Gospodarska zbornica Slovenije

Združenje za informatiko in telekomunikacije

Dimičeva 13 ▪ 1504 Ljubljana ▪ T: (01) 58 98 000 ▪ F: (01) 58 98 100 ▪ info@gzs.si ▪ www.gzs.si

Komentarji na predlog Splošnega akta o zavarovanju hranjenih podatkov

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.

O b r a z l o ž i t e v :

Namen vodstvenega pregleda je pregledati rezultate notranjih presoj SUVI (in SUNP) ter v primeru morebitnih pomanjkljivosti izvesti ustrezne ukrepe za izboljšave. V različici SUVI analize, ki se je izvajala na podlagi, z novim zakonom razveljavljenega Splošnega akta o tajnosti, zaupnosti in varnosti elektronskih komunikacij ter hrambi in zavarovanju hranjenih podatkov, je bil obseg analize omejen. Na podlagi aktualnega Zakona o elektronskih komunikacijah pa mora operater zagotoviti pregled vseh sredstev, ki vplivajo na delovanje operaterjevega omrežja in storitev. Zaradi dejstva, da podroben pregled teh sredstev zahteva veliko časa (v skladu z definicijo sredstva v 4. točki 1. odstavka 2. člena Splošnega akta je namreč sredstvo vse, kar ima določeno vrednost za operaterja, njegovo dejavnost ali izvajanje storitev), pri izdelovanju dokumenta pa morajo sodelovati tudi različni zaposleni pri operaterju, ki podrobneje razumejo in poznajo delovanje ter varovanje posameznega sredstva, predlagamo, da se rok za izdelavo vodstvenega pregleda podaljša na (vsaj) dve leti. Izvedba vodstvenega pregleda v daljšem obdobju bi omogočilo operaterjem ne samo lažjo rezervacijo potrebnih finančnih in delovnih sredstev, ter razpoložljivosti relevantnih zaposlenih, ki morajo pri pregledu sodelovati, temveč posledično tudi (še) bolj poglobljeno in (še) bolj kvalitetno izvedbo analize oziroma vodstvenega pregleda.

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 dosegljivi 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).

Obrazložitev:

Zakon o elektronskih komunikacijah (ZEKom-1) v 165. členu določa, da operaterji zagotavljajo hrambo podatkov v skladu z zakonom, ki ureja varstvo osebnih podatkov (torej ZVOP-1) in da v zvezi s tem, operaterji vsak zase sprejmejo primerne tehnične in organizacijske ukrepe, s katerimi hranjene podatke zaščitijo pred uničenjem, izgubo ali spremembo in nepooblaščenimi ali nezakonitimi oblikami hrambe, obdelave, dostopa ali razkritja. Ker Zakon o varstvu osebnih podatkov (ZVOP-1) za zavarovanje osebnih podatkov terminov dosegljivosti in primernosti za kasnejšo uporabo neposredno ne ureja, bi bilo te termine potrebno ustrezno spremeniti ali dopolniti.

Ugotavljamo namreč, da sta navedena termina dosegljivost in primernost podatkov za kasnejšo uporabo natančneje opredeljena v Zakonu o elektronskem poslovanju in elektronskem podpisu (ZEPEP) in predstavljata standarde, s katerimi zagotovimo, da je elektronska oblika podatka oziroma dokumenta po samem zakonu enakovredna pisni obliki. Zaradi nejasne uporabe terminov v Splošnem aktu bi določbe 2. odstavka 4. člena lahko tolmačili kot, da so operaterji morebiti dolžni zagotoviti dosegljivost in primernost za kasnejšo uporabo v skladu z ZEPEP (torej enakovrednost elektronske oblike podatka s podatkom v pisni obliki), kar pa primarno ni namen določb 165. člena ZEKom-1. Na podlagi dejstva, da ZEKom-1 napotuje zgolj na uporabo Zakona o varstvu osebnih podatkov (ne pa morebiti tudi drugih zakonov) bi bila takšna zahteva (če je to njen namen) v nesorazmerju z zakonsko določenimi zahtevami v 165. členu ZEKom-1 oziroma v nasprotju z njimi.

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.

Obrazložitev:

V Splošnem aktu je opredeljeno, da se celovitost hranjenih podatkov zagotovi z dodajanjem varnostnih vsebin, z drugimi sorodnimi tehnološkimi sredstvi in postopki, ki omogočajo zapisovanje in večkratno branje ali z zagotavljanjem dodatnih organizacijskih ukrepov, medtem ko zaupnost in razpoložljivost podatkov v Splošnem aktu nista natančno definirana. Pomen slednjih je zato v skladu z 2. odstavkom 2. člena Splošnega akta potrebno poiskati v ZEKom-1 (ta v 165. členu napotuje tudi na uporabo Zakona o varstvu osebnih podatkov).

Zakon o elektronskih komunikacijah (ZEKom-1) navedenih terminov v povezavi s podatki

neposredno podrobneje ne ureja, temveč zgolj posredno v zvezi z drugimi sredstvi operaterja (npr. zaupnost komunikacije, razpoložljivost javno odstopnih storitev...).

Zakon o varstvu osebnih podatkov (ZVOP-1) pojmov celovitosti, zaupnosti, razpoložljivost v tej obliki ne uporablja, vendar pa vsebinsko z uporabo drugih terminov opredeljuje, da mora upravljavec osebnih podatkov preprečiti spremembo ali izgubo (npr. celovitost) in nepooblaščeno obdelavo podatkov (npr. zaupnost).

Čeprav gre za pojme, ki se v zvezi z informacijsko varnostjo v zakonodaji, kot tudi v informatiki redno uporabljajo, ugotavljamo, da imajo lahko ti različen pomen, ki jim ga posamezno (pravno) urejeno področje pripisuje. Z namenom preprečiti različno tolmačenje bi bilo le-te smiselno definirati tako, da njihov dejanski pomen ni potrebno iskati (niti je to dovoljeno) v drugih področnih predpisih oziroma tako, da se navedenim pojmom ne pripisuje morebiti preozek ali preširok pomen oziroma pomen, ki je zunaj okvirov določb ZEKom-1, ZVOP-1 ali Splošnega akta (na uporabo navedenih predpisov namreč odkazuje že Splošni akt sam, oziroma je tako izrecno določeno v 165. členu ZEKom-1).

Pojem celovitosti je na primer (kot načelo) definirano tudi v Zakonu o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA), in sicer kot standard nespremenljivosti in integralnosti dokumentarnega gradiva oziroma reprodukcije njegove vsebine, urejenosti dokumentarnega gradiva oziroma njegove vsebine ter dokazljivosti izvora dokumentarnega gradiva. Zaradi ureditve pojma oz. načela celovitosti v drugem predpisu in napotitve Splošnega akta na uporabo elektronskega podpisa, časovnega žiga oziroma sorodnih tehnoloških sredstev (v skladu s katerimi se zagotovi varen zajem in hramba dokumentarnega gradiva tudi po ZVDAGA) bi ureditev oziroma uporaba istega pojma na dveh mestih lahko vodila v zmotno prepričanje, da so operaterji dolžni hranjene podatke zajemati in hraniti v skladu z določbami ZVDAGA.

Zaradi nedoločenosti pojma zaupnosti, ki se v zakonodaji v zvezi s podatki uporablja predvsem v povezavi s tehničnimi zahtevami za varno elektronsko podpisovanje (kot je npr. urejeno v Zakon o elektronskem poslovanju in elektronskem podpisu - ZEPEP) bi njegov pomen lahko iskali v drugi predpisih, ki ta pojem podrobneje urejajo. Pojem zaupnosti bi lahko tako bil predmet razlage v skladu z določbami ZEPEP (že sam Splošni akt v zvezi s celovitostjo v 2. členu 6. odstavka napotuje na uporabo prav elektronskega podpisa, ki je kot ustrezno tehnološko sredstvo urejeno prav v ZEPEP), kar pa bi lahko prav tako vodilo v napačno prepričanje, da so operaterji dolžni zagotoviti obdelavo hranjenih podatkov v skladu z določbami ZEPEP.

Zaradi dejstva, da Splošni akt v zvezi z uporabljenimi pojmi napotuje na uporabo določb ZEKom-1, ta pa v 165. členu na zavarovanje osebnih podatkov v skladu z določbami ZVOP-1, so možnosti razlage posameznih določb sicer omejene, kar med drugim pomeni tudi, da bi bilo morebitno razlaganje pojma celovitosti, zaupnosti ali razpoložljivosti (npr. v skladu z ZVDAGA ali ZEPEP) preširoko in v nesorazmerju z dejanskimi zahtevami 165. člena ZEKom-1 oziroma v nasprotju z njimi (v kolikor je takšno tolmačenje uporabljenih pojmov namen avtorja predloga Splošnega akta).

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.

O b r a z l o ž i t e v :

Zaradi dejstva, da hranjeni podatki niso podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali evidenc, ki se vodijo na podlagi zakona, ki ureja prekrške ali podatki o biometričnih značilnosti (t.j. ne ustrezajo definiciji občutljivih osebnih podatkov po 19. točki 6. člena ZVOP-1), v skladu z zakonom s področja varstva osebnih podatkov le-te ni potrebno obravnavati kot občutljive osebne podatke. Iz navedenega izhaja, da ureditev iz 5. odstavka 5. člena Splošnega akta neutemeljeno od operaterjev zahteva zagotavljanje višje stopnje varnosti, kot sicer to od upravljavcev osebnih podatkov zahteva ZVOP-1 (na uporabo katerega izrecno napotuje zakonodajalec v 165. členu ZEKom-1).

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.

O b r a z l o ž i t e v :

Operaterji morajo v skladu z 167. členom ZEKom-1 na lastne stroške zagotoviti vse potrebne tehnične in organizacijske ukrepe za hrambo podatkov, kar ne vpliva samo na visoke začetne stroške investicije, temveč tudi na višje stroške poslovanja, saj mora operater zagotavljati ustrezno tehnično usposobljenost zaposlenih kot tudi njihovo razpoložljivost. Dodatne obremenjevanje, z implementacijo postopkov (npr. elektronsko podpisovanje), s katerimi se zagotovi avtentičnost in celovitost hranjenih podatkov (npr. po ZEPEP ali ZVDAGA), kot tudi podatkov pri samem zajemanju iz omrežja, za operaterje predstavlja dodatne stroške (poleg stroškov, ki jih imajo ti v zvezi s samo hrambo podatkov v ločenem informacijskem sistemu), ki so hkrati v nesorazmerju z dejanskimi zahtevami ZEKom-1.

Zakon o elektronskih komunikacijah (ZEKom-1) v 165. členu namreč določa, da operaterji zagotavljajo hrambo podatkov v skladu z zakonom, ki ureja varstvo osebnih podatkov (torej

ZVOP-1) in da v zvezi s tem, operaterji vsak zase sprejmejo primerne tehnične in organizacijske ukrepe, s katerimi hranjene podatke zaščitijo pred uničenjem, izgubo ali spremembo in nepooblaščenimi ali nezakonitimi oblikami hrambe, obdelave, dostopa ali razkritja.

Zaradi dejstva, da osebni podatki, ki so predmet hrambe v skladu z 165. členu ZEKom-1, ne ustrezajo definiciji občutljivih osebnih podatkov (kot so opredeljeni v 19. točki 6. člena ZVOP-1) ni razloga, da bi pri prenosu podatkov v hrambo drugemu operaterju ali tretjim strankam preko elektronskih komunikacijskih omrežij, operaterji morali uporabljati kriptografske metode, tako da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom oziroma toliko več ni razloga, da bi v skladu z ZVOP-1 bili operaterji zavezani zagotavljati avtentičnost in celovitost podatkov (z uporabo el. podpisa, drugih kriptografskih metod) že pri njihovem zajemu iz omrežja in nadaljnji hrambi teh podatkov.

Zagotavljanje avtentičnosti, celovitost ter kasnejše dostopnosti hranjenih podatkov (z uporabo tehnoloških sredstev kot je elektronsko podpisovanje ali sorodnimi tehnološkimi sredstvi) je pomembno predvsem takrat, kadar želimo, da se dokumentom (podatkom) v elektronski obliki pred sodiščem (po zakonu samem) priznava enaka dokazna vrednost v primerjavi z dokumenti v pisni obliki.

Enako dokazno vrednost podatkov v elektronski obliki pa je mogoče zagotoviti zgolj ob smiselni uporabi določb Zakona o elektronskem poslovanju in elektronskem podpisu (ZEPEP) ali Zakona o varstvu dokumentarnega in arhivskega gradiva (ZVDAGA), tako da se pri samem zajemu kot hrambi in arhiviranju podatkov upoštevajo tehnološki postopki in druge zahteve, ki jih navedena predpisa urejata, medtem ko ZVOP-1 (na uporabo katerega napotuje v 165. členu ZEKom-1 sam) takšnega zavarovanja osebnih podatkov od upravljavcev osebnih podatkov ne zahteva.

Splošni akt v zvezi s pojmi, ki v tem aktu niso izrecno definirani, napotuje na uporabo določb ZEKom-1, ta pa v 165. členu na zavarovanje osebnih podatkov v skladu z določbami ZVOP-1, zato so možnosti razlage posameznih določb Splošnega akta sicer pravno gledano omejene. Vendar zaradi specifičnosti namena hrambe prometnih podatkov, t.j. zagotavljanje na zalogo zbranih dokazov v morebitnem sodnem postopku, ne gre prezreti povezave med dokazno vrednostjo hranjenih podatkov (predloženih kot dokazno gradivo) in zahtevami iz Splošnega akta, ki so sorodne ureditvi po ZEPEP in ZVDAGA - na podlagi katerih je v skladu z veljavno zakonodajo mogoče zagotoviti, da so podatki zajeti in hranjeni v elektronski obliki enakovredni podatkom, ki so hranjeni v pisni obliki.

V zvezi z navedenim lahko ugotovimo, da bi morebitne zahteve po skladnosti obdelave hranjenih podatkov z določbami ZEPEP ali ZVDAGA presegale zahteve postavljene v 165. členu ZEKom-1, ki določajo, da so operaterji dolžni zagotoviti zavarovanje osebnih podatkov (le) v skladu z Zakonom o varstvu osebnih podatkov (in ne morebiti s katerim drugim predpisom). Da so operaterji zavezani obdelovati hranjene podatke (le) v skladu z ZVOP-1 povsem sovpada z dejstvom, da so hranjeni prometni podatki (zgolj) osebni podatki (poseben režim obdelave ni potreben), katerih namen zbiranja je opredeljen z zakonom.

V kolikor pa je namen Splošnega akta zagotoviti prav to, da se dokumentom oz. podatkom v elektronski obliki že po zakonu samem priznava enaka dokazna vrednost v primerjavi z dokumenti v pisni obliki, menimo, da bi zagotavljanje skladnosti z navedenimi zakoni za operaterje pomenilo dodatne (in hkrati neutemeljene) finančne, tehnične in administrativne obremenitve, saj je npr. samo v skladu z ZVDAGA potrebno pripraviti in sprejeti notranja pravila za zajem in hrambo gradiva v digitalni obliki ter zagotoviti in vpeljati postopke za varen zajem in hrambo dokumentarnega gradiva, kot tudi skladnost z mnogimi drugimi zahtevami, ki jih ta zakon in temu zakonu podrejeni predpisi določajo.

Neupravičenost takšne dodatne obremenitve temelji tudi na dejstvu, da so Ustavna sodišča v Nemčiji, Romuniji in na Češkem kot tudi Višje sodišče na Irskem prepoznala že sam ukrep obvezne hrambe podatkov o prometu elektronskih komunikacij kot sporen ter dejstvu, da

Ustavno sodišče Republike Avstrije zaradi dvomov o skladnosti Direktive z Evropsko konvencijo o temeljnih pravicah in svoboščinah v decembru 2012 na Sodišče EU naslovilo zahtevo za predhodno odločanje in da je navsezadnje Informacijski pooblaščenec (čigar predhodno mnenje mora pred sprejetjem tega Splošnega akta pridobiti tudi Agencija) na Ustavno sodišče Republike Slovenije naslovil zahtevo za oceno ustavnosti in zakonitosti ukrepa hrambe prometnih podatkov – kar pomeni, da bi lahko bile dodatne, kot tudi že vse pretekle, z ZEKom in ZEKom-1 zahtevane investicije v sistem hrambe ekonomsko neupravičene (nesmiselne), vsaj do trenutka, ko relevantno sodišče odloči o morebitni ukinitvi zbiranja teh podatkov na zalogo. Da so (lastna) že zagotovljena finančna sredstva operaterjev presegla dejanski učinek z zakonom predvidenega ukrepa, je razvidno tudi iz podatkov Informacijskega pooblaščenca, ki je podal ugotovitev, da operaterji na leto obdelajo več sto milijonov osebnih podatkov, pri čemer letno prejmejo le 400 do 700 sodnih odredb za njihovo posredovanje (številka končnih obsodb ravno na podlagi hranjenih podatkov pa je še manjša).

V skladu z navedenimi dejstvi bi bilo torej neupravičeno trditi, da so dodatna obvezna (tehnološka in administrativna) vlaganja v informacijski sistem hrambe podatkov z namenom zagotoviti avtentičnost in celovitost podatkov zajetih iz omrežja (v skladu z ZEPEP ali ZVDAGA) bodisi utemeljena bodisi v sorazmerju z negativnimi (ali pozitivnimi) učinki.

Poleg navedenega pa implementacija ustreznih ukrepov, ki zagotavljajo avtentičnost in celovitost podatkov od njihovega nastanka (zajem podatkov iz omrežja) do hrambe v ločenem in neodvisnem informacijskem sistemu ni nujno tehnično izvedljiva, saj bi to pomenilo, da bi morali operaterji že na baznih postajah npr. elektronsko podpisovati podatke, ki se ustvarijo – torej še preden se preselijo v t.i. mediacijo in naprej v bazo hranjenih podatkov. Trenutne tehnične možnosti takšne rešitve niti ne dopuščajo.

Stroške implementacije organizacijskih postopkov, tehničnih ukrepov in dodatnih tehničnih zmogljivosti, s katerimi bi mogoče lahko zagotovili avtentičnost in celovitost osebnih podatkov, bi (navkljub neutemeljenim razlogom) bili najverjetneje tehnično sposobni vzpostaviti in financirati ter v praksi izvajati zgolj največji operaterji elektronskih komunikacijskih storitev, vsekakor pa ne tudi vsi operaterji, ki izvajajo to dejavnost na ozemlju Republike Slovenije.

Ob morebitnem izvajanju nadzora (in izrekanju globe) le pri tistih operaterjih, ki morda lahko zagotovijo ustrezna sredstva (ne pa tudi pri vseh operaterjih), bi z nedoslednim upoštevanjem izpolnjevanja zakonsko določenih zahtev lahko prišlo do kršitev ustavno zavarovanega načela, t.j. da so vsi (brez izjeme) pred zakonom enako obravnavani. V skladu z navedenim bi bilo torej smiselno zahtevati takšno raven zavarovanja hranjenih podatkov, ki so jo sposobni implementirati v svoje poslovne procese vsi operaterji telekomunikacijskih storitev (ali pa vsaj velika večina) – t.j. v skladu z določbami ZVOP-1 (in ne morebiti drugih področnih prepisov).

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.

O b r a z l o ž i t e v :

V morebitnem nadzorstvenem (inšpekcijskem) postopku so operaterji (oz. stranke v postopku) že v skladu z določbami 19. člena Zakona o inšpekcijskem nadzoru dolžni nadzorstvenem organu predložiti vsa dokaze in podatke, ki jih ta zahteva. V skladu z navedenim gre torej za

podvajanje dolžnosti stranke v inšpekcijskem postopku, zato se ta določba lahko briše oziroma odstrani.

V kolikor ne gre za dokazovanje v morebitnem inšpekcijskem nadzoru, temveč je imel avtor Splošnega akta pred očmi drugo vrsto dokazovanja, potem bi bilo le-to smiselno bolj natančno opredeliti, in sicer tako, da lahko operaterji natančno razumejo dolžnosti, naložene s tem Splošnim aktom.

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).

O b r a z l o ž i t e v :

Splošni akt v vsebini predloga, ki je bil predstavljen zainteresirani javnosti od operaterjev zahteva določene (dodatne) spremembe, katerih realizacija v nekaj dneh sploh ni mogoča.

Operaterji morajo namreč primarno rezervirati in zagotoviti ustrezna finančna sredstva za izvedbo potrebnih (in nepričakovanih) prilagoditev, sprejeti ustrezne informacijske rešitve, ki omogočajo obdelovanje hranjenih podatkov v skladu z zahtevami Agencije, ter čas za implementacijo vseh organizacijskih, tehničnih in drugih postopkov ter ukrepov, potrebnih za preprečitev izgube hranjenih podatkov ali začasno nedelovanje obstoječega in spremenjenega sistema za hrambo osebnih podatkov (v skladu z vsemi drugimi zahtevami ZEKom-1).

Poleg navedenega je Informacijski pooblaščenec na Ustavno sodišče Republike Slovenije naslovil zahtevo za oceno ustavnosti in zakonitosti ukrepa hrambe prometnih podatkov, kar bi ob razsodbi sodišča, da ukrep hrambe prometnih podatkov neupravičeno ali v prevelikem obsegu posega v ustavnopravne zavarovane pravice posameznika, pomenilo, da operaterji dodatnih ukrepov za zavarovanje osebnih podatkov sploh ne bi potrebovali implementirati v poslovne procese.

Dušan Zupančič
Direktor Združenja za informatiko in telekomunikacije pri GZS

Špela Dekleva
Predsednica Sekcije operaterjev elektronskih komunikacij SOEK pri ZIT, GZS