APEK

Agencija za pošto in elektronske komunikacije Republike Slovenije
Stegne 7, p. p. 418
1001 Ljubljana
telefon: 01 583 63 00, faks: 01 511 11 01
e-naslov: info.box@apek.si, http://www.apek.si
davčna št.: 10482369

Številka: 0073-46/2013/7
Datum: 23.8.2013

Zadeva: **Odgovori na pripombe, predloge in dopolnitve zainteresirane javnosti k predlogu Splošnega akta o zavarovanju hranjenih podatkov**

Agencija je na podlagi 165. člena Zakona o elektronskih komunikacijah (Ur. l. RS št. 109/2012, v nadaljevanju: ZEKom-1) pripravila predlog Splošnega akta o zavarovanju hranjenih podatkov (v nadaljevanju: predlog splošnega akta) in ga 30.5.2013 objavila na svoji spletni strani ter zainteresirano javnost povabila, da do 30.6.2013 posreduje svoje pripombe, predloge ali dopolnitve. Agencija je prejela pripombe, predloge in dopolnitve naslednjih zainteresiranih oseb:

- Družbe GVO d.o.o., Cigaletova 10, 1000 Ljubljana (v nadaljevanju: GVO) in ,
- Sekcije operaterjev elektronskih komunikacij SOEK pri ZIT, GSZ, Dimičeva 13, 1504 Ljubljana (v nadaljevanju: Sekcija).

Agencija v nadaljevanju odgovarja na pripombe vseh navedenih zainteresiranih oseb. Pripombe, ki so vsebinsko podobne oz. se nanašajo na iste dele predloga splošnega akta, je Agencija združila in nanje odgovarja po vsebinskih sklopih.

Splošna pripomba

Dopis GVO:

1. Naša generalna in ključna pripomba je, da se vsem operaterjem nalagajo enake obveznosti, ne glede na to, ali ti operaterji ponujajo storitve končnim uporabnikom ali zgolj ponujajo pasivno infrastrukturo ponudnikom storitev. Ta distinkcija je še posebej izrazita pri tem Splošnem aktu, ki »določa organizacijske ukrepe, ki jih operaterji morajo sprejeti, za zaščito hranjenih podatkov...« (1. člen).

   GVO, d.o.o. namreč kot operater, ki ponuja zgolj pasivno infrastrukturo, ne hrani nikakršnih podatkov v smislu 13. Alinee 2. člena Splošnega akta, čeprav se celotna vsebina Splošnega akta navezuje ravno na te podatke. Citirana alinea namreč kot »hranjene podatke« opredeljuje naslednje podatke (164. člen ZEKom-1): 1. podatke, ki so potrebni za odkritje in prepoznanje vira komunikacije, 2. podatke, ki so potrebni za prepoznanje cilja komunikacije, 3. podatke, ki so potrebni za ugotovitev datuma, časa in trajanja komunikacije, 4. podatke, ki so potrebni za ugotovitev vrste komunikacije, 5. podatke, ki so potrebni za razpoznavo komunikacijske opreme uporabnikov in 6. podatke, ki so potrebni za ugotovitev lokacije opreme za mobilno komunikacijo.

   Glede na zapisano v prejšnjem odstavku tako nastane protislovna situacija, v kateri je (npr. GVO, d.o.o. kot) ponudnik pasivne infrastrukture dolžan (oz. mora) izvajati določene ukrepe za zavarovanje hranjenih podatkov (npr. 1. odstavek 3. člena, ki določa, da »operater mora sprejeti in izvajati postopke in ukrepe za zavarovanje hranjenih podatkov...«), čeprav tega ne more narediti, saj ne hrani in zato ne razpolaga s hranjenimi podatki v smislu 164. člena ZEKom-1.

Predlagamo, da se vse obveznosti, ki se nanašajo na zavarovanje hranjenih podatkov (celoten Splošni akt), predpiše izključno operaterjem, ki dejansko hranijo tovrstne podatke. V nasprotnem primeru bomo operaterji, ki podatkov v smislu 164. Člena ne hranimo, avtomatično v prekršku (oz. v nasprotju z zahtevami Splošnega akta), saj ukrepov za zavarovanje hranjenih podatkov ne bomo mogli sprejeti, ker ne moremo sprejeti ukrepov za zavarovanje nečesa, kar ne obstaja (kot že opisano zgoraj).

Ne moremo tudi pristati na razlago, ki je bila v odgovor na to konkretno dilemo predstavljena na javnem posvetu dne 10.6.2013, in sicer, da morajo operaterji sami oceniti, ali morajo tovrstne ukrepe sprejeti in izvajati ali ne. Splošni akt je pri tem vprašanju nesporen: »Operater mora sprejeti in izvajati postopke za zavarovanje hranjenih podatkov«, zato menimo, da trenutna dikcija operaterjem ne dopušča možnosti, da sami ocenijo, ali morajo Splošni akt in njegove zahteve upoštevati ali ne. Splošni akt v tem smislu operaterjem neposredno nalaga obveznosti, brez možnosti kakršnekoli lastne presoje oz. brez kakršnihkoli izjem.

Agencija v zvezi s pripombo družbe GVO pojasnjuje, da priprava predmetnega splošnega akta temelji na zahtevi 165. člena ZEKom-1, ki v prvem odstavku nalaga vsem operaterjem, da zagotovijo zavarovanje hranjenjih podatkov. V skladu z navedenim gre torej za obveznost, ki jo je zakonodajalec naložil tako operaterjem omrežja, kot tudi operaterjem izvajalcem storitev in zaradi tega agencija predloga ne bo upoštevala. Predlog splošnega akta je splošne narave in je primeren za vse operaterje. Operater bo z določitvijo obsega in meje sistema upravljanja varovanja informacij ter analizo tveganj ugotovil, kateri ukrepi so zanj primerni.

Pripomba na 2. člen

Dopis Sekcije:

1)

Splošni akt o zavarovanju hranjenih podatkov (v nadaljevanju besedila Splošni akt) v **12. točki 1. odstavka 2. člena** določa, da je vodstveni pregled dokumentiran pregled, ki ga vodstvo opravi najmanj enkrat letno, da zagotovi ustreznost in učinkovitost SUVI.

Predlagamo, da se obveznost izvedbe dokumentiranega (vodstvenega) pregleda iz enega leta podaljša na npr. vsaki dve leti.

Splošni akt v **2. členu** opredeljuje nekatere pojme (sredstva, grožnja, tveganja), za katerimi v tem aktu ni nobenih določb.

Predlagamo črtanje pojmov v 2. členu, saj drugi odstavek tega člena na enostaven način določa, da imajo ostali pojmi uporabljeni v tem splošnem aktu enak pomen, kot so določeni v ZEKom-1.

Agencija pojasnjuje, da so zahteve predloga splošnega akta povzete po standardu SIST ISO/IEC 27001, ki predstavlja dobro prakso na področju zagotavljanja varnosti. Omenjeni standard priporoča izvajanje vodstvenega pregleda najmanj enkrat letno oz. ob vsaki spremembi poslovanja, organizacije itd. Agencija bo definicijo vodstvenega pregleda črtala iz 1. odstavka 2. člena splošnega akta, ker se ta pojem v splošnem aktu ne uporablja. Vodstveni pregled se bo izvajal na podlagi splošnega akta o varnosti omrežij in storitev, na katerega se splošni akt sklicuje v 2. odstavku 3. člena.

Agencija se strinja s predlogom Sekcije v zvezi s črtanjem razlage pojmov iz 1. odstavka 2. člena predloga splošnega akta in bo predlog upoštevala. V predlogu splošnega akta se bodo črtali vsi pojmi, ki se ne uporabljajo v splošnem aktu.

Pripomba 4. člen

Dopis Sekcije:

2)

Splošni akt v **2. odstavku 4. člena** določa, da morajo biti hranjeni podatki dosegljivi in primerni za kasnejšo uporabo za namene iz prvega odstavka 163. člena ZEKom-1.

Predlagamo, da se obveznost hrambe podatkov na način, ki omogoča, da so podatki doscgljivi in primerni za kasnejšo uporabo, spremeni tako, da se predpišejo zahteve zavarovanja osebnih podatkov, kot so opredeljene v ZVOP-1 (dosegljivost in primernost kasnejše uporabe v ZVOP-1 ni neposredno definirana).

Agencija se s pripombo Sekcije strinja in bo v predlogu splošnega akta črtala 2. odstavek 4. člena, ker je to določilo že zajeto v 1. odstavku 163. člena ZEKom-1.

Agencija na pripombo sekcije, v zvezi s 1. odstavkom 4. člena, ki jo je Sekcija podala k pripombi 6. člena predloga splošnega akta pojasnjuje, da se s pripombo delno strinja in jo bo delno tudi upoštevala.

Pripomba na 5. člen

Dopis Sekcije:

3)

Splošni akt v **1. stavku 1. odstavka 5. člena** določa, da morajo postopki in tehnologija za hrambo podatkov zagotavljati nadzor dostopa do hranjenih podatkov in popolno sledljivost obdelave hranjenih podatkov z zagotavljanjem celovitosti, zaupnosti in razpoložljivosti hranjenih podatkov.

Predlagamo, da se pojmi celovitost, zaupnost in razpoložljivost podatkov definirajo tako, da njihov dejanski pomen ni potrebno iskati (niti je to dovoljeno) v drugih področnih predpisih, kot npr. Zakonu o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA) ali Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP) oziroma, da operaterji s Splošnim aktom, razen k določbam ZEKom-1 in ZVOP-1, niso morebiti zavezani zagotavljati zavarovanja hranjenih podatkov še v skladu z določbami zgoraj navedenih predpisov.

V 3. odstavku 5. člena je zelo splošna določba »Zagotovljena mora biti zaščita pred vplivi okolja«.

Določbo je potrebno konkretizirati.

Agencija se strinja s pripombo Sekcije in bo dodala razlage pojmov: zagotavljanje celovitosti, zaupnost in razpoložljivost.

Agencija na pripombo sekcije v zvezi s konkretizacijo 3. odstavka 5. člena in zagotavljanjem zaščite pred vplivi okolja pojasnjuje, da konkretizacija ukrepov ni potrebna, ker gre za ukrepe, ki so inženirski stroki splošno znani.

Dopis Sekcije:

4)

V **5. odstavku 5. člena Splošnega akta** je določeno, da je potrebno pri prenosu podatkov v hrambo drugemu operaterju ali tretjim strankam preko elektronskih komunikacijskih omrežij, uporabiti kriptografske metode, tako da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom.

Predlagamo, da se pri prenosu podatkov v hrambo drugem operaterju ali tretjim strankam preko elektronskih komunikacijskih omrežij ne zahteva posredovanje z uporabo kriptografskih metod, kot to sicer določa ZVOP-1, vendar le za občutljive osebne podatke.

Agencija na pripombo sekcije pojasnjuje, da med ZVOP-1 in splošnim aktom ni nobene zavezujoče povezave, tako da splošni akt lahko predpiše višje zahteve, kot jih ima ZVOP-1. ZVOP-1 namreč določa, da morajo biti postopki in ukrepi ustrezni glede na tveganja. Če gre torej za bolj tvegane osebne podatke, oziroma če bi bila tveganja visoka, potem so lahko tudi zahteve višje. Načeloma gre pri hranjenih podatkih za takšne podatke, ki sicer res ne sodijo v kategorijo taksativno naštetih občutljivih osebnih podatkov, a so tveganja z njimi dovolj visoka, da je upravičena zahteva za kriptiranje podatkov med prenosom po nezavarovanih elektronskih omrežjih. Agencija pripombe Sekcije ne bo upoštevala.

Pripomba na 4. In 6. člen

Dopis Sekcije:

5)

V **6. členu Splošnega akta je v 1. odstavku** določeno, da morajo postopki in tehnologija za hrambo podatkov onemogočiti spremembo (avtentičnost) ali izbris podatkov (celovitost) med potjo podatkov od izvirnih naprav do sistema za hrambo ter v času hrambe in zagotavljati povezanost reproducirane vsebine z vsebino izvirnih podatkov iz omrežja ter zagotavljati nesprejemljivost in neokrnjenost podatkov ter revizijsko sled.

V **2. odstavku 6. člena** je nadalje določeno, da se avtentičnost in celovitost hranjenih podatkov zagotovi z dodajanjem varnostnih vsebin (npr. elektronski podpis, časovni žig in podobno), z drugimi sorodnimi tehnološkimi sredstvi in postopki, ki omogočajo zapisovanje in večkratno branje ali z zagotavljanjem dodatnih organizacijskih ukrepov.

Splošni akt v **4. členu** določa, da morajo biti hranjeni podatki enake kakovosti kot podatki, ki so bili zajeti v omrežju in da vse določbe tega splošnega akta, ki veljajo za hranjene podatke, veljajo tudi za prenos podatkov od zajetja v omrežju do informacijskega sistema za hrambo podatkov.

Predlagamo, da določbe Splošnega akta o zavarovanju hranjenih podatkov za prenos podatkov od zajetja v omrežju do informacijskega sistema za hrambo podatkov ne veljajo smiselno enako kot za samo hrambo podatkov oziroma, da se odpravi zahteva po zagotavljanju avtentičnosti in celovitosti podatkov od njihovega zajema iz omrežja do izteka obdobja, v katerem morajo operaterji posamezen podatek hraniti.

Agencija se s pripombo ne strinja in je ne bo upoštevala.

Dopis Sekcije:

6)

V **4. odstavku 6. člena** Splošnega akta je določeno, da breme dokazovanja avtentičnosti, celovitosti in preprečevanja tajenja obdelave hranjenih podatkov in revizijske sledi nosi operater.

Predlagamo, da se določbe o bremenu dokazovanja izbrišejo oziroma da se le-te ne prenesejo na operaterje.

Agencija v zvezi s pripombo Sekcije pojasnjuje, da je v vseh primerih, ko pride do dvoma o avtentičnosti, celovitosti itd. hranjenih podatkov, dokazno breme na operaterju. Agencija pripombe sekcije ne bo upoštevala.

Pripomba na 8. člen

Dopis Sekcije:

7)

V **8. členu** Splošnega akta je navedeno, da ta akt začne veljati naslednji dan po objavi v Uradnem listu Republike Slovenije.

Predlagamo, da se akt začne uporabljati po preteku primernega obdobja, ki operaterjem dopušča prilagoditev na zahtevane spremembe (npr. 6 mesecev oziroma, da se počaka na odločitev Ustavnega sodišča).

Agencija pojasnjuje, da predlog splošnega akta ne prinaša nikakršnih bistvenih novosti ali dodatnih zahtev na področju zavarovanja hranjenih podatkov, ki jih ne bi že obravnaval do sedaj veljavni Splošni akt o tajnosti, zaupnosti in varnosti elektronskih komunikacij ter hrambi in zavarovanju hranjenih podatkov. V skladu z navedenim agencija meni, da ni razlogov za prehodno obdobje. V zvezi s pripombo o vloženi zahtevi za oceno ustavnosti in zakonitosti pa agencija odgovarja, da sama vložitev take zahteve nima učinka zadržanja ali odložitve uveljavitve ZEKom-1 in na njem temelječih podzakonskih aktov.

Direktor

Franc Dolenc