SKLEP KOMISIJE (EU, Euratom) 2018/559

z dne 6. aprila 2018

o določitvi izvedbenih pravil za člen 6 Sklepa (EU, Euratom) 2017/46 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 Sklepa Komisije (EU, Euratom) 2017/46 z dne 10. januarja 2017 o varnosti komunikacijskih in informacijskih sistemov v Evropski komisiji ([1]) ter zlasti člena 6 Sklepa,

ob upoštevanju naslednjega:

(1) S sprejetjem Sklepa (EU, Euratom) 2017/46 mora Komisija pregledati, posodobiti in konsolidirati izvedbena pravila, povezana z razveljavljenim Sklepom Komisije C(2006) 3602 o varnosti komunikacijskih in informacijskih sistemov, ki jih uporablja.

(2) V skladu z internim poslovnikom je bil član Komisije, pristojen za varnost, pooblaščen za določitev izvedbenih pravil v skladu s členom 13 Sklepa (EU, Euratom) 2017/46 ([2]).

(3) Izvedbena pravila Sklepa C(2006) 3602 bi bilo zato treba razveljaviti –

SPREJELA NASLEDNJI SKLEP:

POGLAVJE 1

SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja in področje uporabe

1. Predmet urejanja in področje uporabe tega sklepa sta določena v členu 1 Sklepa (EU, Euratom) 2017/46.

2. Določbe v tem sklepu se uporabljajo za vse komunikacijske in informacijske sisteme (KIS). Vendar se odgovornosti iz tega sklepa ne uporabljajo za KIS, ki obdelujejo tajne podatke EU. Ustrezne odgovornosti za te sisteme določita lastnik sistema in varnostni organ Komisije v skladu s Sklepom Komisije (EU, Euratom) 2015/444 ([3]).

3. Poglavje 2 tega sklepa vsebuje pregled praktičnega izvajanja organizacije in odgovornosti v zvezi z varnostjo IT. Poglavje 3 tega sklepa vsebuje pregled postopkov v zvezi s členom 6 Sklepa (EU, Euratom) 2017/46.

Člen 2

Opredelitev pojmov

Opredelitve pojmov v členu 2 Sklepa (EU, Euratom) 2017/46 se uporabljajo za ta sklep. V tem sklepu se uporabljajo tudi naslednje opredelitve pojmov:

1. „organ za odobritev šifrirnih metod in izdelkov“ (CAA) je funkcija, ki jo ima Varnostni organ Komisije, ki spada v pristojnost Generalnega direktorja za človeške vire in varnost;

([1]) UL L 6, 11.1.2017, str. 40.
([2]) Sklep Komisije C(2017) 7428 z dne 8. novembra 2017 o odobritvi pooblastila za sprejemanje izvedbenih pravil, standardov in smernic v zvezi z varnostjo komunikacijskih in informacijskih sistemov v Evropski komisiji.
([3]) 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).

2. „zunanja omrežna povezava“ pomeni katera koli elektronska komunikacijska povezava med internim omrežjem Komisije in katerim koli drugim omrežjem, vključno z internetom. ta opredelitev izključuje omrežja tretjih oseb, ki se zagotavljajo v okviru pogodbe in so del internega omrežja Komisije.

3. „hramba ključev pri tretji osebi“ pomeni postopek za shranjevanje kopij kriptografskih ključev pri eni ali več ločenih strankah, s čimer se zagotavlja ločevanje nalog, da se omogoči njihova obnovitev, če se operativna kopija izgubi. Ključi se lahko razdelijo na dva ali več delov, od katerih se vsak deponira pri drugi stranki, da se zagotovi, da nobena posamezna stranka nima celotnega ključa.

4. „RASCI“ je kratica za dodeljevanje odgovornosti na podlagi naslednjih kazalnikov značilnosti:

(a) „pristojen“ (R) pomeni dolžan ukrepati in sprejemati odločitve za dosego potrebnih rezultatov;

(b) „odgovoren“ (A) pomeni nositi odgovornost za ukrepe, odločitve in izvedbo;

(c) „daje podporo“ (S) pomeni dolžan sodelovati z osebo, odgovorno za izvedbo naloge;

(d) „posvetovan“ (C) pomeni zaprošen za nasvet ali mnenje;

(e) „obveščen“ (I) pomeni biti seznanjen s pomembnimi informacijami.

POGLAVJE 2

ORGANIZACIJA IN ODGOVORNOSTI

Člen 3

Vloge in odgovornosti

Vloge in odgovornosti v zvezi s členi 4 do 8 tega sklepa so opredeljeni v Prilogi v skladu z modelom RASCI.

Člen 4

Usklajenost z informacijsko varnostno politiko Komisije

1. Generalni direktorat za človeške vire in varnost pregleda politiko Komisije za varnost IT ter s tem povezane standarde in smernice, da se zagotovi njihova skladnost s splošno varnostno politiko Komisije, zlasti Sklepom Komisije (EU, Euratom) 2015/443 ([1]) in Sklepom (EU, Euratom) 2015/444.

2. Na zahtevo drugih služb Komisije lahko Generalni direktorat za človeške vire in varnost pregleda njihove politike za varnost IT ali drugo dokumentacijo o varnosti IT, da se zagotovi njihova skladnost z informacijsko varnostno politiko Komisije. Vodja zadevne službe Komisije poskrbi, da se odpravijo vsa neskladja.

3. V okviru svoje odgovornosti za varnost informacij Generalni direktorat za človeške vire in varnost sodeluje z Generalnim direktoratom za informatiko, da se zagotovi, da se v varnostnih postopkih IT v celoti upoštevajo stopnja tajnosti in načela varnosti iz Sklepa (EU, Euratom) 2015/443, zlasti člena 3 in 9.

POGLAVJE 3

VARNOSTNI POSTOPKI IT

Člen 5

Šifrirne tehnologije

1. Uporaba šifrirnih tehnologij za varstvo tajnih podatkov EU je v skladu s Sklepom (EU, Euratom) 2015/444.

2. Odločitve o uporabi šifrirnih tehnologij za varstvo netajnih podatkov EU sprejme lastnik sistema vsakega KIS, pri čemer upošteva tveganja, ki naj bi se zmanjšala s šifriranjem, in nevarnosti, ki jih šifriranje prinaša.

3. Predhodna odobritev CAA je potrebna za vse vrste uporabe šifrirnih tehnologij, razen če se šifriranje uporablja le za varovanje zaupnosti netajnih podatkov EU v tranzitu in se uporabljajo standardni omrežni komunikacijski protokoli.

([1]) Sklep Komisije (EU, Euratom) 2015/443 z dne 13. marca 2015 o varnosti v Komisiji (UL L 72, 17.3.2015, str. 41).

4. Z izjemo iz odstavka 3 tega člena službe Komisije zagotovijo shranjevanje varnostnih kopij ključev za dešifriranje v hrambi ključev pri tretji osebi za obnovitev shranjenih podatkov, če ključ za dešifriranje ni na voljo. Obnovitev šifriranih podatkov z uporabo varnostnih kopij ključev za dešifriranje se izvede samo z odobritvijo v skladu s standardom, ki ga opredeli CAA.

5. Prošnje za odobritev uporabe šifrirnih tehnologij se uradno dokumentirajo in vključujejo podrobnosti o komunikacijskih in informacijskih sistemih ter podatkih, ki jih je treba varovati, tehnologijah, ki se uporabijo, ter povezanih varnostno-operativnih postopkih. Te zahteve za odobritev podpiše lastnik sistema.

6. Prošnje za odobritev uporabe šifrirnih tehnologij ovrednoti CAA v skladu z objavljenimi standardi in zahtevami.

Člen 6

Varnostni inšpekcijski pregledi IT

1. Generalni direktorat za človeške vire in varnost izvaja varnostne inšpekcijske preglede IT, da preveri, ali so varnostni ukrepi na področju IT skladni s politikami za varnost IT Komisije ter ali so ti nadzorni ukrepi celoviti.

2. Generalni direktorat za človeške vire in varnost lahko varnostni inšpekcijski pregled IT izvede:

(a) na lastno pobudo;

(b) na zahtevo Usmerjevalnega odbora za varnost informacij (ISSB);

(c) na zahtevo lastnika sistema;

(d) po incidentu v zvezi z varnostjo podatkov ali

(e) po ugotovitvi velikega tveganja za posamezen sistem.

3. Lastniki podatkov lahko zahtevajo varnostni inšpekcijski pregled IT, preden svoje podatke shranijo v KIS.

4. Rezultati inšpekcijskega pregleda se dokumentirajo v uradnem poročilu lastniku sistema, poročilo pa se pošlje v vednost lokalnemu varnostnemu uradniku za informatiko (LISO) ter vsebuje ugotovitve in priporočila za izboljšanje skladnosti KIS s politiko za varnost informacijske tehnologije. Generalni direktorat za človeške vire in varnost pomembna vprašanja in priporočila sporoči ISSB.

5. Generalni direktorat za človeške vire in varnost spremlja izvajanje priporočil.

6. Po potrebi varnostni inšpekcijski pregledi IT vključujejo pregled storitev, prostorov in opreme, zagotovljene lastniku sistema, pri čemer so zajeti notranji in zunanji ponudniki storitev.

Člen 7

Dostop iz zunanjih omrežij

1. Generalni direktorat za človeške vire in varnost določi pravila v standardu o odobritvi dostopa med KIS Komisije in zunanjimi omrežji.

2. Pravila razlikujejo med različnimi vrstami zunanjih omrežnih povezav in določajo ustrezna varnostna pravila za vsako vrsto povezave, vključno s tem, ali je potrebno predhodno dovoljenje za povezavo od ustreznega organa, kot je navedeno v odstavku 4 tega člena.

3. Če je potrebno, se dovoljenje izda na podlagi uradnega zahtevka in postopka odobritve. Odobritev velja za določeno obdobje in se pridobi pred aktivacijo povezave.

4. Generalni direktorat za človeške vire in varnost je splošno odgovoren za odobritev zahtevkov, vendar lahko prenese pristojnost za odobritev nekaterih vrst povezav po lastni presoji v skladu s členom 17(3) Sklepa (EU, Euratom) 2015/443 in v skladu s pogoji iz točke 8.

5. Pooblaščeni subjekt lahko kot pogoj za odobritev naloži dodatne varnostne zahteve, da se KIS in omrežja Komisije zaščitijo pred tveganji nepooblaščenega dostopa ali drugimi kršitvami varstva.

6. Generalni direktorat za informatiko je standardni ponudnik omrežnih storitev za Komisijo. Druge službe Komisije, ki upravljajo omrežje, ki ga ne zagotavlja Generalni direktorat za informatiko, najprej pridobijo soglasje ISSB. Služba Komisije dokumentira poslovno utemeljitev zahteve in dokaže, da nadzor omrežja zadostuje za izpolnitev zahtev za nadzor vhodnih in izhodnih tokov informacij.

7. Lastnik sistema KIS določi varnostne zahteve za zunanji dostop do tega KIS in zagotovi izvedbo ustreznih ukrepov za zaščito njegove varnosti ob podpori LISO.

8. Varnostni ukrepi, izvedeni za zunanje omrežne povezave, temeljijo na načelih potrebe po seznanitvi in najmanjšega privilegija, ki zagotavljajo, da fizične osebe prejmejo le informacije in pravice dostopa, ki jih potrebujejo za opravljanje svojih uradnih dolžnosti za Komisijo.

9. Vse zunanje omrežne povezave se filtrirajo in spremljajo, da se ugotovijo morebitne kršitve varstva.

10. Če so vzpostavljene povezave za zunanje izvajanje KIS, je dovoljenje odvisno od uspešnega zaključka postopka iz člena 8.

Člen 8

Zunanje izvajanje KIS

1. Za namene tega sklepa se šteje, da KIS upravlja zunanji izvajalec, če se zagotovi na podlagi pogodbe z zunanjim izvajalcem, v skladu s katero je KIS nameščen v prostorih, ki niso prostori Komisije. To vključuje zunanje izvajanje posameznih ali več KIS ali drugih storitev IT, podatkovne centre v prostorih, ki niso prostori Komisije, in obdelavo podatkovnih nizov Komisije s strani zunanjih storitev.

2. Zunanje izvajanje KIS upošteva občutljivost ali stopnjo tajnosti obravnavanih podatkov:

(a) KIS, ki obdeluje tajne podatke EU, se akreditira v skladu s Sklepom (EU, Euratom) 2015/444, vnaprej pa se opravi posvetovanje z organom Komisije za varnostno akreditacijo (SAA). Sistemov, ki obdelujejo tajne podatke EU, ne smejo upravljati zunanji izvajalci.

(b) Lastnik sistema KIS, ki obdeluje netajne podatke EU, sprejme sorazmerne ukrepe za obravnavo varnostnih potreb v skladu z ustreznimi pravnimi obvezami ali občutljivostjo informacij, pri čemer upošteva tveganja, povezana z zunanjim izvajanjem. Generalni direktorat za človeške vire in varnost lahko naloži dodatne zahteve.

(c) Razvojni projekti, ki jih upravljajo zunanji izvajalci, upoštevajo občutljivost razvite šifre in vse testne podatke, uporabljene med razvojem.

3. Poleg načel iz člena 3 Sklepa (EU, Euratom) 2017/46 veljajo za KIS, ki jih upravlja zunanji izvajalec, naslednja načela:

(a) dogovori o zunanjem izvajanju so oblikovani tako, da se prepreči odvisnost od določenih dobaviteljev;

(b) zunanje izvajanje varnostnih dogovorov kar najbolj zmanjšuje možnosti dostopa tretjih oseb do podatkov Komisije ali spreminjanja teh podatkov;

(c) osebje tretjih strank, ki ima dostop do KIS, ki ga upravlja zunanji izvajalec, zagotovi sporazume o zaupnosti;

(d) zunanje upravljanje KIS se navede v evidenci KIS.

4. Lastnik sistema v sodelovanju z lastnikom podatkov:

(a) oceni in dokumentira tveganja v zvezi z zunanjim izvajanjem;

(b) določi ustrezne varnostne zahteve;

(c) se posvetuje z lastniki sistema vseh drugih povezanih KIS za zagotovitev, da so njihove varnostne zahteve vključene;

(d) zagotovi, da so ustrezne varnostne zahteve in pravice zajete v pogodbi o zunanjem izvajanju;

(e) izpolni vse druge zahteve, določene v podrobnem postopku, kot je navedeno v odstavku 8 tega člena.

Ti ukrepi se zaključijo pred podpisom pogodbe ali drugega dogovora o zunanjem izvajanju enega ali več KIS.

5. Lastniki sistema upravljajo tveganja, povezana z zunanjim izvajanjem v obdobju trajanja KIS, da se izpolnijo opredeljene varnostne zahteve.

6. Lastniki sistema zagotovijo, da so izvajalci tretjih strank dolžni nemudoma obvestiti Komisijo o vseh varnostnih incidentih IT, ki zadevajo KIS Komisije, ki ga upravlja zunanji izvajalec.

7. Lastnik sistema je odgovoren za zagotovitev skladnosti KIS, pogodbe o zunanjem izvajanju in varnostnih ureditev s pravili Komisije o varnosti podatkov in varnosti IT.

8. Generalni direktorat za človeške vire in varnost določi podrobni standard glede odgovornosti in dejavnosti iz točk (1) do (7) v skladu s členom 10 v nadaljevanju.

POGLAVJE 4

RAZNE IN KONČNE DOLOČBE

Člen 9

Preglednost

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

Člen 10

Standardi

1. Določbe tega sklepa se po potrebi podrobneje opredelijo v standardih in/ali smernicah, ki se sprejmejo v skladu s Sklepom Komisije (EU, Euratom) 2017/46 in Sklepom C(2017) 7428. Standardi in smernice za varnost IT zagotavljajo dodatne informacije o teh izvedbenih pravilih, Sklep (EU, Euratom) 2017/46 pa posebna varnostna področja v skladu s Prilogo A k standardu ISO 27001:2013. Ti standardi in smernice temeljijo na najboljših praksah v sektorju in so izbrani tako, da ustrezajo okolju IT Komisije.

2. Standardi se, kadar je potrebno, razvijejo v skladu s Prilogo A k standardu ISO 27001:2013 na naslednjih področjih:

(1) organizacija informacijske varnosti;

(2) varnost človeških virov;

(3) upravljanje sredstev;

(4) nadzor dostopa;

(5) kriptografija;

(6) fizična in okoljska varnost;

(7) operativna varnost;

(8) varnost komunikacij;

(9) nakup, razvoj in vzdrževanje sistemov;

(10) odnosi z dobavitelji;

(11) obvladovanje incidentov na področju varnosti podatkov;

(12) vidiki informacijske varnosti pri upravljanju neprekinjenega poslovanja;

(13) skladnost s predpisi.

3. ISSB odobri standarde iz odstavkov 1 in 2 tega člena pred njihovim sprejetjem.

4. Izvedbena pravila Sklepa C(2006) 3602 v zvezi s področjem uporabe tega sklepa se razveljavijo.

5. Standardi in smernice, sprejeti v skladu s Sklepom C(2006) 3602 z dne 16. avgusta 2006, ostajajo v veljavi v delu, v katerem niso v nasprotju s temi izvedbenimi pravili, dokler se ne razveljavijo ali nadomestijo s standardi ali smernicami, ki bodo sprejete v skladu s členom 13 Sklepa (EU, Euratom) 2017/46.

Člen 11

Začetek veljavnosti

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

V Bruslju, 6. aprila 2018

Za Komisijo
V imenu predsednika
Günther OETTINGER
Član Komisije

PRILOGA

VLOGE IN ODGOVORNOSTI (RASCI)

Model RASCI subjektom dodeljuje naloge z uporabo naslednjih okrajšav:

(a) R – pristojen (*responsible*)

(b) A – odgovoren (*accountable*)

(c) S – daje podporo (*supporting*)

(d) C – posvetovan (*consulted*)

(e) I – obveščen (*informed*)

Vloga / Proces	ISSB	HR (DS)	Službe Komisije	Lastnik sistema	Lastnik podatkov	LISO	GD za informatiko	Izvajalci
Usklajenost z informacijsko varnostno politiko Komisije		**R/A**	**S**				**S**	
Šifrirne tehnologije		**C**	**A**	**R**	**I**	**C**		
Varnostni inšpekcijski pregledi IT	**I**	**A/R**		**S**	**I**	**I**	**S**	
Dostop iz zunanjih omrežij	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Zunanje izvajanje KIS		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] Z ISSB se opravi posvetovanje v zvezi z upravljanjem notranjih omrežij s strani katere koli službe Komisije, ki ni Generalni direktorat za informatiko.

[2] Lastnik sistema KIS, ki ga upravlja zunanji izvajalec, je odgovoren, z lastnikom sistema katerega koli drugega KIS, s katerim se KIS, ki ga upravlja zunanji izvajalec, povezuje, pa se opravi posvetovanje.