ODLUKA KOMISIJE (EU, Euratom) 2018/559

od 6. travnja 2018.

o utvrđivanju provedbenih pravila za članak 6. Odluke (EU, Euratom) 2017/46 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,

uzimajući u obzir Odluku Komisije (EU, Euratom) 2017/46 od 10. siječnja 2017. o sigurnosti komunikacijskih i informacijskih sustava u Europskoj komisiji ([1]), a posebno njezin članak 6.,

budući da:

(1) Donošenjem Odluke (EU, Euratom) 2017/46 Komisija mora preispitati, ažurirati i konsolidirati provedbena pravila povezana s Odlukom Komisije C(2006) 3602 o sigurnosti komunikacijskih i informacijskih sustava kojima se Komisija koristi, koja je stavljena izvan snage.

(2) U potpunosti u skladu s unutarnjim pravilima postupanja, član Komisije odgovoran za sigurnost ovlašten je za utvrđivanje provedbenih pravila u skladu s člankom 13. Odluke (EU, Euratom) 2017/46 ([2]).

(3) Provedbena pravila iz Odluke C(2006) 3602 trebalo bi stoga staviti izvan snage,

DONIJELA JE OVU ODLUKU:

POGLAVLJE 1.

OPĆE ODREDBE

Članak 1.

Predmet i područje primjene

1. Predmet i područje primjene ove Odluke navedeni su u članku 1. Odluke (EU, Euratom) 2017/46.

2. Odredbe ove Odluke primjenjuju se na sve komunikacijske i informacijske sustave (CIS). Međutim, nadležnosti utvrđene u ovoj Odluci ne primjenjuju se na CIS-ove koji rukuju klasificiranim podacima EU-a. Odgovarajuće nadležnosti za te sustave određuje vlasnik sustava i sigurnosno tijelo Komisije u skladu s Odlukom Komisije (EU, Euratom) 2015/444 ([3]).

3. Poglavlje 2. ove Odluke pregled je praktične provedbe organizacije i nadležnosti u pogledu sigurnosti informatičkih tehnologija. Poglavlje 3. ove Odluke pregled je postupaka povezanih s člankom 6. Odluke (EU, Euratom) 2017/46.

Članak 2.

Definicije

Definicije iz članka 2. Odluke (EU, Euratom) 2017/46 primjenjuju se na ovu Odluku. Za potrebe ove Odluke primjenjuju se i sljedeće definicije:

1. „Tijelo za odobravanje kriptomaterijala” (CAA) funkcija je koju obavlja sigurnosno tijelo Komisije koje je pod nadležnošću glavnog direktora za ljudske resurse i sigurnost.

([1]) SL L 6, 11.1.2017., str. 40.
([2]) Odluka Komisije C(2017) 7428 final od 8. studenoga 2017. o davanju ovlasti za donošenje provedbenih pravila, standarda i smjernica u pogledu sigurnosti komunikacijskih i informacijskih sustava u Europskoj komisiji.
([3]) 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.).

2. „Veza s vanjskom mrežom” znači svaka elektronička komunikacijska veza između unutarnje Komisijine mreže i bilo koje druge mreže, uključujući internet. Ta se definicija ne odnosi na mreže trećih strana kojima je pristup omogućen na temelju ugovora i koje su dio Komisijine unutarnje mreže.

3. „Pohrana ključa kod treće strane” znači postupak za pohranu kopija kriptografskih ključeva kod jedne ili više različitih strana, radi razdvajanja nadležnosti, kako bi se osigurao dohvat ključeva ako se izgubi aktivni ključ. Ključevi se mogu podijeliti na dva dijela ili više njih te se svaki dio povjerava nekoj drugoj strani kako bi se osiguralo da ni jedna strana nema cijeli ključ.

4. „RASCI” je pokrata za dodjelu nadležnosti na temelju sljedećih pokazatelja:

(a) „Nadležnost” (R) znači da ima obvezu odlučivati i djelovati kako bi se postigli željeni ciljevi;

(b) „Odgovornost” (A) znači da odgovara za mjere, odluke i djelovanje;

(c) „Potpora” (S) znači da ima obvezu surađivati s osobom nadležnom za izvršenje zadatka;

(d) „Savjetovanje” (C) znači da na zahtjev pruža savjet ili mišljenje;

(e) „Obaviještenost” (I) znači da raspolaže ažurnim informacijama.

POGLAVLJE 2.

ORGANIZACIJA I NADLEŽNOSTI

Članak 3.

Uloge i nadležnosti

Uloge i nadležnosti povezane s člancima 4. do 8. ove Odluke definirani su u Prilogu u skladu s modelom RASCI.

Članak 4.

Usklađivanje s Komisijinom politikom u području informacijske sigurnosti

1. Glavna uprava za ljudske resurse i sigurnost revidira Komisijinu politiku u području sigurnosti informatičkih tehnologija te povezanih standarda i smjernica kako bi se osiguralo da budu u skladu s Komisijinim općim politikama u području sigurnosti, osobito s Odlukom Komisije (EU, Euratom) 2015/443 ([1]) i Odlukom (EU, Euratom) 2015/444.

2. Na zahtjev drugih Komisijinih službi Glavna uprava za ljudske resurse i sigurnost može, radi usklađivanja s Komisijinom politikom u području informacijske sigurnosti, revidirati svoje politike u području informatičkih tehnologija ili ostalu dokumentaciju povezanu sa sigurnošću informatičkih tehnologija. Načelnik predmetne Komisijine službe osigurava uklanjanje nedosljednosti.

3. U okviru svoje nadležnosti za sigurnost podataka Glavna uprava za ljudske resurse i sigurnost surađuje s Glavnom upravom za informatiku kako bi se u postupcima za sigurnost informatičkih tehnologija u potpunosti u obzir uzeli klasifikacija i načela sigurnosti utvrđeni u Odluci (EU, Euratom) 2015/443, a posebno njezinim člancima 3. i 9.

POGLAVLJE 3.

POSTUPCI ZA SIGURNOST INFORMATIČKIH TEHNOLOGIJA

Članak 5.

Tehnologije šifriranja

1. Upotreba tehnologija šifriranja za zaštitu klasificiranih podataka EU-a (EUCI) u skladu je s Odlukom (EU, Euratom) 2015/444.

2. Odluke o upotrebi tehnologija šifriranja za zaštitu podataka koji nisu EUCI donosi vlasnik svakog CIS-a, uzimajući u obzir rizike koji se namjeravaju ublažiti s pomoću šifriranja i rizike koje se njime uvode.

3. Za sve vrste upotrebe tehnologija šifriranja potrebno je prethodno odobrenje CAA-a, osim ako se šifriranje koristi samo za zaštitu povjerljivosti podataka u tranzitu koji nisu EUCI uz upotrebu standardnih komunikacijskih protokola mreže.

([1]) Odluka Komisije (EU, Euratom) 2015/443 od 13. ožujka 2015. o sigurnosti u Komisiji (SL L 72, 17.3.2015., str. 41.).

4. Uz iznimke navedene u stavku 3. ovog članka Komisijine službe osiguravaju pohranjivanje sigurnosnih kopija svih ključeva za dešifriranje kod treće strane kako bi se, u slučaju da ključ za dešifriranje nije dostupan, do pohranjenih podataka moglo doći. Dohvat šifriranih podataka s pomoću sigurnosnih kopija ključeva za dešifriranje provodi se samo kada je odobren u skladu sa standardom koji je odredio CAA.

5. Zahtjevi za odobrenje upotrebe tehnologija šifriranja službeno se dokumentiraju te sadržavaju pojedinosti o CIS-u i podacima koje treba zaštititi, tehnologijama koje će se upotrebljavati te povezanim sigurnosnim operativnim postupcima. Te zahtjeve za odobrenje potpisuje vlasnik sustava.

6. Zahtjeve za odobrenje za upotrebu tehnologija šifriranja ocjenjuje CAA u skladu s objavljenim standardima i uvjetima.

Članak 6.

Inspekcijski pregledi informatičkih tehnologija

1. Glavna uprava za ljudske resurse i sigurnost provodi inspekcijske preglede sigurnosti informatičkih tehnologija kako bi se provjerilo jesu li mjere sigurnosti informatičkih tehnologija u skladu s Komisijinim politikama u području sigurnosti informatičkih tehnologija te kako bi se provjerila cjelovitost tih kontrolnih mjera.

2. Glavna uprava za ljudske resurse i sigurnost može provoditi inspekcijske preglede sigurnosti informatičkih tehnologija:

(a) na vlastitu inicijativu;

(b) na zahtjev Upravljačkog odbora za informacijsku sigurnost (ISSB);

(c) na zahtjev vlasnika sustava;

(d) nakon incidenta povezanog sa sigurnošću; ili

(e) nakon utvrđivanja visokog rizika na određenom sustavu.

3. Vlasnici podataka mogu zatražiti inspekcijski pregled sigurnosti informatičkih tehnologija prije nego što pohrane svoje podatke na CIS.

4. Rezultati inspekcijskog pregleda dokumentiraju se u izvješću vlasniku sustava čija se kopija šalje LISO-u (lokalni službenik za informacijsku sigurnost), a sadržava zaključke i preporuke za poboljšanje usklađenosti CIS-a s politikom sigurnosti informatičkih tehnologija. Glavna uprava za ljudske resurse i sigurnost izvješćuje ISSB o važnim problemima i preporukama.

5. Glavna uprava za ljudske resurse i sigurnost prati provedbu tih preporuka.

6. Prema potrebi, inspekcijski pregledi sigurnosti informatičkih tehnologija uključuju pregled usluga, prostora i opreme koje vlasniku sustava osiguravaju unutarnji ili vanjski pružatelji usluga.

Članak 7.

Pristup iz vanjskih mreža

1. Glavna uprava za ljudske resurse i sigurnost utvrđuje pravila u okviru standarda za odobravanje pristupa između CIS-ova Komisije i vanjskih mreža.

2. U okviru pravila razlikuju se vrste veza s vanjskom mrežom i utvrđuju odgovarajuća sigurnosna pravila za svaku vrstu veze te se određuje je li nužno prethodno odobrenje nadležnog tijela za tu vezu, kako je navedeno u stavku 4. ovog članka.

3. Ako je potrebno, odobrenje se izdaje na temelju službenog zahtjeva i postupka odobrenja. Odobrenje ima određeno vremensko trajanje i dobavlja se prije aktivacije veze.

4. Glavna uprava za ljudske resurse i sigurnost u potpunosti je nadležna za odobravanje zahtjeva, no nadležnost za odobravanje određenih vrsta priključaka može po vlastitom nahođenju delegirati u skladu s člankom 17. stavkom 3. Odluke (EU, Euratom) 2015/443, podložno uvjetima utvrđenima u stavku 8.

5. Nadležna tijela mogu odrediti dodatne uvjete u pogledu sigurnosti kao preduvjet za odobrenje, kako bi Komisijine CIS-ove i mreže zaštitila od rizika neovlaštenog pristupa ili drugih povreda sigurnosti.

6. Glavna uprava za informatiku standardni je pružatelj mrežnih usluga za Komisiju. Svaka druga Komisijina služba koja upravlja mrežom koja ne pripada Glavnoj upravi za informatiku prvo pribavlja suglasnost ISSB-a. Komisijina služba dužna je dokumentirati poslovnu opravdanost tog zahtjeva i dokazati da su mrežne kontrole dovoljne za ispunjenje uvjeta za kontrolu dolaznih i odlaznih informacija.

7. Vlasnik CIS-a određuje sigurnosne zahtjeve za vanjski pristup CIS-u i osigurava provedbu odgovarajućih mjera za zaštitu njegove sigurnosti, uz podršku LISO-a.

8. Sigurnosne mjere provedene za veze s vanjskom mrežom temelje se na načelu informiranosti samo o najnužnijemu i dobivanja najužih ovlasti, čime se osigurava da pojedinci dobiju samo one informacije i ostvare samo ono pravo pristupa koje im je potrebno za obavljanje službenih dužnosti za Komisiju.

9. Sve veze s vanjskom mrežom filtriraju se i prate kako bi se otkrile moguće povrede sigurnosti.

10. Kada su veze uspostavljene kako bi se omogućila eksternalizacija CIS-a, odobrenje ovisi o uspješnom dovršetku postupka opisanog u članku 8.

Članak 8.

Eksternalizacija CIS-ova

1. Za potrebe ove Odluke CIS se smatra eksternaliziranim kada je uspostavljen na temelju ugovora s trećim izvođačem, na temelju kojeg je CIS smješten izvan Komisijinih prostora. To uključuje eksternalizaciju pojedinačnih ili višestrukih CIS-ova ili drugih usluga u području informatičkih tehnologija, podatkovne centre izvan Komisijinih prostora i vanjske usluge rukovanja Komisijinim skupovima podataka.

2. Pri eksternalizaciji CIS-a na sljedeći se način u obzir uzima osjetljivost ili klasifikacija podataka kojima se rukuje:

(a) CIS koji omogućuje rukovanje klasificiranim podacima EU-a akreditiran je u skladu s Odlukom (EU, Euratom) 2015/444, a od Komisijina tijela za sigurnosnu akreditaciju (SAA) traži se prethodno mišljenje. Sustavi koji omogućuju rukovanje EUCI-jem ne eksternaliziraju se.

(b) Vlasnik CIS-a koji omogućuje rukovanje podacima koji nisu EUCI provodi odgovarajuće mjere za ispunjavanje sigurnosnih potreba u skladu s relevantnim pravnim obvezama ili osjetljivošću podataka, uzimajući u obzir rizike povezane s eksternalizacijom. Glavna uprava za ljudske resurse i sigurnost može odrediti dodatne uvjete.

(c) Pri eksternalizaciji razvojnih projekata u obzir se uzimaju osjetljivost razvijenog koda i svi testni podaci korišteni tijekom njegova razvijanja.

3. Sljedeća se načela primjenjuju na eksternalizirane CIS-ove, uz one iz članka 3. Odluke (EU, Euratom) 2017/46:

(a) sporazumi o eksternalizaciji sastavljaju se tako da se izbjegne ovisnost o određenim dobavljačima;

(b) sporazumima o sigurnosti u pogledu eksternalizacije smanjuje se mogućnost da osoblje treće strane pristupi informacijama Komisije ili ih promijeni;

(c) osoblje treće strane koje ima pristup eksternaliziranim CIS-ovima sklapa ugovore o povjerljivosti;

(d) eksternalizacija CIS-a navodi se u evidenciji CIS-ova.

4. Vlasnik sustava uz sudjelovanje vlasnika podataka dužan je:

(a) procijeniti i dokumentirati rizike povezane s eksternalizacijom;

(b) utvrditi odgovarajuće uvjete u pogledu sigurnosti;

(c) savjetovati se s vlasnicima svih drugih povezanih CIS-ova kako bi se osiguralo uključivanje njihovih sigurnosnih uvjeta;

(d) navesti odgovarajuće sigurnosne uvjete i prava u ugovoru o eksternalizaciji;

(e) ispuniti sve ostale uvjete utvrđene u detaljnom postupku, kako je navedeno u stavku 8. ovog članka.

Te se radnje obavljaju prije sklapanja ugovora ili drugih sporazuma o eksternalizaciji jednog CIS-a ili više njih.

5. Vlasnici sustava upravljaju rizicima povezanima s eksternalizacijom tijekom trajanja CIS-a radi ispunjenja utvrđenih sigurnosnih uvjeta.

6. Vlasnici sustava dužni su treće izvođače obvezati na hitno obavještavanje Komisije o svim incidentima u području sigurnosti informatičkih tehnologija koji zahvaćaju eksternalizirane CIS-ove Komisije.

7. Vlasnik sustava nadležan je za osiguravanje usklađenosti CIS-a, ugovora o eksternalizaciji i sporazuma o sigurnosti s pravilima Komisije o sigurnosti informacija i sigurnosti informatičkih tehnologija.

8. Glavna uprava za ljudske resurse i sigurnost utvrđuje detaljne standarde povezane s nadležnostima i aktivnostima navedenima u stavcima od 1. do 7. u skladu s člankom 10. u nastavku.

POGLAVLJE 4.

RAZNE I ZAVRŠNE ODREDBE

Članak 9.

Transparentnost

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

Članak 10.

Standardi

1. Odredbe ove Odluke, prema potrebi, detaljnije su opisane u standardima i/ili smjernicama koje je potrebno donijeti u skladu s Odlukom (EU, Euratom) 2017/46 i Odlukom C(2017)7428. Standardi sigurnosti informacijskih tehnologija i smjernice sadržavaju dodatne pojedinosti o tim provedbenim pravilima, a Odluka (EU, Euratom) 2017/46 o posebnim područjima sigurnosti u skladu s normom ISO 27001:2013, Prilog A. Ti standardi i smjernice temelje se na najboljim praksama industrije i biraju se tako da odgovaraju Komisijinu okruženju informatičkih tehnologija.

2. Standardi su, prema potrebi, razvijani u skladu sa standardom ISO 27001:2013 Prilog A u sljedećim područjima:

(1) organizacija informacijske sigurnosti;

(2) sigurnost ljudskih potencijala;

(3) upravljanje imovinom;

(4) kontrola pristupa;

(5) kriptografija;

(6) fizička sigurnost i sigurnost okruženja;

(7) operativna sigurnost;

(8) sigurnost komunikacija;

(9) nabava, razvoj i održavanje sustava;

(10) odnosi s dobavljačima;

(11) rješavanje incidenata povezanih sa sigurnošću informacija;

(12) aspekti informacijske sigurnosti u području upravljanja kontinuitetom poslovanja;

(13) usklađivanje.

3. ISSB odobrava standarde navedene u stavcima 1. i 2. ovog članka prije njihova donošenja.

4. Provedbena pravila iz Odluke C(2006) 3602 koja se odnose na područje primjene ove Odluke ovime se stavljaju izvan snage.

5. Standardi i smjernice doneseni u skladu s Odlukom C(2006) 3602 od 16. kolovoza 2006. ostaju na snazi ako nisu u suprotnosti s ovim provedbenim pravilima, sve dok ih se ne stavi izvan snage ili zamijeni standardima ili smjernicama koje je potrebno donijeti u skladu s člankom 13. Odluke (EU, Euratom) 2017/46.

Članak 11.

Stupanje na snagu

Ova Odluka stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Sastavljeno u Bruxellesu 6. travnja 2018.

Za Komisiju,
u ime predsjednika,
Günther OETTINGER
Član Komisije

PRILOG

ULOGE I NADLEŽNOSTI (RASCI)

Modelom RASCI subjektima se dodjeljuje uloga s pomoću sljedećih pokrata:

(a) R – Nadležnost

(b) A – Odgovornost

(c) S – Potpora

(d) C – Savjetovanje

(e) I – Obaviještenost

Uloga / Postupak	ISSB	HR (DS)	Službe Komisije	Vlasnik sustava	Vlasnik podataka	LISO	DIGIT	Vanjski suradnici
Usklađivanje s Komisijinom politikom u području informacijske sigurnosti		**R/A**	**S**				**S**	
Tehnologije šifriranja		**C**	**A**	**R**	**I**	**C**		
Inspekcijski pregledi sigurnosti informatičkih tehnologija	**I**	**A/R**		**S**	**I**	**I**	**S**	
Pristup iz vanjskih mreža	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Eksternalizacija CIS-ova		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] ISSB provodi savjetovanja o radu bilo koje službe Komisije s unutarnjim mrežama, osim Glavne uprave za informatiku.

[2] Nadležan je eksternalizirani vlasnik sustava CIS, a obvezno je savjetovanje s vlasnikom sustava bilo kojeg drugog CIS-a s kojim je eksternalizirani CIS povezan.