službenika Europske unije, mogu se primijeniti ugovorne sankcije i/ili se može pokrenuti sudski postupak u skladu s nacionalnim zakonima i propisima.

3. Glavnu upravu za informatiku obavješćuje se o svim iznimkama od politike IT sigurnosti.

4. Ako ISSB odluči da postoji stalni neprihvatljivi rizik za Komisijin CIS, Glavna uprava za informatiku u suradnji s vlasnikom podataka predlaže mjere za smanjenje rizika ISSB-u na odobrenje. Te mjere među ostalim mogu sadržavati pojačano praćenje i izvješćivanje, ograničavanje usluge i prekid.

5. ISSB nameće provedbu odobrenih mjera za smanjenje rizika kad god je to potrebno. ISSB ujedno može glavnom direktoru Glavne uprave za ljudske resurse i informatiku preporučiti otvaranje upravne istrage. Glavna uprava za informatiku izvješćuje ISSB o svim situacijama u kojima su uvedene mjere za smanjenje rizika.

Postupci koji se odnose na te odgovornosti i aktivnosti detaljnije se utvrđuju u provedbenim pravilima.

Članak 15.

Postupanje u slučaju incidenata povezanih s IT sigurnosti

1. Glavna uprava za informatiku nadležna je za pružanje glavnog operativnog odgovora na incidente u području IT sigurnosti unutar Europske komisije.

2. Glavna uprava za ljudske resurse i sigurnost kao dionik koji pridonosi odgovoru na incidente u području IT sigurnosti:

(a) ima pravo na pristup sažetku informacija za sve zapisnike o incidentima i potpunim zapisnicima na zahtjev;

(b) sudjeluje u skupinama za upravljanje kriznim situacijama za incidente IT sigurnosti i postupcima u slučaju nužde u pogledu IT sigurnosti;

(c) zadužena je za odnose s tijelima kaznenog progona i obavještajnim službama;

(d) provodi forenzičke analize u pogledu kibernetičke sigurnosti u skladu s člankom 11. Odluke (EU, Euratom) 2015/443;

(e) odlučuje o potrebi pokretanja službene istrage;

(f) obavješćuje Glavnu upravu za informatiku o svim incidentima u području IT sigurnosti koji mogu predstavljati rizik drugim CIS-ovima.

3. Glavna uprava za informatiku i Glavna uprava za ljudske resurse i sigurnost održavaju redovitu komunikaciju kojom razmjenjuju informacije i koordiniraju postupanje u slučaju sigurnosnih incidenata, osobito u slučaju svih incidenata u području IT sigurnosti koji bi mogli zahtijevati službenu istragu.

4. Službe za koordinaciju u slučaju incidenata tima za hitne računalne intervencije europskih institucija, tijela i agencija (CERT-EU) mogu se prema potrebi upotrebljavati za potporu postupku upravljanja incidentima te za razmjenu znanja s drugim institucijama i agencijama EU-a koje bi mogle biti pogođene.

5. Vlasnici sustava uključeni u incidente u području IT sigurnosti dužni su:

(a) odmah obavijestiti načelnika Komisijine službe, Glavnu upravu za informatiku, Glavnu upravu za ljudske resurse, lokalnog službenika za sigurnost i prema potrebi vlasnika podataka o svim većim incidentima u području IT sigurnosti, osobito onima koji uključuju povredu povjerljivosti podataka;

(b) surađivati s relevantnim tijelima Komisije i slijediti njihove upute o obavješćivanju o incidentu, odgovoru na incident i uklanjanju njegovih posljedica.

6. Korisnici pravodobno izvješćuju relevantnu informatičku službu za pomoć o svim stvarnim ili pretpostavljenim incidentima u području IT sigurnosti.

7. Vlasnici podataka pravodobno izvješćuju relevantni tim za odgovor na incidente u području IT sigurnosti o svim stvarnim ili pretpostavljenim incidentima u području IT sigurnosti.

8. Glavna uprava za informatiku nadležna je, uz potporu drugih dionika, za upravljanje svim otkrivenim incidentima u području IT sigurnosti koji se odnose na Komisijine CIS-ove koji nisu eksternalizirani sustavi.

9. Glavna uprava za informatiku izvješćuje pogođene službe Komisije o incidentima u području IT sigurnosti i relevantne lokalne službenike za sigurnost te, po potrebi, tim za hitne računalne intervencije europskih institucija, tijela i agencija (CERT-EU) na temelju načela nužnosti njihova saznanja.

10. Glavna uprava za informatiku redovito izvješćuje ISSB o većim incidentima u području IT sigurnosti koji utječu na Komisijine CIS-ove.

11. Relevantni lokalni službenik za sigurnost na zahtjev ima pristup zapisnicima o incidentima u području IT sigurnosti koji se odnose na CIS službe Komisije.

12. U slučaju većeg incidenta u području IT sigurnosti Glavna uprava za informatiku služi kao kontaktna točka za upravljanje kriznim situacijama na način da koordinira skupine za upravljanje kriznim situacijama za incidente u području IT sigurnosti.

13. Glavni direktor Glavne uprave za informatiku u hitnim slučajevima može odlučiti o pokretanju postupka u slučaju nužde u pogledu IT sigurnosti. Glavna uprava za informatiku razvija postupke u slučaju nužde koje odobrava ISSB.

14. Glavna uprava za informatiku izvješćuje ISSB i načelnike pogođenih službi Komisije o izvršenju postupaka u slučaju nužde.

Postupci koji se odnose na te odgovornosti i aktivnosti detaljnije se utvrđuju u provedbenim pravilima.

POGLAVLJE 4.

ZAVRŠNE ODREDBE

Članak 16.

Transparentnost

O ovoj se Odluci obavješćuje osoblje Komisije i pojedince na koje se odnosi te se objavljuje u *Službenom listu Europske unije*.

Članak 17.

Povezanost s drugim aktima

Odredbama ove Odluke ne dovode se u pitanje Odluka (EU, Euratom) 2015/443, Odluka (EU, Euratom) 2015/444, Uredba (EZ) br. 45/2001, Uredba (EZ) br. 1049/2001 Europskog parlamenta i Vijeća ([1]), Odluka Komisije 2002/47/EZ, EZUČ, Euratom ([2]), Uredba (EU, Euratom) br. 883/2013 Europskog parlamenta i Vijeća ([3]) i Odluka 1999/352/EZ, EZUČ, Euratom.

Članak 18.

Stavljanje izvan snage i prijelazne mjere

Odluka C(2006) 3602 od 16. kolovoza 2006. stavlja se izvan snage.

Provedbena pravila i standardi IT sigurnosti doneseni u skladu s člankom 10. Odluke C(2006) 3602 ostaju na snazi ako nisu u suprotnosti s ovom Odlukom, dok ih se ne zamijeni provedbenim pravilima i standardima koji se donose u skladu s člankom 13. ove Odluke. Svako upućivanje na članak 10. Odluke C(2006) 3602 treba tumačiti kao upućivanje na članak 13. ove Odluke.

Članak 19.

Stupanje na snagu

Ova Odluka stupa na snagu 20. dana nakon objave u *Službenom listu Europske unije*.

Sastavljeno u Bruxellesu 10. siječnja 2017.

Za Komisiju

Predsjednik

Jean-Claude JUNCKER

([1]) Uredba (EZ) br. 1049/2001 Europskog parlamenta i Vijeća od 30. svibnja 2001. o javnom pristupu dokumentima Europskog parlamenta, Vijeća i Komisije (SL L 145, 31.5.2001., str. 43.).

([2]) Odluka Komisije 2002/47/EZ, EZUČ, Euratom od 23. siječnja 2002. o izmjeni njezina Poslovnika (SL L 21, 24.1.2002., str. 23.).

([3]) Uredba (EU, Euratom) br. 883/2013 Europskog parlamenta i Vijeća od 11. rujna 2013. o istragama koje provodi Europski ured za borbu protiv prijevara (OLAF) i stavljanju izvan snage Uredbe (EZ) br. 1073/1999 Europskog parlamenta i Vijeća te Uredbe Vijeća (Euratom) br. 1074/1999 (SL L 248, 18.9.2013., str. 1.).