SKLEPI

SKLEP KOMISIJE (EU, Euratom) 2017/46

z dne 10. januarja 2017

o varnosti komunikacijskih in informacijskih sistemov v Evropski komisiji

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 249 Pogodbe,

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti za atomsko energijo,

ob upoštevanju naslednjega:

(1) Komunikacijski in informacijski sistemi Komisije so sestavni del delovanja Komisije in varnostni incidenti IT lahko močno vplivajo na delovanje Komisije in tretjih strani, tudi posameznikov, podjetij in držav članic.

(2) Obstaja veliko groženj, ki lahko okrnijo zaupnost, celovitost ali dosegljivost komunikacijskih in informacijskih sistemov Komisije ter informacij, ki se obdelujejo v njih. Med temi grožnjami so incidenti, napake, namerni napadi in naravni dogodki, ki jih je treba šteti za operativno tveganje.

(3) Zato je treba za komunikacijske in informacijske sisteme zagotoviti stopnjo zaščite, sorazmerno z verjetnostjo, učinkom in naravo tveganj, ki so jim izpostavljeni.

(4) Varnost IT v Komisiji bi morala zagotavljati, da komunikacijski in informacijski sistemi (KIS) Komisije ščitijo informacije, ki jih obdelujejo, in da delujejo, kot je treba in kadar je treba, pod nadzorom zakonitih uporabnikov.

(5) Politiko Komisije za varnost IT bi bilo treba izvajati tako, da bo skladna z varnostnimi politikami v Komisiji.

(6) Direktorat za varnost Generalnega direktorata za človeške vire in varnost je splošno odgovoren za varnost v Komisiji pod vodstvom in v pristojnosti člana Komisije, odgovornega za varnost.

(7) Pristop Komisije bi moral upoštevati pobude politik in zakonodajo o varnosti omrežij in informacij, skupnih standardov in dobrih praks, moral bi biti skladen z upoštevno zakonodajo ter omogočati interoperabilnost in združljivost.

(8) Službe Komisije, odgovorne za komunikacijske in informacijske sisteme, bi morale zasnovati in izvesti ustrezne ukrepe, varnostne ukrepe na področju IT za zaščito komunikacijskih in informacijskih sistemov pa bi bilo treba uskladiti v vsej Komisiji, da bi zagotovili učinkovitost in uspešnost.

(9) Pri varnosti IT bi pravila in postopki za dostop do informacij, vključno z obvladovanjem varnostnih incidentov, morali biti sorazmerni z grožnjo Komisiji ali njenemu osebju in skladni z načeli iz Uredbe (ES) št. 45/2001 Evropskega parlamenta in Sveta [1] o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Unije in o prostem pretoku takih podatkov ob upoštevanju načela poklicne skrivnosti, kot je določeno v členu 339 PDEU.

[1] Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12.1.2001, str. 1).

(10) Politike in pravila za komunikacijske in informacijske sisteme, ki obdelujejo tajne podatke EU, občutljive netajne podatke in netajne podatke, morajo biti v celoti v skladu s sklepoma Komisije (EU, Euratom) 2015/443 ([1]) in (EU, Euratom) 2015/444 ([2]).

(11) Komisija bi morala pregledati in posodobiti določbe o varnosti komunikacijskih in informacijskih sistemov, ki jih uporablja.

(12) Sklep Komisije C(2006) 3602 bi bilo zato treba razveljaviti –

SPREJELA NASLEDNJI SKLEP:

POGLAVJE 1

SPLOŠNE DOLOČBE

Člen 1

Vsebina in področje uporabe

1. Ta sklep se uporablja za vse komunikacijske in informacijske sisteme (KIS), ki jih ima Komisija v lasti, jih je zagotovila, vodi ali z njimi upravlja oziroma ki so v lasti, se zagotavljajo, vodijo ali upravljajo v imenu Komisije, ter vsako njeno uporabo navedenih KIS.

2. Ta sklep določa osnovna načela, cilje, organizacijo in obveznosti glede varnosti navedenih KIS, zlasti za službe Komisije, ki imajo v lasti, zagotavljajo ali upravljajo KIS, vključno s KIS, ki jih izvaja notranji izvajalec storitev IT. Če zunanji subjekt izvaja KIS ali je ta v njegovi lasti, ga vodi ali upravlja na podlagi dvostranskega sporazuma ali pogodbe s Komisijo, so pogoji sporazuma ali pogodbe skladni s tem sklepom.

3. Ta sklep se uporablja za vse službe Komisije in izvajalske agencije. Če KIS Komisije uporabljajo drugi organi in institucije na podlagi dvostranskega sporazuma ali pogodbe s Komisijo, so pogoji sporazuma ali pogodbe skladni s tem sklepom.

4. Ta sklep se ne glede na posebne navedbe za nekatere skupine osebja uporablja za člane Komisije, osebje Komisije, za katero veljajo Kadrovski predpisi za uradnike Evropske unije (v nadaljnjem besedilu „kadrovski predpisi“) in Pogoji za zaposlitev drugih uslužbencev Evropske unije (v nadaljnjem besedilu „CEOS“) ([3]), napotene nacionalne strokovnjake, dodeljene Komisiji (v nadaljnjem besedilu „SNE“) ([4]), zunanje ponudnike storitev in njihovo osebje, pripravnike in vse posameznike z dostopom do KIS na področju uporabe tega sklepa.

5. Ta sklep se uporablja za Evropski urad za boj proti goljufijam (OLAF), kolikor je to skladno z zakonodajo Unije in Sklepom Komisije 1999/352/ES, ESPJ, Euratom ([5]). Zlasti ukrepi iz tega sklepa, vključno z navodili, inšpekcijskimi pregledi, preiskavami in enakovrednimi ukrepi, se ne smejo uporabljati za KIS Evropskega urada za boj proti goljufijam, če to ni skladno z neodvisnostjo njegove preiskovalne funkcije in zaupnostjo informacij, ki jo je Evropski urad za boj proti goljufijam pridobil pri opravljanju te funkcije.

Člen 2

Opredelitev pojmov

V tem sklepu se uporabljajo naslednje opredelitve pojmov:

1. „odgovoren“ pomeni nositi odgovornost za ukrepe, odločitve in izvedbo;

([1]) Sklep Komisije (EU, Euratom) 2015/443 z dne 13. marca 2015 o varnosti v Komisiji (UL L 72, 17.3.2015, str. 41).
([2]) Sklep Komisije (EU, Euratom) 2015/444 z dne 13. marca 2015 o varnostnih predpisih za varovanje tajnih podatkov EU (UL L 72, 17.3.2015, str. 53).
([3]) Določeni z Uredbo Sveta (EGS, Euratom, ESPJ) št. 259/68 z dne 29. februarja 1968 o določitvi Kadrovskih predpisov za uradnike in Pogojev za zaposlitev drugih uslužbencev Evropskih skupnosti ter posebnih ukrepov, ki se začasno uporabljajo za uradnike Komisije (UL L 56, 4.3.1968, str. 1).
([4]) Sklep Komisije z dne 12. novembra 2008 o določitvi pravil za začasno dodelitev nacionalnih izvedencev in nacionalnih izvedencev na strokovnem usposabljanju (C(2008) 6866 final).
([5]) Sklep Komisije 1999/352/ES, ESPJ, Euratom z dne 28. aprila 1999 o ustanovitvi Evropskega urada za boj proti goljufijam (OLAF) (UL L 136, 31.5.1999, str. 20).

2. „CERT-EU“ je skupina za odzivanje na računalniške grožnje za ustanove in agencije EU. Njena naloga je nuditi pomoč evropskim ustanovam pri zaščiti pred namernimi in zlonamernimi napadi, ki bi okrnili celovitost njihovih sredstev IT in škodovali interesom EU. Področje dejavnosti „CERT-EU“ zajema preprečevanje, odkrivanje, odzivanje in ponovno vzpostavitev;

3. „služba Komisije“ pomeni kateri koli generalni direktorat ali službo Komisije ali kateri koli kabinet člana Komisije;

4. „varnostni organ Komisije“ se nanaša na funkcijo iz Sklepa (EU, Euratom) 2015/444;

5. „komunikacijski in informacijski sistem“ ali „KIS“ pomeni sistem, ki omogoča obravnavanje podatkov v elektronski obliki, vključno z vsemi sestavnimi deli, potrebnimi za delovanje, ter infrastrukturo, organizacijo, osebjem in informacijskimi viri. Ta opredelitev zajema poslovne aplikacije, skupne storitve IT, sisteme, ki jih upravlja zunanji izvajalec, in naprave končnih uporabnikov;

6. „interni upravni odbor“ (*Corporate Management Board*, CMB) izvaja upravljalni nadzor na najvišji ravni nad operativnimi in upravnimi vprašanji v Komisiji;

7. „lastnik podatkov“ pomeni osebo, ki je odgovorna za zagotavljanje zaščite in uporabe posebnega nabora podatkov, s katerim ravna KIS;

8. „nabor podatkov“ pomeni sklop informacij, ki se uporablja za poseben poslovni postopek ali dejavnost Komisije;

9. „postopek v izrednih razmerah“ pomeni vnaprej opredeljen sklop metod in obveznosti za odziv na nujne situacije zaradi preprečevanja hujših posledic za Komisijo;

10. „politika za varnost informacij“ je sklop ciljev za varnost informacij, ki so ali morajo biti določeni, uresničeni ali preverjeni. Med drugim zajema sklepa (EU, Euratom) 2015/444 in (EU, Euratom) 2015/443;

11. „Usmerjevalni odbor za varnost informacij“ (ISSB) pomeni organ upravljanja, ki nudi pomoč internemu upravnemu odboru pri njegovih nalogah, povezanih z varnostjo IT;

12. „notranji ponudnik storitev IT“ pomeni službo Komisije, ki izvaja skupne storitve IT;

13. „varnost IT“ ali „varnost KIS“ pomeni ohranjanje zaupnosti, celovitosti in razpoložljivosti KIS in naborov podatkov, ki jih obdelujejo;

14. „smernice za varnost IT“ so sestavljene iz priporočenih, toda prostovoljnih ukrepov, ki se izvajajo za podporo standardom varnosti IT ali se uporabljajo kot referenca, kadar ni nobenega veljavnega standarda;

15. „varnostni incident IT“ pomeni dogodek, ki bi lahko škodljivo vplival na zaupnost, celovitost ali razpoložljivost KIS;

16. „varnostni ukrep na področju IT“ pomeni tehnični ali organizacijski ukrep za ublažitev tveganja za varnost IT;

17. „varnostna potreba IT“ pomeni natančno in nedvoumno opredelitev stopnje zaupnosti, celovitosti in razpoložljivosti, povezane z informacijo ali sistemom IT, za določitev potrebne ravni zaščite;

18. „cilj glede varnosti IT“ pomeni izjavo o namenu obrambe pred posebnimi grožnjami in/ali izpolnjevanju posebnih organizacijskih zahtev ali domnev glede varnosti;

19. „varnostni načrt IT“ pomeni dokumentacijo o varnostnih ukrepih na področju IT, potrebnih za izpolnitev varnostnih potreb KIS na področju IT;

20. „politika za varnost IT“ je sklop ciljev varnosti IT, ki so ali morajo biti določeni, uresničeni ali preverjeni. Vsebuje ta sklep in njegova izvedbena pravila;

21. „zahteva glede varnosti IT“ pomeni varnostno potrebo na področju IT, ki je bila formalizirana v vnaprej določenem postopku;

22. „tveganje za varnost IT“ pomeni učinek, ki bi ga lahko imela grožnja za varnost IT na KIS, če bi se izkoristila šibka točka. Za tveganje za varnost IT sta značilna dva dejavnika: (1) negotovost, tj. verjetnost, da bo grožnja za varnost IT povzročila nezaželen dogodek, in (2) učinek, tj. posledice, ki bi jih tak nezaželen dogodek lahko imel za KIS;

23. „standardi varnosti IT“ pomeni posebne obvezne varnostne ukrepe na področju IT za izvajanje politike za varnost IT in podpore tej politiki;

24. „strategija varnosti IT“ pomeni sklop projektov in dejavnosti za dosego ciljev Komisije, ki jih je treba določiti, uresničiti in preveriti;

25. „grožnja za varnost IT“ pomeni dejavnik, ki bi lahko povzročil nezaželen dogodek, katerega posledica bi bila škoda v KIS. Take grožnje so lahko naključne ali namerne, zanje pa so značilni grozilni elementi, morebitni cilji in načini napada;

26. „lokalni varnostni uradnik za informatiko“ (*Local Informatics Security Officer*, LISO) pomeni uradnika, ki je v službi Komisije odgovoren za zvezo za varnost IT;

27. „osebni podatki“, „obdelava osebnih podatkov“, „upravljavec“ in „zbirka osebnih podatkov“ imajo isti pomen kot v Uredbi (ES) št. 45/2001, zlasti njenem členu 2;

28. „obdelava podatkov“ pomeni vse funkcije KIS v zvezi z nabori podatkov, vključno z ustvarjanjem, spreminjanjem, prikazovanjem, shranjevanjem, prenosom, brisanjem in arhiviranjem podatkov. KIS lahko obdelavo podatkov opravlja kot sklop funkcij za uporabnike in kot storitve IT za druge KIS;

29. „poklicna skrivnost“ pomeni varstvo poslovnih podatkov, za katere velja obveznost varovanja poslovne skrivnosti, zlasti informacij o podjetjih, njihovih poslovnih odnosih ali sestavinah stroškov, kot so določene v členu 339 PDEU;

30. „odgovoren“ pomeni dolžan ukrepati in sprejemati odločitve za dosego potrebnih ciljev;

31. „varnost v Komisiji“ pomeni varnost oseb, sredstev in podatkov v Komisiji, zlasti fizično celovitost oseb in sredstev, celovitost, zaupnost in razpoložljivost podatkov ter komunikacijskih in informacijskih sistemov ter neovirano opravljanje dejavnosti Komisije;

32. „skupne storitve IT“ pomeni storitve pri obdelavi podatkov, ki jih KIS opravlja za druge KIS;

33. „lastnik sistema“ je posameznik, ki je odgovoren za celotno nabavo, razvoj, združevanje, spreminjanje, upravljanje, vzdrževanje in umik KIS;

34. „uporabnik“ pomeni posameznika znotraj ali zunaj Komisije, ki uporablja funkcijo iz KIS.

Člen 3

Načela za varnost IT v Komisiji

1. Varnost IT v Komisiji temelji na načelih zakonitosti, preglednosti, sorazmernosti in prevzemanja odgovornosti.

2. Vprašanja glede varnosti IT se upoštevajo od vsega začetka razvoja in uvedbe KIS Komisije. V ta namen Generalni direktorat za informatiko in Generalni direktorat za človeške vire in varnost sodelujeta na svojem področju pristojnosti.

3. Učinkovita varnost IT zagotavlja ustrezno stopnjo:

(a) avtentičnosti: zagotovilo, da so podatki pravi in iz zaupanja vrednih virov;

(b) razpoložljivosti: podatki so dostopni in jih je mogoče uporabljati na zahtevo pooblaščenega subjekta;

(c) zaupnosti: podatki se ne razkrijejo nepooblaščenim posameznikom in subjektom ali ne uporabijo v postopkih, kjer to ni dovoljeno;

(d) celovitosti: zagotavljanje točnosti in popolnosti sestavnih delov in podatkov;

(e) nezatajljivosti: zmožnost dokazati, da se je dejanje zgodilo ali da je prišlo do dogodka, tako da tega kasneje ni mogoče zanikati;

(f) varstva osebnih podatkov: izvajanje ustreznih zaščitnih ukrepov v zvezi z osebnimi podatki ob popolnem upoštevanju Uredbe (ES) št. 45/2001;

(g) poklicne skrivnosti: varstvo podatkov, za katere velja obveznost varovanja poslovne skrivnosti, zlasti informacij o podjetjih, njihovih poslovnih odnosih ali sestavinah stroškov, kot so določene v členu 339 PDEU.

4. Varnost IT temelji na postopku obvladovanja tveganja. Cilj tega postopka je določiti ravni tveganj za varnosti IT in opredeliti varnostne ukrepe za ublažitev takih tveganj do ustrezne stopnje in ob sorazmernih stroških.

5. KIS se določi, dodeli lastniku sistema in vnese v evidenco.

6. Varnostne zahteve vseh KIS se ugotovijo na podlagi njihovih varnostnih potreb in varnostnih potreb informacij, ki jih obdelujejo. KIS, ki opravljajo storitve za druge KIS, so lahko zasnovani tako, da podpirajo določene stopnje varnostnih potreb.

7. Varnostni načrti IT in varnostni ukrepi na področju IT so v sorazmerju z varnostnimi potrebami KIS.

Postopki v zvezi s temi načeli in dejavnostmi se podrobneje določijo v izvedbenih pravilih.

POGLAVJE 2

ORGANIZACIJA IN OBVEZNOSTI

Člen 4

Interni upravni odbor

Interni upravni odbor je splošno odgovoren za upravljanje varnosti IT kot celote znotraj Komisije.

Člen 5

Usmerjevalni odbor za varnost informacij (Information Security Steering Board, ISSB)

1. Predsednik ISSB je namestnik generalnega sekretarja, odgovoren za upravljanje varnosti IT v Komisiji. Njegovi člani predstavljajo poslovne, tehnološke in varnostne interese v vseh službah Komisije, med njimi so tudi predstavniki Generalnega direktorata za informatiko, Generalnega direktorata za človeške vire in varnost, Generalnega direktorata za proračun, in, po sistemu rotacije na dve leti, predstavniki še štirih udeleženih služb Komisije, v katerih je varnost IT zelo pomembna za njihovo delovanje. Članstvo je na ravni višjega vodstva.

2. ISSB nudi pomoč internemu upravnemu odboru pri nalogah, povezanih z varnostjo IT. ISSB je operativno odgovoren za upravljanje varnosti IT kot celote znotraj Komisije.

3. ISSB predlaga Komisiji v sprejetje politiko Komisije za varnost IT.

4. ISSB vsaki dve leti pregleda položaj upravljanja in vprašanja o varnosti IT, vključno z resnimi varnostnimi incidenti IT, ter o njih poroča internemu upravnemu odboru.

5. ISSB spremlja in pregleduje celotno izvajanje tega sklepa in o njem poroča internemu upravnemu odboru.

6. ISSB na predlog Generalnega direktorata za informatiko pregleda, odobri in spremlja izvajanje veljavne strategije varnosti IT. ISSB o njej poroča internemu upravnemu odboru.

7. ISSB spremlja, oceni in nadzoruje položaj na področju obvladovanja tveganja glede informacijske varnosti organizacije in je po potrebi pristojen za izdajo formalnih zahtevkov za izboljšave.

Postopki v zvezi s temi obveznostmi in dejavnostmi se podrobneje določijo v izvedbenih pravilih.

Člen 6

Generalni direktorat za človeške vire in varnost

Generalni direktorat za človeške vire in varnost ima glede varnosti IT obveznosti, ki so navedene v nadaljevanju. Direktorat izvaja naslednje naloge:

1. zagotavlja usklajenost politike za varnost IT s politiko Komisije za varnost informacij;

2. določa okvir za dovoljevanje uporabe šifrirnih tehnologij za shranjevanje in sporočanje informacij s strani KIS;

3. obvešča Generalni direktorat za informatiko o posebnih grožnjah, ki bi lahko znatno vplivale na varnost KIS in naborov podatkov, ki jih obdelujejo;

4. izvaja varnostne preglede za oceno upoštevanja varnostne politike v KIS Komisije in o rezultatih poroča ISSB;

5. določi okvir za dovoljevanje dostopa v KIS Komisije iz zunanjih omrežij in z njim povezana ustrezna varnostna pravila ter oblikuje standarde in smernice za varnost IT v tesnem sodelovanju z Generalnim direktoratom za informatiko;

6. predlaga načela in pravila za zunanje izvajanje KIS, da bi ohranil ustrezen nadzor nad varnostjo informacij;

7. oblikuje sorodne standarde in smernice za varnost IT v zvezi s členom 6 v tesnem sodelovanju z Generalnim direktoratom za informatiko.

Postopki v zvezi s temi obveznostmi in dejavnostmi se podrobneje določijo v izvedbenih pravilih.

Člen 7

Generalni direktorat za informatiko

Generalni direktorat za informatiko ima glede splošne varnosti IT Komisije obveznosti, ki so navedene v nadaljevanju. Direktorat izvaja naslednje naloge:

1. oblikuje standarde in smernice za varnost IT, razen kakor je določeno v členu 6, v tesnem sodelovanju z Generalnim direktoratom za človeške vire in varnost, da zagotovi skladnost med politiko za varnost IT in politiko Komisije za varnost informacij, in jih predlaga ISSB;

2. ocenjuje metode, postopke in rezultate obvladovanja tveganja za varnost IT vseh služb Komisije in o tem redno poroča ISSB;

3. predlaga ISSB veljavno strategijo varnosti IT v pregled in odobritev ter v nadaljnje sprejetje v internem upravnem odboru ter predlaga program, vključno z načrtovanjem projektov in dejavnosti za izvajanje strategije varnosti IT;

4. spremlja izvajanje strategije Komisije za varnost IT in o njem redno poroča ISSB;

5. spremlja tveganja za varnost IT in varnostne ukrepe na področju IT, ki jih izvajajo KIS, in o njih redno poroča ISSB;

6. redno poroča ISSB o celotnem izvajanju in upoštevanju tega sklepa;

7. po posvetovanju z Generalnim direktoratom za človeške vire in varnost zahteva od lastnikov sistema, da izvedejo posebne varnostne ukrepe na področju IT za ublažitev tveganj za varnost IT za KIS Komisije;

8. zagotavlja, da je lastnikom sistema in lastnikom podatkov na razpolago ustrezen seznam storitev varnosti IT Generalnega direktorata za informatiko, da lahko izpolnjujejo svoje obveznosti za varnost IT in upoštevajo politiko in standarde za varnost IT;

9. lastnikom sistema in podatkov zagotavlja ustrezno dokumentacijo ter se po potrebi posvetuje z njimi o varnostnih ukrepih na področju IT, ki jih izvajajo za svoje storitve IT, da bi olajšal upoštevanje politike za varnost IT in nudil pomoč lastnikom sistema pri obvladovanju tveganj na področju IT;

10. organizira redna srečanja omrežja LISO in jih podpira pri opravljanju dolžnosti;

11. opredeljuje potrebe po usposabljanju in usklajuje programe usposabljanja na področju varnosti IT s službami Komisije ter v tesnem sodelovanju z Generalnim direktoratom za človeške vire in varnost oblikuje, izvaja in usklajuje kampanje ozaveščanja glede varnosti IT;

12. zagotavlja, da so lastniki sistema, lastniki podatkov in nosilci drugih vlog z obveznostmi glede varnosti IT v službah Komisije seznanjeni s politiko za varnost IT;

13. obvešča GD za človeške vire in varnost o posebnih grožnjah za varnost IT, incidentih in izjemah od politike Komisije za varnost IT, ki so jih uradno sporočili lastniki sistema in ki bi lahko znatno vplivali na varnost v Komisiji;

14. glede na svojo vlogo notranjega izvajalca storitev IT Komisiji predloži seznam skupnih storitev IT, ki omogočajo opredeljene ravni varnosti. To se opravlja s sistematičnim ocenjevanjem, upravljanjem in spremljanjem tveganj za varnost IT s ciljem izvajanja varnostnih ukrepov za dosego opredeljene ravni varnosti.

Sorodni postopki in podrobnejše obveznosti se dodatno opredelijo v izvedbenih pravilih.

Člen 8

Službe Komisije

Vsak vodja službe Komisije glede varnosti IT v svoji službi:

1. za vsak KIS uradno imenuje lastnika sistema, ki je uradnik ali začasni uslužbenec in ki bo odgovoren za varnost IT navedenega KIS, ter uradno imenuje lastnika podatkov za vsak nabor podatkov, s katerim upravlja KIS; imenovani lastnik podatkov mora spadati v upravno enoto, ki je upravljavec podatkov za nabore podatkov, za katere velja Uredba (ES) št. 45/2001;

2. uradno imenuje lokalnega varnostnega uradnika za informatiko (LISO), ki lahko izpolnjuje obveznosti neodvisno od lastnikov sistema in lastnikov podatkov. LISO se lahko imenuje za eno ali več služb Komisije;

3. zagotavlja pripravo in izvajanje ustreznih ocen tveganja za varnost IT in varnostnih načrtov IT;

4. zagotavlja redno poročanje Generalnemu direktoratu za informatiko v obliki povzetka tveganj in ukrepov za varnost IT;

5. ob podpori Generalnega direktorata za informatiko zagotavlja uvedbo ustreznih procesov, postopkov in rešitev za učinkovito odkrivanje varnostnih incidentov IT v zvezi s svojimi KIS, poročanje o njih in njihovo reševanje;

6. v izrednih razmerah v zvezi z varnostjo IT začne postopek za izredne razmere;

7. je na končni stopnji odgovoren za varnost IT, vključno z obveznostmi lastnika sistema in lastnika podatkov;

8. je lastnik tveganj v zvezi s svojimi KIS in nabori podatkov;

9. razrešuje nesoglasja med lastniki podatkov in lastniki sistema, v primeru trajnega nesoglasja pa zadevo preda v reševanje ISSB;

10. zagotavlja izvajanje varnostnih načrtov IT in varnostnih ukrepov na področju IT in ustrezno obvladovanje tveganj.

Postopki v zvezi s temi obveznostmi in dejavnostmi se podrobneje določijo v izvedbenih pravilih.

Člen 9

Lastniki sistema

1. Lastnik sistema odgovarja za varnost IT v KIS in poroča vodji službe Komisije.

2. Lastnik sistema v zvezi z IT:

(a) zagotavlja upoštevanje politike za varnost IT v KIS;

(b) zagotavlja, da je KIS natančno evidentiran v ustrezni evidenci;

(c) v sodelovanju z lastniki podatkov in v posvetovanju z Generalnim direktoratom za informatiko ocenjuje tveganja za varnost IT in določa varnostne potrebe IT za vsak KIS;

(d) pripravlja varnostni načrt, po potrebi tudi s podrobnimi podatki o ocenjenih tveganjih in potrebnih dodatnih varnostnih ukrepih;

(e) izvaja ustrezne varnostne ukrepe na področju IT, ki so v sorazmerju z ugotovljenimi tveganji za varnost IT, in upošteva priporočila, ki jih je odobril ISSB;

(f) ugotavlja odvisnost od drugih KIS ali skupnih storitev IT in izvaja varnostne ukrepe, kot je primerno, na podlagi varnostnih ravni, ki so jih predlagali navedeni KIS ali skupne storitve IT;

(g) obvladuje in spremlja tveganja za varnost IT;

(h) redno poroča vodji službe Komisije o profilu tveganja za varnost IT svojega KIS, Generalnemu direktoratu za informatiko pa poroča o povezanih tveganjih, dejavnostih obvladovanja tveganja in sprejetih varnostnih ukrepih;

(i) se posvetuje z LISO ustreznih služb Komisije o vidikih varnosti IT;

(j) daje navodila uporabnikom o uporabi KIS in povezanih podatkov ter o obveznostih uporabnikov v zvezi s KIS;

(k) zaprosi Generalni direktorat za človeške vire in varnost kot organ za šifrirne metode in izdelke (*Crypto Authority*) za avtorizacijo za vsak KIS, ki uporablja šifrirno tehnologijo;

(l) se predhodno posvetuje z varnostnim organom Komisije o vsakem sistemu, ki obdeluje tajne podatke EU;

(m) zagotavlja hranjenje varnostnih kopij ključev za dešifriranje na računu za hrambo. Obnovitev šifriranih podatkov se izvede samo z odobritvijo v skladu z okvirom, ki ga opredeli Generalni direktorat za človeške vire in varnost;

(n) upošteva navodila ustreznih upravljavcev podatkov za varstvo osebnih podatkov in uporabo pravil o varstvu podatkov glede varnosti obdelave;

(o) uradno obvešča Generalni direktorat za informatiko o izjemah od politike Komisije za varnost IT, vključno z zadevnimi utemeljitvami;

(p) poroča vodji službe Komisije o nerešljivih nesoglasjih med lastnikom podatkov in lastnikom sistema, ustrezne zainteresirane strani pravočasno obvesti o varnostnih incidentih IT, kakor je primerno glede na njihovo resnost v skladu s členom 15;

(q) pri sistemih, ki jih upravlja zunanji izvajalec, zagotavlja, da pogodbe o zunanjem izvajanju vsebujejo ustrezne določbe o varnosti IT in da se o varnostnih incidentih IT v KIS, ki ga upravlja zunanji izvajalec, poroča v skladu s členom 15;

(r) pri KIS, ki opravljajo skupne storitve IT, skrbi za zagotavljanje in ustrezno dokumentiranje opredeljene ravni varnosti ter izvajanje varnostnih ukrepov pri navedenem KIS za dosego opredeljene ravni varnosti.

3. Lastniki sistema lahko nekatere ali vse svoje naloge v zvezi z varnostjo IT uradno prenesejo na druge osebe, vendar ostajajo odgovorni za varnost IT svojih KIS.

Postopki v zvezi s temi obveznostmi in dejavnostmi se podrobneje določijo v izvedbenih pravilih.

Člen 10

Lastniki podatkov

1. Lastnik podatkov je vodji službe Komisije odgovoren za varnost IT posebnega nabora podatkov in je odgovoren tudi za njegovo zaupnost, celovitost in razpoložljivost.

2. V zvezi s tem naborom podatkov lastnik podatkov:

(a) zagotavlja, da so vsi nabori podatkov, za katere je odgovoren, ustrezno razvrščeni v skladu s sklepoma (EU, Euratom) 2015/443 in (EU, Euratom) 2015/444;

(b) opredeljuje potrebe po varnosti informacij in o njih obvešča ustrezne lastnike sistema;

(c) sodeluje pri oceni tveganja v KIS;

(d) poroča vodji službe Komisije o nerešljivih nesoglasjih med lastnikom podatkov in lastnikom sistema;

(e) obvešča o varnostnih incidentih IT v skladu s členom 15.

3. Lastniki podatkov lahko nekatere ali vse svoje naloge pri varnosti IT uradno prenesejo na druge osebe, vendar njihove obveznosti, kot so opredeljene v tem členu, ostajajo nespremenjene.

Postopki v zvezi s temi obveznostmi in dejavnostmi se podrobneje določijo v izvedbenih pravilih.

Člen 11

Lokalni varnostni uradniki za informatiko (LISO)

Lokalni varnostni uradniki za informatiko glede varnosti IT:

(a) proaktivno določajo politiko za varnost IT in o njej obveščajo lastnike sistema, lastnike podatkov in nosilce drugih vlog z obveznostmi glede varnosti IT v službah Komisije;

(b) se glede vprašanj o varnosti IT v službah Komisije povezujejo z Generalnim direktoratom za informatiko kot sestavnim delom mreže LISO;

(c) se udeležujejo rednih sestankov LISO;

(d) ohranjajo pregled nad postopkom obvladovanja tveganja za varnost informacij ter oblikovanjem in izvajanjem varnostnih načrtov za informacijski sistem;

(e) svetujejo lastnikom podatkov, lastnikom sistema in vodjem služb Komisije glede vprašanj o varnosti IT;

(f) sodelujejo z Generalnim direktoratom za informatiko pri širjenju dobrih praks pri varnosti IT in predlagajo posebne programe ozaveščanja in usposabljanja;

(g) poročajo vodjem služb Komisije o varnosti IT ter ugotavljajo pomanjkljivosti in izboljšave.

Postopki v zvezi s temi obveznostmi in dejavnostmi se podrobneje določijo v izvedbenih pravilih.

Člen 12

Uporabniki

1. Uporabniki glede varnosti IT:

(a) upoštevajo politiko za varnost IT in navodila, ki jih za uporabo vsakega KIS daje lastnik sistema;

(b) obveščajo o varnostnih incidentih IT v skladu s členom 15.

2. Kršitev politike za varnost IT ali navodil, ki jih daje lastnik sistema, pri uporabi KIS Komisije je lahko razlog za uvedbo disciplinskega postopka.

Postopki v zvezi s temi obveznostmi in dejavnostmi se podrobneje določijo v izvedbenih pravilih.

POGLAVJE 3

DOLŽNOSTI IN OBVEZNOSTI GLEDE VARNOSTI

Člen 13

Izvajanje tega sklepa

1. Izvedbena pravila za člen 6 ter povezani standardi in smernice bodo sprejeti pod pogojem, da Komisija sklene izdati pooblastilo članu Komisije, odgovornemu za varnostne zadeve.

2. Vsa druga izvedbena pravila v zvezi s tem sklepom ter povezani standardi in smernice bodo sprejeti pod pogojem, da Komisija sklene izdati pooblastilo članu Komisije, odgovornemu za informatiko.

3. Vsa izvedbena pravila, standarde in smernice iz odstavkov 1 in 2 pred sprejetjem odobri ISSB.

Člen 14

Obveznost upoštevanja določb

1. Upoštevanje določb iz politike za varnost IT in standardov je obvezno.

2. Zaradi neupoštevanja politike in standardov za varnost IT se lahko izvedejo disciplinski ukrepi v skladu s Pogodbama, kadrovskimi predpisi in CEOS ter pogodbene sankcije in/ali se začnejo pravni postopki v skladu z nacionalnimi zakoni in predpisi.

3. O kakršnih koli izjemah od politike za varnost IT je treba uradno obvestiti Generalni direktorat za informatiko.

4. Če ISSB sprejme odločitev, da obstaja trajno nesprejemljivo tveganje za KIS Komisije, Generalni direktorat za informatiko v sodelovanju z lastnikom sistema predlaga ukrepe za ublažitev tveganja v odobritev ISSB. Med temi ukrepi so lahko tudi okrepljeno spremljanje in poročanje, omejitev storitev ali odklop.

5. ISSB po potrebi naloži izvedbo odobrenih ukrepov za ublažitev tveganja. ISSB lahko generalnemu direktorju Generalnega direktorata za človeške vire in varnost priporoči tudi uvedbo upravne preiskave. Generalni direktorat za informatiko poroča ISSB o vsakem položaju, v katerem se naloži izvedba ukrepov za ublažitev tveganja.

Postopki v zvezi s temi obveznostmi in dejavnostmi se podrobneje določijo v izvedbenih pravilih.

Člen 15

Obvladovanje varnostnih incidentov IT

1. Generalni direktorat za informatiko je odgovoren za zagotovitev glavne zmogljivosti za operativni odziv na varnostni incident IT znotraj Evropske komisije.

2. Generalni direktorat za človeške vire in varnost kot sodelujoča zainteresirana stran pri odzivu na varnostni incident IT:

(a) ima pravico do dostopa do povzetka informacij za vse evidence incidentov in na zahtevo do celotne evidence;

(b) sodeluje v kriznih skupinah za odzivanje na varnostne incidente IT in v postopkih za izredne razmere v zvezi z varnostjo IT;

(c) je pristojen za stike z organi kazenskega pregona in obveščevalnimi službami;

(d) opravlja forenzično analizo v zvezi s kibernetsko varnostjo v skladu s členom 11 Sklepa (EU, Euratom) 2015/443;

(e) odloča o potrebi po uvedbi uradne preiskave;

(f) obvešča Generalni direktorat za informatiko o varnostnih incidentih IT, ki bi lahko pomenili tveganje za druge KIS.

3. Med Generalnim direktoratom za informatiko in Generalnim direktoratom za človeške vire in varnost poteka redna komunikacija, pri kateri se izmenjujejo podatki in usklajuje obvladovanje varnostnih incidentov, zlasti varnostnih incidentov IT, zaradi katerih bi lahko bila potrebna uradna preiskava.

4. Po potrebi in za izmenjavo znanja z drugimi institucijami in agencijami EU, ki so bile morebiti prizadete, lahko podporo pri obvladovanju incidentov nudijo službe za koordinacijo incidentov skupine za odzivanje na računalniške grožnje za evropske institucije, organe in agencije (CERT-EU).

5. Lastniki sistema, ki so udeleženi pri varnostnem incidentu IT:

(a) nemudoma obvestijo svojega vodjo službe Komisije, Generalni direktorat za informatiko, Generalni direktorat za človeške vire, LISO, po potrebi pa tudi lastnika podatkov, o vseh večjih varnostnih incidentih IT, zlasti tistih, pri katerih je prišlo do kršitve zaupnosti podatkov;

(b) sodelujejo z ustreznimi organi Komisije in se ravnajo po njihovih navodilih glede obveščanja o incidentu, odziva nanj in odprave njegovih posledic.

6. Uporabniki o vseh dejanskih varnostnih incidentih IT ali sumu takih incidentov pravočasno obvestijo ustrezno službo za računalniško pomoč.

7. Lastniki podatkov o vseh dejanskih varnostnih incidentih IT ali sumu takih incidentov pravočasno obvestijo ustrezno skupino za odzivanje na varnostne incidente IT.

8. Generalni direktorat za informatiko je ob podpori drugih sodelujočih zainteresiranih strani odgovoren za obvladovanje vseh varnostnih incidentov IT, odkritih v zvezi s KIS Komisije, ki niso oddani zunanjim izvajalcem.

9. Generalni direktorat za informatiko o varnostnih incidentih IT obvešča prizadete službe Komisije, ustrezne LISO ter po potrebi CERT-EU, in sicer na podlagi načela potrebe po seznanitvi.

10. Generalni direktorat za informatiko redno poroča ISSB o večjih varnostnih incidentih IT, ki so prizadeli KIS Komisije.

11. Ustrezni LISO imajo na zahtevo dostop do evidenc varnostnih incidentov IT, ki zadevajo KIS službe Komisije.

12. Kontaktna točka za obvladovanje izrednih razmer v primeru večjega varnostnega incidenta IT je Generalni direktorat za informatiko, ki usklajuje krizne skupine za varnostne incidente IT.

13. Generalni direktor Generalnega direktorata za informatiko lahko v izrednih razmerah sprejme odločitev o začetku izvajanja postopka za izredne razmere v zvezi z varnostjo IT. Generalni direktorat za informatiko oblikuje postopke za izredne razmere, ki jih odobri ISSB.

14. Generalni direktorat za informatiko poroča ISSB in vodjem prizadetih služb Komisije o izvedbi postopkov za izredne razmere.

Postopki v zvezi s temi obveznostmi in dejavnostmi se podrobneje določijo v izvedbenih pravilih.

POGLAVJE 4

KONČNE DOLOČBE

Člen 16

Preglednost

O tem sklepu se obvesti osebje Komisije in vse osebe, za katere se uporablja, objavi se v *Uradnem listu Evropske unije*.

Člen 17

Povezava z drugimi akti

Določbe tega sklepa ne posegajo v Sklep (EU, Euratom) 2015/443, Sklep (EU, Euratom) 2015/444, Uredbo (ES) št. 45/2001, Uredbo (ES) št. 1049/2001 Evropskega parlamenta in Sveta ([1]), Sklep Komisije 2002/47/ES, ESPJ, Euratom ([2]), Uredbo (EU, Euratom) št. 883/2013 Evropskega parlamenta in Sveta ([3]) ter Sklep 1999/352/ES, ESPJ, Euratom.

Člen 18

Razveljavitev in prehodni ukrepi

Sklep C(2006) 3602 z dne 16. avgusta 2006 se razveljavi.

Izvedbena pravila in standardi za varnost IT, sprejeti v skladu s členom 10 Sklepa C(2006) 3602, ostajajo v veljavi v delu, v katerem niso v nasprotju s tem sklepom, dokler ne bodo nadomeščeni z izvedbenimi pravili in standardi, ki bodo sprejeti v skladu s členom 13 tega sklepa. Vsako sklicevanje na člen 10 Sklepa C(2006) 3602 se razume kot sklicevanje na člen 13 tega sklepa.

Člen 19

Začetek veljavnosti

Ta sklep začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

V Bruslju, 10. januarja 2017

Za Komisijo
Predsednik
Jean-Claude JUNCKER

([1]) Uredba (ES) št. 1049/2001 Evropskega parlamenta in Sveta z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije (UL L 145, 31.5.2001, str. 43).
([2]) Sklep Komisije 2002/47/ES,ESPJ, Euratom z dne 23. januarja 2002 o spremembi njenega poslovnika (UL L 21, 24.1.2002, str. 23).
([3]) Uredba (EU, Euratom) št. 883/2013 Evropskega parlamenta in Sveta z dne 11. septembra 2013 o preiskavah, ki jih izvaja Evropski urad za boj proti goljufijam (OLAF) in razveljavitvi Uredbe (ES) št. 1073/1999 Evropskega parlamenta in Sveta in Uredbe Sveta (Euratom) št. 1074/1999 (UL L 248, 18.9.2013, str. 1).