Varstvo osebnih podatkov & računalništvo v oblaku

INFORMACIJSKI POOBLAŠČENEC
&
Cloud Security Alliance Slovenia Chapter
Slovenski inštitut za revizijo
Slovenski odsek ISACA
Zavod e-Oblak, Eurocloud Slovenia

Namen dokumenta:	Namen smernic je podati enotne kontrolne točke, s pomočjo katerih bodo lahko tako **uporabniki** kot **nadzorni organi** sprejemali bolj informirane odločitve glede uporabe in nadzora računalništva v oblaku v delu, ki se nanaša na obdelavo osebnih podatkov, **ponudnikom storitev** računalništva v oblaku ter **iniciativam za varnost in certificiranje tovrstnih storitev** pa naj bi ponudile napotke za nadaljnji razvoj s ciljem skladnosti z zakonodajo o varstvu osebnih podatkov.
Ciljne javnosti:	• uporabniki storitev računalništva v oblaku – mala in srednje velika podjetja in organizacije • (lokalni) ponudniki storitev računalništva v oblaku • državni nadzorniki za varstvo osebnih podatkov • (preizkušeni) revizorji informacijskih sistemov • notranji in zunanji presojevalci in revizorji
Status:	javno
Verzija:	1.0
Datum izdaje:	15.6.2012
Ključne besede:	smernice, računalništvo v oblaku, ZVOP-1, varstvo osebnih podatkov, varnost, zasebnost, iznos osebnih podatkov v tretje države, pogodbena obdelava osebnih podatkov, analiza tveganj, informacijska varnost.

KAZALO

O SMERNICAH INFORMACIJSKEGA POOBLAŠČENCA

Namen smernic IP je podati skupne praktične napotke za upravljavce zbirk osebnih podatkov (OP) na jasen, razumljiv in uporaben način in s tem odgovoriti na najpogosteje zastavljena vprašanja s področja varstva osebnih podatkov, s katerimi se srečujejo posamezni upravljavci zbirk OP. S pomočjo smernic naj bi upravljavci dobili priporočila, kako naj v praksi zadostijo zahtevam Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljevanju ZVOP-1). Konkretne smernice so namenjene tako potencialnim uporabnikom storitev računalništva v oblaku kakor tudi nadzornim, revizorskim in svetovalnim inštitucijam.

Pravno podlago za izdajo smernic Pooblaščencu daje 49. člen ZVOP-1, ki med drugim določa, da Pooblaščenec daje neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način ter pripravlja in daje neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju.

Oglejte si tudi:

- Mnenja IP: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/
- Brošure IP: http://www.ip-rs.si/publikacije/prirocniki/

Smernice IP so objavljene na spletni strani: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/

1. UVOD

Računalništvo v oblaku obljublja dostopnost do računalniških zmogljivosti iz katerekoli lokacije na ekonomičen, prilagodljiv in nadgradljiv način, zato ne preseneča, da se za oblak zanima čedalje več organizacij, ki obdelujejo osebne podatke. To pa neizogibno poraja dvome glede skladnosti z zakonodajo na področju varstva osebnih podatkov in zasebnosti. Zlasti javne oblike računalništva v oblaku vzbujajo pomisleke glede varstva osebnih podatkov, ki izvirajo iz narave računalništva v oblaku, ki prinaša specifična tveganja, ta pa se kažejo predvsem na področju ureditve pogodbene obdelave oz. zunanjega izvajanja storitev, informacijske varnosti oz. zavarovanja osebnih podatkov ter izvoza podatkov v tretje države. Potenciali računalništva v oblaku so izjemni, ne sme pa zaradi tega priti do nižanja ravni varstva osebnih podatkov kot temeljne človekove pravice, kar je tudi eno temeljnih priporočil mednarodne delovne skupine IWGDPT v t.i. Sopot Memorandumu o varstvu osebnih podatkov pri računalništvu v oblaku[1].

Za pravno nespornost in praktično sprejemljivost računalništva v oblaku je pri izvajalcih, ki jih nimamo pod neposrednim nadzorom, bistveno zaupanje. Naročnik oziroma upravljavec osebnih podatkov je tisti, ki mora bodisi sam ali s pomočjo ustrezno usposobljenih tretjih strank izvesti analizo tveganja in sprejeti odločitev ali bo zaupal določenemu ponudniku ali ne. Ponudnik kakršnekoli storitve, ki naročniku ne zmore ponuditi

[1] IWGDPT: Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum" - 51st meeting, 23-24 April 2012, Sopot (Poland): http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

zadovoljivih odgovorov in zagotovil glede tega, kako bodo zavarovani naročnikovi podatki, bi moral pri naročniku, ki zna pravilno oceniti tveganja v povezavi s svojimi podatki, vzbuditi določeno mero previdnosti in zadržanosti.

Namen pričujočih smernic je dvigniti stopnjo ozaveščenosti predvsem o tveganjih, ki jih prinaša obdelava osebnih podatkov v oblaku, s pomočjo kontrolnega seznama pa tudi ponuditi jasnejšo sliko o obstoječih zahtevah zakona o varstvu osebnih podatkov. Informacijski pooblaščenec je mnenja, da številni ponudniki storitev računalništva v oblaku potencialnim uporabnikom trenutno večinoma še ne ponudijo zadostnih informacij za izvedbo ustreznih analiz tveganja in da je treba vzpostaviti mehanizme, ki bodo omogočali ločevanje zaupanja vrednih ponudnikov računalništva v oblaku od tistih tveganih. V času, ko potekajo številne aktivnosti na področjih standardizacije, certifikacije in drugih mehanizmov za izgradnjo zaupanja v računalništvo v oblaku, vam bodo te smernice upamo v pomoč.

2. KONCEPT IN GLAVNE ZNAČILNOSTI RAČUNALNIŠTVA V OBLAKU

Računalništvo v oblaku je vzorec uporabe informacijske tehnologije, ki ne zahteva velikih investicij v zmogljivo programsko opremo. Pri tem se do aplikacij in storitev dostopa prek omrežja in je za to potreben le internetni dostop. Dostop do oblaka je možen z uporabo klasičnega odjemalca, kjerkoli in kadarkoli uporabnik potrebuje določeno informacijsko sredstvo, brez potrebe po posebni programski opremi. Računalništvo v oblaku torej omogoča takojšnji dostop do prednastavljenih skupnih informacijskih virov (npr. omrežja, strojne opreme, pomnilniških enot, programske opreme, različnih informacijskih storitev), ki so lahko uporabniku na razpolago takoj, z minimalnim dogovarjanjem s ponudnikom. **Oblikuje ga 5 bistvenih značilnosti, 3 storitveni modeli in 4 izvedbeni modeli.**

2.1 Bistvene značilnosti računalništva v oblaku

»Samopostrežba na zahtevo«
Uporabnik se lahko samostojno odloči za zakup računalniških zmogljivosti, kot so strežniški čas in omrežna hramba, glede na trenutne potrebe brez odvečne komunikacije s posameznimi ponudniki storitev.

Širok mrežni dostop
Računalniške zmogljivosti so dostopne prek omrežja skozi standardizirane mehanizme, ki podpirajo različne odjemalce, kot so mobilniki, tablice, prenosniki in delovne postaje.

Združevanje sredstev
Računalništvo v oblaku razen klasične virtualizacije uporablja tudi zmožnosti avtomatizacije in orkestracije storitev ter sobivanja uporabnikov na istih informacijskih virih (angl. »multiten ancy«). Ta je bistvena lastnost računalništva v oblaku, kadar več uporabnikov hkrati pristopa do istih tehnoloških virov. Do tega mehanizma je namreč veljalo, da je ponudnik za vsakega uporabnika zagotovil ločeno infrastrukturo, s pojavom mehanizmov sobivanja pa je možno zagotoviti enovito konfiguracijo, enoten nadzor nad storitvami, nadgradnje in enostavnejše okrevanje v primeru katastrofe in/ali restavriranje podatkov. S tem je tesno povezana ena od temeljnih značilnosti računalništva v oblaku in sicer odsotnost vezave podatkov na natančno opredeljeno fizično lokacijo, saj se lahko podatki (hkrati) nahajajo v več podatkovnih centrih, ki se lahko nahajajo kjerkoli po svetu.

Visoka elastičnost
Uporabnik lahko glede na svoje trenutne potrebe hitro poveča ali zmanjša obseg zakupljenih računalniških zmogljivosti, ki jih uporabnik dojema kot neomejene.

Plačilo na osnovi uporabe
Oblačni sistemi avtomatično nadzirajo in optimizirajo vire glede na vrsto storitve (npr. hramba, procesiranje, pasovna širina, število aktivnih uporabnikov). Transparentnost porabe virov je zagotovljena z njihovim nadzorom in spremljanjem.

2.2 Storitveni modeli

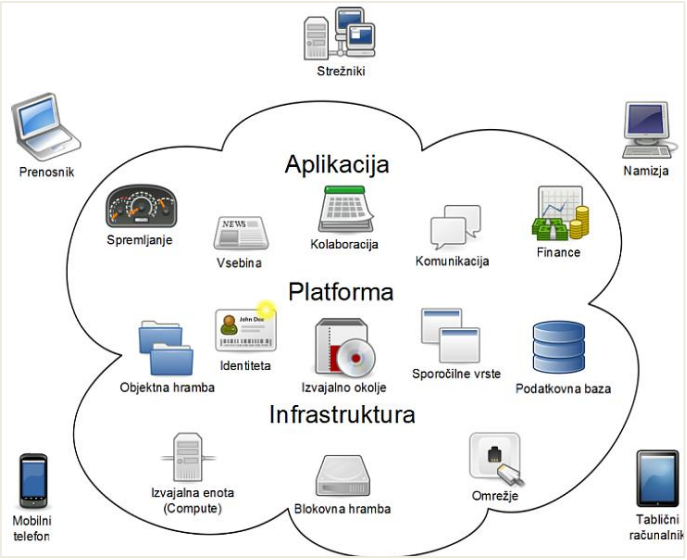
Storitveni modeli se nanašajo na vrsto storitve. Model storitev v oblaku je lahko izveden na tri različne načine, ki pa so običajno zgrajeni drug vrh drugega in se lahko uporabljajo neodvisno drug od drugega.

Infrastruktura kot storitev (angl. »Infrastructure as a Service - IaaS«)
Infrastruktura kot storitev se nanaša na računalniško infrastrukturo, pogosto ponujeno z uporabo virtualizacije. V to kategorijo sodijo strežniki, hramba, omrežje ali infrastruktura kot storitev (IaaS) – najpomembnejši ponudniki[2] so VMware, Oracle, IBM, Microsoft, KVM, OpenStack, Xen, Eucalyptus, Nimbus, OpenNebula,Citrix Cloud, AppNexus, Amazon EC2, itd.

Platforma kot storitev (angl. »Platform as a Service - PaaS«)
Platforma kot storitev že vključuje osnovne dodatne funkcionalnosti (običajno v obliki programskega vmesnika, ang. »Application Programming Interface – API«), ki jih uporabnik kot platformo uporablja pri razvoju in uporabi lastnih informacijskih rešitev. V to kategorijo med drugim sodi okolje za razvoj aplikacij ali platforma kot storitev (PaaS). Vidnejši ponudniki so Google AppEngline, Microsoft Azure, Oracle PaaS, IBM PaaS, VMware SpringSource, itd.

Programska oprema kot storitev (angl. »Software as a Service - SaaS«)
Programska oprema kot storitev pomeni zagotavljanje celotne infrastrukture skupaj s programsko opremo in nastavitvami za njeno delovanje. V to kategorijo sodijo funkcionalnosti poslovnih aplikacij ali programska oprema kot storitev (SaaS). Vidnejši ponudniki so salesforce.com, Microsoft (npr. Office 365), Google Apps (vključno z Gmail). Povedano drugače – običajno uporabnik potrebuje le brskalnik in dostop do interneta, vse ostalo zagotavlja ponudnik storitve, v nekaterih primerih celo brezplačno.

[2] Pregleden prikaz ponudnikov storitev računalništva v oblaku:
http://www.opencrowd.com/assets/images/views/views_cloud-tax-lrg.png



Slika 1: Abstraktni prikaz koncepta računalništva v oblaku

2.3 Izvedbeni modeli računalništva v oblaku

Izvedbeni modeli računalništva v oblaku so naslednji:

Javni oblaki (ang. »Public Cloud«) so dostopni javnosti in ni omejitev glede tega kdo jih lahko uporablja. So IKT storitve ponudnika, do katerih lahko preko interneta dostopa kdorkoli.
Zasebni oblaki (angl. »Private Cloud«) so dostopni samo v zasebnem omrežju. IKT storitve so ponujene iz lastnega podatkovnega centra. Vse storitve kot tudi infrastruktura je pod nadzorom ponudnika, upravljanje pa se lahko izvaja tudi s pomočjo tretjega. Storitve so dostopne preko interneta ali preko navideznih zasebnih omrežij.
Oblaki skupnosti (angl. »Community Cloud«) so dostopni omejenemu številu uporabnikov, z znanimi značilnostmi.
Hibridni oblaki (angl. ».»Hybrid Cloud«) so IKT storitve računalništva v oblaku, ki so sestavljene iz storitev javnega in zasebnega oblaka.

Ponudniki storitev računalništva v oblaku navajajo številne prednosti računalništva v oblaku: od nižjih stroškov zaradi odsotnosti potreb po vložkih v npr. strojno opremo, do večje in hitrejše prilagodljivosti potrebam naročnika (enostavno lahko zakupite dodatne zmogljivost takrat, ko jih potrebujete) ter domnevno nižjih stroškov vzdrževanja, podpore in drugih storitev, ki so vezane na IKT človeške vire. Pri določenih izvedbenih modelih je pogosto vse, kar potrebujete, dostop do interneta in brskalnik.

Bistvene značilnosti računalništva v oblaku se lahko odrazijo tako kot prednosti kot slabosti, vsekakor pa so povezane tudi s tveganji, ki niso značilna za druge oblike zunanjega izvajanja IKT storitev.

3. RAČUNALNIŠTVO V OBLAKU SKOZI TEMELJNA NAČELA VARSTVA OSEBNIH PODATKOV

3.1 OSNOVNI POJMI

Glede na določbe ZVOP-1 se uporabnik oz. **naročnik** storitev računalništva v oblaku običajno[3] šteje za **upravljavca osebnih podatkov**, **ponudnik storitev** računalništva v oblaku pa za njegovega **pogodbenega obdelovalca**, ki za naročnika izvaja določena ravnanja z osebnimi podatki, kot so hramba, kopiranje, posredovanje in podobno. Ne pozabite – vsakršno ravnanje z osebnimi podatki se šteje za obdelavo osebnih podatkov[4], osebni podatki pa so vsi podatki, ki se nanašajo na določenega ali določljivega posameznika. Pozor – tudi če sami ne vemo, na koga se podatek nanaša, lahko morda drugi brez nesorazmerno velikega napora ali sredstev ugotovijo, na koga se določen podatek nanaša. Na določljivost posameznika je tako treba gledati široko in ne zgolj skozi lastne zmožnosti ali neposredno prisotnost drugih podatkov, ki omogočajo določljivost posameznika.

Določeni vidiki varstva osebnih podatkov, kot so načela sorazmernosti, namenskosti in rokov hrambe so seveda sestavni del ureditve varstva osebnih podatkov, a ne predstavljajo posebne specifike pri odločitvi za uporabo storitev računalništva v oblaku. Vidiki varstva osebnih podatkov, ki se ob uporabi računalništva v oblaku najbolj izpostavljajo, so predvsem naslednji:

- pogodbena obdelava osebnih podatkov,
- zavarovanje osebnih podatkov in
- iznos osebnih podatkov v tretje države.

Področje računalništva v oblaku z vidika varstva osebnih podatkov pokrivata pred kratkim objavljeni mnenji Mednarodne delovne skupine za varstvo osebnih podatkov v telekomunikacijah[5] in Delovne skupine iz člena 29[6].

3.2 POGODBENA OBDELAVA OSEBNIH PODATKOV

Upravljavec osebnih podatkov se lahko odloči, da bo določena ravnanja z osebnimi podatki zaupal pogodbenemu obdelovalcu. Praviloma naj bi naročnik določal, kaj in kako bo počel pogodbeni obdelovalec, pri današnji ponudbi storitev računalništva v oblaku pa so praviloma ponudniki storitev računalništva v oblaku tisti, ki določajo pogoje uporabe, ravni zavarovanja podatkov in druge pomembne elemente poslovanja. Ne glede na to pa so naročniki tisti, ki imajo pravno podlago za obdelavo osebnih podatkov in tisti, ki so določili namen in sredstva obdelave, zato moramo praviloma **naročnike šteti kot upravljavce osebnih podatkov**, **ponudnike**

[3] V določenih primerih lahko gre tudi za dva upravljavca, predvsem kadar ponudnik obdeluje osebne podatke tudi izven navodil naročnika, seveda pa mora imeti za to pravno podlago. Ključno je, da naročnik in ponudnik storitve jasno opredelita svoji vlogi.

[4] Tu je treba poudariti, da gre tudi v situacijah, ko pogodbeni obdelovalec sploh ne ve, na koga se podatki nanašajo (npr. nudi zgolj storitev gostovanja prostora za hrambo podatkov), za obdelavo osebnih podatkov. Še več – tudi če upravljavec osebnih podatkov svoje podatke hrani pri zunanjemu ponudniku hrambe in na njegovih diskovnih zmogljivostih hrani svoje podatke v kriptirani, zunanjemu ponudniku hrambe neberljivi obliki, tudi takrat gre za hrambo osebnih podatkov, s tem pa za obdelavo osebnih podatkov in zakonske dolžnosti tako naročnika kot ponudnika storitve.

[5] Sopot Memorandum, dostopno prek: http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

[6] http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

storitev računalništva v oblaku pa kot pogodbene obdelovalce[7]. Pogodbena obdelava osebnih podatkov je torej dopustna praksa pod pogojem, da so vzpostavljene določene varovalke, med njimi pa je bistveno to, da upravljavec osebnih podatkov lahko računa na določeno raven zavarovanja osebnih podatkov tako s strani pogodbenega izvajalca kot s strani njegovih podizvajalcev. ZVOP-1 tako v 11. členu določa, da sme zunanji izvajalec opravljati posamezna opravila v zvezi z obdelavo osebnih podatkov v okviru naročnikovih pooblastil in osebnih podatkov, ne sme pa jih obdelovati za noben drug namen. Medsebojne pravice in obveznosti morata urediti s pogodbo, ki mora biti sklenjena v pisni obliki in mora vsebovati tudi dogovor o postopkih in ukrepih, s katerimi bodo podatki zavarovani pred slučajnim ali namernim nepooblaščenim uničevanjem podatkov, njihovo spremembo ali izgubo ter nepooblaščeno obdelavo teh podatkov (24. člen. ZVOP-1). Delovna skupina iz člena 29 je v svojem mnenju o računalništvu v oblaku natančneje opredelila, kaj naj bi vsebovala pogodba.

Na tej točki pa pridemo tudi do glavnega pomisleka varuhov zasebnosti – ali in kdaj lahko zaupamo (zunanjemu) ponudniku računalništva v oblaku?

Naročniki so namreč pogosto soočeni s splošnimi pogoji uporabe storitev, pri katerih je upravljavec osebnih podatkov pogosto stranka z manjšo pogajalsko močjo, ki lahko običajno zgolj sprejme ali zavrne splošne pogoje uporabe storitev, ki mu jih je predložil ponudnik storitev računalništva v oblaku, čeprav naj bi bil upravljavec osebnih podatkov tisti, ki določa namene, okoliščine in sredstva obdelave ter zahtevano raven zavarovanja osebnih podatkov.

3.3 ZAVAROVANJE OSEBNIH PODATKOV

Informacijska varnost je bistveni del in eno temeljnih načel vseh aktov, ki urejajo področje varstva osebnih podatkov in kot *ožji del varstva osebnih podatkov* pomeni varovanje celovitosti, zaupnosti in razpoložljivosti osebnih podatkov. Na pomen zavarovanja osebnih podatkov je zelo podrobno opozoril danski nadzorni organ za varstvo osebnih podatkov, ki predvsem zaradi teh pomislekov eni od danskih občin ni dovolil uporabe storitve v oblaku ponudnika iz ZDA[8] podobno stališče je sprejel tudi norveški nadzorni organ[9]. Ali so naši podatki v oblaku bolje varovani ali ne, ni enostavno vprašanje in nanj ni dopustno pavšalno odgovoriti v smislu, da je nekaj, kar imamo sami pod nadzorom, tudi bolj varno (ENISA[10], 2009). Kot poudarjajo nekateri avtorji gre predvsem za vprašanje zaupanja (Schneier[11], 2009). Tako kot moramo zaupati operacijskemu sistemu, strojni opremi, programski opremi, moramo zaupati tudi ponudniku računalništva v oblaku – gre pravzaprav za podobno stvar in le za dodatnega ponudnika, ki ga moramo presojati z vidika zaupanja. Pri zunanjem izvajanju pa je vseeno ena pomembna razlika – če imamo računalniške zmogljivosti pod svojim nadzorom, lahko sami ali s pomočjo drugih poskrbimo za varnost s pomočjo drugih varnostnih mehanizmov (dokumente na svojem računalniku lahko npr. varujemo z varnostnimi kopijami, protivirusnimi programi, če recimo popolnoma na zaupamo posamezni rešitvi, npr. brskalniku ali operacijskem sistemu). Pri zunanjemu izvajalcu pa gre za zaupanje v celoti, kar ne vključuje le zaupanja v varnostne postopke in ukrepe, temveč gre tudi za zanesljivost,

[7] Delovna skupina iz člena 29 je v mnenju št. 1/2010 o upravljavcu-obdelovalcu zapisala: »neravnovesje pogodbene moči med majhnim upravljavcem podatkov in velikimi ponudniki storitev ne sme šteti za utemeljitev tega, da upravljavec sprejme pogodbene klavzule in pogoje, ki niso v skladu z zakonodajo o varstvu podatkov.« Mnenje je dostopno na povezavi http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_sl.pdf.

[8] Občina je želela uporabljati Google Apps. Datatilsynet, The Danish Data Protection Agency: Processing of sensitive personal data in a cloud solution. Dostopno na: http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/ (objavljeno 3.2.2011).

[9] http://datatilsynet.no/English/Publications/Will-not-let-Norwegian-enterprises-of-Google-Apps

[10] ENISA: Cloud Computing Risk Assessment. Dostopno na: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment (objavljeno 20.9.2009).

[11] Schneier, B.(2009): Cloud Computing. Dostopno na: http://www.schneier.com/blog/archives/2009/06/cloud_computing.html (objavljeno 4.6.2009).

dostopnost in stanovitnost obratovanja. Pri lastnem izvajanju nas ne skrbi, da bo naša diskovna polja kupil neposredni tekmec, da bi morali čez noč plačati (več) za dostop do svojih podatkov in da bomo podatke morda izgubili, če imamo ustrezne postopke varnostnega kopiranja. Ali – oziroma kdaj – smo pri oblaku lahko v to prepričani? Nikakor ne gre pozabiti tudi na človeški faktor, saj se ljudje kljub jasnim navodilom pogosto poslužujemo različnih bližnjic (npr. posojanje uporabniškega imena). Obstaja seveda tudi druga plat medalje – tako se lahko vprašamo, ali lahko mali upravljavec resnično zagotovi enako raven zavarovanja podatkov kot veliki ponudnik storitev računalništva v oblaku ob upoštevanju virov in ekonomije obsega?

Naročnik mora biti tako sposoben oceniti ali ponujene storitve ustrezajo njegovim in zakonskim zahtevam. Tega ne more storiti brez:

- zadostnih in transparentnih informacij s strani ponudnika,
- analize tveganj, ki jih predstavlja sprejem ponudbe.

Če upravljavec sam ni sposoben pridobiti ali izvesti navedenega, si pri tem lahko pomaga s storitvami tretjih usposobljenih strank ali pa s pomočjo standardizacijskih in certifikacijskih postopkov in potrdil, ki pa se trenutno na področju računalništva v oblaku šele razvijajo. Upravljavci osebnih podatkov pogosto nimajo vseh informacij o tem, kako ponudnik zagotavlja nekatere bistvene elemente zavarovanja osebnih podatkov, kot so sledljivost obdelave, uničevanje podatkov po izpolnitvi namena obdelave ter informacije o dejanskih lokacijah osebnih podatkov. Upravljavci osebnih podatkov v takšnih razmerah težko izvedejo ustrezne analize tveganj pred samo odločitvijo o uporabi teh storitev. **Transparentnost** ponudnikov storitev računalništva v oblaku je zato bistvena – naročnikom mora jasno predstaviti, kje se bodo obdelovali njihovi osebni podatki, kako bo zagotovljena njihova zaupnost, celovitost in razpoložljivost, ali in v katerih tretjih državah se bodo obdelovali, kdaj in kako bodo uničeni po preteku pogodbe, kateri vse podizvajalci in kako bodo sodelovali pri obdelavah podatkov itd.

3.4 IZNOS OSEBNIH PODATKOV V TRETJE DRŽAVE

Posebne težave pri zagotavljanju pričakovane ravni zavarovanja osebnih podatkov porajajo tudi povezana vprašanja izvoza osebnih podatkov v tretje države, ki (ne) zagotavljajo enake ravni varstva osebnih podatkov kot domača jurisdikcija.

O iznosu podatkov v tretje države govorimo takrat, ko upravljavec iz države članice Evropske unije osebne podatke iz takega ali drugačnega razloga **posreduje v države izven Evropske unije**, ali ko je dostop do podatkov omogočen organizacijam, posameznikom, ipd. iz tretjih držav izven EU, pa čeprav so podatki hranjeni znotraj EU (62. člen ZVOP-1).

Iznos osebnih podatkov iz držav članic EU v tretje države, ki ne zagotavljajo ustrezne ravni varstva osebnih podatkov, je možen le pod določenimi pogoji, ki jih ZVOP-1 ureja v 2. poglavju (členi 63.-71.). Pred iznosom podatkov mora upravljavec običajno pridobiti dovoljenje Informacijskega pooblaščenca.

3.4.1 Prenos v <u>državo</u>, ki zagotavlja ustrezno raven varstva osebnih podatkov (ang. »adequacy«)

Upravljavec lahko osebne podatke, po tem, ko je dobil dovoljenje Pooblaščenca, posreduje v tretjo državo, kadar **<u>država kot taka</u> zagotavlja ustrezno raven varstva osebnih podatkov** – pri odločanju je Pooblaščenec vezan na odločitve Evropske komisije, ki je za naslednje države že ugotovila, da zagotavljajo ustrezno raven varstva osebnih podatkov: Andora, Argentina, Avstralija, Kanada, Švica, Ferski otoki, Guernsey, Izrael, Isle of

man, Jersey, ZDA (samo v določenem delu: varni pristan in podatki potnikov)[12]. V tem primeru po prejemu vloge Pooblaščenec upravljavcu izda dovoljenje po hitrem postopku in državo umesti na svoj seznam iz 66. člena ZVOP-1. Če države ni na seznamu Evropske komisije, Pooblaščenec izvede postopek ugotavljanja sam.

3.4.2 Prenos organizaciji, ki zagotavlja ustrezno raven varstva osebnih podatkov (SPK in BCR)

Upravljavec lahko osebne podatke, po tem, ko je dobil dovoljenje Pooblaščenca, posreduje v tretjo državo kadar **upravljavec in točno določena organizacija, ki ji bodo podatki posredovani, zagotavljata ustrezno raven varstva osebnih podatkov, predvsem z določili v pogodbi, ipd.** Upravljavcem so na voljo naslednji instrumenti:

1. tipske pogodbe, ki jih je pripravila Evropska komisija – standardne pogodbene klavzule (SPK),
2. multi-nacionalna podjetja se lahko k ustrezni ravni varstva osebnih podatkov zavežejo tudi z zavezujočimi poslovnimi pravili (ang. »Binding Corporate Rules – BCR«), oziroma sestavijo
3. drugo pogodbo ali pogoje poslovanja, ki zadosti pogojem ustreznega varstva osebnih podatkov.

Najpogostejše izmed navedenih orodij so **standardne pogodbene klavzule**, ki veljajo za takšne, da zagotavljajo primerne zaščitne ukrepe glede varstva zasebnosti in hkrati zadostijo tudi vsem zahtevam iz 11. člena ZVOP-1, saj štejejo kot pisna pogodba med upravljavcem osebnih podatkov in pogodbenim obdelovalcem, iz katere so razvidne medsebojne pravice in obveznosti, poleg tega pa skupaj z obema dodatkoma vsebujejo tudi dogovor o postopkih in ukrepih za zavarovanje osebnih podatkov iz 24. člena ZVOP-1. Prvi model SPK je namenjen prenosu podatkov od upravljavca k pogodbenemu obdelovalcu v tretji državi[13], drugi model SPK pa je namenjen prenosu podatkov od upravljavca k drugemu upravljavcu v tretji državi[14], ki ne zagotavlja ustrezne ravni varstva osebnih podatkov. V SPK je urejena tudi podobdelava, kar pomeni, da pogodbeni obdelovalec lahko zaupa podatke v podobdelavo naslednjemu obdelovalcu, vendar je za njegova dejanja odgovoren ter mora o tem seznaniti upravljavca[15].

Vse bolj v porastu je tudi uporaba **zavezujočih poslovnih pravil** (ang. »Binding Corporate Rules – BCR«), ki so interni akt multi-nacionalne korporacije – skupine podjetij, od katerih so določena podjetja morda locirana zunaj EU, v tretjih državah, ki ne zagotavljajo ustreznega varstva osebnih podatkov. V internem aktu je definirana politika korporacije glede iznosa podatkov v tretje države – skladno z zahtevami Direktive o varstvu osebnih podatkov glede iznosa osebnih podatkov v tretje države. Ko so BCR sprejete s strani nadzornih organov v EU, se šteje, da zagotavljajo ustrezno raven varstva za posredovanje podatkov znotraj skupine podjetij/korporacije, ki so se zavezala k spoštovanju BCR. **Na podlagi BCR ni mogoč prenos podatkov podjetjem zunaj korporacije.** Namen BCR je, da je v korporaciji, ki ima lahko člane tudi izven EU, torej v tretjih državah, prost pretok osebnih podatkov in da ni potrebno za vsak iznos podatkov v tretje države posebno dovoljenje nadzornega organa. BCR mora sprejeti nadzorni organ (kot je opisano zgoraj), potem pa korporacija na podlagi sprejetih BCR zaprosi za dovoljenje za iznos podatkov. Velja opozorilo, da je prenos podatkov na

[12] Spisek je dostopen preko http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

[13] Model standardnih pogodbenih klavzul in oba dodatka iz Sklepa Komisije z dne 5. februarja 2010 o standardnih pogodbenih klavzulah za prenos osebnih podatkov obdelovalcem s sedežem v tretjih državah v skladu z Direktivo 95/46/ES (notificirana pod dokumentarno številko C(2010) 593) (2010/87/ES) je dostopen na tej povezavi: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:SL:PDF.

[14] Model standardnih pogodbenih klavzul in oba dodatka iz Sklepa Komisije z dne 27. decembra 2004 o spremembi Odločbe 2001/479/ES glede uvedbe alternativnega sklopa standardnih pogodbenih klavzul za prenos osebnih podatkov v tretje države (Notificirana pod dokumentarno številko K(2004) 5271 je dostopen na tej povezavi: https://www.ip-rs.si/fileadmin/user_upload/Pdf/Contractual_clauses_slo.pdf.

[15] Podrobneje v Smernicah Pooblaščenca o iznosu podatkov v tretje države: https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/.

podlagi BCR mogoč le znotraj skupine korporacije. Če bi želela korporacija podatke iznašati zunanjemu obdelovalcu v tretji državi, bi morala imeti zato pravno podlago (npr. sklenjene standardne pogodbene klavzule) ter pridobiti posebno dovoljenje nadzornega organa.

*Nov mehanizem, trenutno v razvoju, ki naj bi bil posebej primeren za ponudnike računalništva v oblaku, so **Zavezujoča poslovna pravila za pogodbene obdelovalce (ang. »BCR for processors«)**. Tako bi lahko ponudnik oblaka z internim aktom poskrbel za varstvo osebnih podatkov, skladno z zahtevami evropske zakonodaje.

Iznos brez dovoljenja Pooblaščenca

1. Dovoljenje Pooblaščenca ni potrebno, če je tretja država na seznamu tistih držav iz 66. člena ZVOP-1, za katere je že ugotovljeno, da v celoti zagotavljajo ustrezno raven varstva osebnih podatkov, ali pa le to zagotavljajo delno, če se posredujejo tisti osebni podatki in za tiste namene, za katere je ugotovljena ustrezna raven varstva: **Švicarska konfederacija, Hrvaška, ZDA, Makedonija v delu ko gre za organizacije, zavezane načelom varnega pristana.**[16]

2. Dovoljenje prav tako ni potrebno, kadar gre za katero od situacij iz 70(1). člena ZVOP-1, za katere pa velja, da se uporabljajo izjemoma – torej ne za masovne in pogoste iznose. Dovoljenje Informacijskega pooblaščenca za iznos podatkov tako ni potrebno, kadar:
   - tako določa drug zakon ali obvezujoča mednarodna pogodba;
   - je podana osebna privolitev posameznika, na katerega se nanašajo osebni podatki in je seznanjen s posledicami takšnega posredovanja;
   - je iznos potreben za izpolnitev pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem osebnih podatkov ali za izvršitev predpogodbenih ukrepov, sprejetih kot odgovor na zahtevo posameznika, na katerega se nanašajo osebni podatki;
   - je iznos potreben za sklenitev ali izvršitev pogodbe, ki je v korist posameznika, na katerega se nanašajo osebni podatki, sklenjeno med upravljavcem osebnih podatkov in tretjo stranko;
   - je iznos potreben, da se pred hujšim ogrožanjem zavaruje življenje ali telo posameznika, na katerega se nanašajo osebni podatki;
   - se iznos opravi iz registrov, javnih knjig ali uradnih evidenc, ki so po zakonu namenjene zagotavljanju informacij javnosti in so na voljo za vpogled javnosti na splošno ali katerikoli osebi, ki lahko izkaže pravni interes, da so v posameznem primeru izpolnjeni pogoji, ki jih za vpogled določa zakon 70(1). člen ZVOP-1.

3.4.3 Iznos v ZDA na podlagi zaveze varnemu pristanu

Med države, pri katerih je ugotovljeno delno ustrezno varstvo osebnih podatkov, na podlagi odločbe Pooblaščenca sodijo tudi ZDA, vendar le za tiste organizacije, ki so se zavezale dogovoru Varni pristan (angl. »Safe Harbor«). Evropski režim varstva osebnih podatkov se namreč precej razlikuje od režima ZDA, od koder prihaja nekaj največjih ponudnikov javnega računalništva v oblaku. Nekateri medsebojni dogovori, kot je dogovor Varni pristan pa naj bi omogočili lažjo izmenjavo podatkov med tema različnima režimoma. Varni pristan omogoča upravljavcem osebnih podatkov, da svoje podatke posredujejo upravljavcem ali pogodbenim obdelovalcem iz ZDA (kot so npr. Google, Amazon ipd.), če so se ta podjetja zavezala k spoštovanju načel

[16] Seznam je dostopen na spletni strani Pooblaščenca: https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/iznos-osebnih-podatkov-v-tretje-drzave/seznam-tretjih-drzav-66-clen-zvop-1/.

Varnega pristana[17]. Organizacija iz ZDA se za pridobitev ugodnosti Varnega pristana samocertificira pri Ministrstvu za trgovino ZDA, kar pomeni, da se zaveže k spoštovanju načel Varnega pristana in to tudi javno razglasi v svojih politikah varnosti podatkov. Seznam organizacij, ki so se zavezale, da bodo osebne podatke obdelovale v skladu z načeli je objavljen na spletni strani Ministrstva za trgovino ZDA: www.export.gov/safeharbor/.

Informacijski pooblaščenec je glede dogovora Varni pristan odločil[18], da Združene države Amerike zagotavljajo ustrezno raven varstva osebnih podatkov v delu, ko gre za iznos osebnih podatkov organizacijam, ki delujejo po načelih varnega pristana, uveljavljenih v skladu z najpogosteje zastavljenimi vprašanji – FAQ, ki jih je 21. julija 2000 izdalo Ministrstvo za trgovino ZDA. V primeru iznosa podatkov v ZDA se namreč po odločbi Evropske Komisije 2000/520/ES zavezanost organizacije načelom Varni pristan šteje kot zagotovilo, da organizacija ustrezno varuje osebne podatke.

To posledično pomeni, da za iznos osebnih podatkov organizacijam, ki delujejo **po načelih Varnega pristana, posebna odločba Informacijskega pooblaščenca ni potrebna**, vendar pa Pooblaščenec v zvezi z dogovorom Varni pristan opozarja, da članstvo v omenjenem dogovoru sicer predstavlja enega od pogojev, pod katerimi je tudi brez odločbe Pooblaščenca dopusten iznos osebnih podatkov v tretje države, a morata tako upravljavec osebnih podatkov kot njegovi pogodbeni obdelovalci osebnih podatkov zagotoviti spoštovanje določbe prvega odstavka 25. člena ZVOP-1, po katerem so **upravljavci osebnih podatkov in pogodbeni obdelovalci dolžni zagotoviti zavarovanje osebnih podatkov na način iz 24. člena tega zakona.** V zvezi s tem trčimo na odprta vprašanja v povezavi z zavarovanjem osebnih podatkov pri iznosu osebnih podatkov v (zlasti) javne oblike računalništva v oblaku in ustreznosti zagotovil, ki naj bi jih nudil dogovor Varni pristan. **Pooblaščenec je mnenja, da če upravljavec in pogodbeni obdelovalec osebnih podatkov ne moreta izpolniti zahtev, ki jih glede zavarovanja osebnih podatkov zahteva 24. člen ZVOP-1, ima upravljavec s pridobitvijo odločbe sicer pravno podlago za iznos osebnih podatkov, lahko pa s samim iznosom osebnih podatkov pride do kršitve določb 24. člena ZVOP-1.**

Pooblaščenec posebej opozarja, da glede na trenutno stanje marsikateri ponudnik storitev računalništva v oblaku po oceni Pooblaščenca ne zagotavlja vseh postopkov in ukrepov, ki jih opredeljuje 24. člen ZVOP-1, kljub temu, da velja na njihovi strani prepričanje, da z vključenostjo v Varni pristan to zagotavljajo.

Upravljavci, ki nameravajo uporabiti storitve računalništva v oblaku, morajo torej biti posebej pozorni na naslednje dolžnosti po ZVOP-1:

- pogodbena obdelava osebnih podatkov (11. člen),
- zavarovanje osebnih podatkov (24., 25. člen),
- iznos osebnih podatkov v tretje države (63.-71. člen).

[17] Več podrobnosti o dogovoru Varni pristan najdete na spletni strani Pooblaščenca: https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/iznos-osebnih-podatkov-v-tretje-drzave/safe-harbor/

[18] Odločba št. 0601-2/2010/5.

Računalništvo v oblaku prinaša s seboj določna specifična tveganja, ki niso značilna za »običajno« zunanje izvajanje storitev oziroma (v terminologiji ZVOP-1) pogodbeno obdelavo osebnih podatkov. Tovrstna tveganja zelo dobro obravnava poročilo ENISA, omenimo pa lahko naslednja:

- *neenakomerne pogajalske moči (ponudnik-uporabnik),*
- *netransparentnost ponudnikov,*
- *zamegljena lokacija podatkov,*
- *razkritje podatkov organom pregona, industrijska špionaža,*
- *problem« multi-tenancy« (sobivanje naročnikov na isti opremi),*
- *zmanjšana prenosljivost podatkov,*
- *neustrezna raven medsebojne izolacije souporabnikov virov,*
- *nezmožnost preverjanja izvajanja politik varovanja podatkov,*
- *nezadostno, nepopolno ali neučinkovito brisanje podatkov,*
- *nerazumevanje prenosa odgovornosti na ponudnika,*
- *zmanjšanje vpliva na upravljanje,*
- *odpoved storitve ali prenehanje ponudnika,*
- *prevzem ponudnika skupaj s podatki,*
- *zloraba posebnih (najvišjih) pooblastil,*
- *zloraba vmesnika za upravljanje storitve,*
- *razkritje podatkov med njihovim prenosom,*
- *odtekanje podatkov pri nalaganju/snemanju ali znotraj oblaka,*
- *razkritje ali izguba šifrirnih ključev ter*
- *neskladnost pri zaščiti podatkov pri ponudniku in odjemalcu (običajno nezadostna zaščita pri odjemalcu).*

4. KONTROLNI SEZNAM ZA PREVERJANJE SKLADNOSTI

Kot smo uvodoma pojasnili, je namen pričujočih smernic **dvigniti stopnjo ozaveščenosti predvsem o tveganjih, ki jih prinaša obdelava osebnih podatkov v oblaku** ter ponuditi kontrolni seznam za lažje ugotavljanje skladnosti z obstoječimi zahtevami zakona o varstvu osebnih podatkov.

Kako uporabljati kontrolni seznam?
Določene kontrole mora izpolniti naročnik (oznaka »N«), določene ponudnik (oznaka »P«), pri nekaterih pa morata zahtevam kontrole zadostiti oba (gre torej za odgovornost oziroma dolžnost). Kontrolni seznam predstavlja niz **obveznih kontrol, ki predstavljajo minimalne zahteve brez izpolnitve katerih odsvetujemo odločitev za uporabo storitev računalništva v oblaku**. Pri vsaki kontroli je v stolpcu z opombami dodan podrobnejši opis kontrole. Za podrobnejše presoje ustreznosti ponujenih storitev, izvedbo ocen tveganja in ostale metodološke pripomočke, pa priporočamo uporabo virov in referenc, ki so navedeni v zadnjem poglavju.

Kako <u>NE</u> uporabljati kontrolnega seznama?

- Kontrolni seznam se osredotoča na zahteve, ki so specifične za varstvo osebnih podatkov v oblaku. Izpolnitev kontrolnega seznama še ne pomeni, da ste s tem izpolnili tudi ostale obveznosti po ZVOP-1 (npr. imenovanje odgovornih oseb za zbirke osebnih podatkov, upoštevanje načela roka hrambe itd.).
- Kontrolni seznam je namenjen tako naročniku kot ponudniku storitev računalništva v oblaku – ni primerno, da naročnik zgolj posreduje kontrolni seznam v izpolnitev (potencialnemu) ponudniku.
- Praktičnih primerov in pojasnil ne interpretirajte kot dokončnih in ne posplošujte dejanskega stanja na vse situacije.

Zap.št.	Kontrolna točka	DA	NE	N	P	Smernice za izpolnitev	Zakonska referenca
Obdelava osebnih podatkov - splošno							
1	Naročnik razpolaga s pravno podlago za obdelavo osebnih podatkov.	☐	☐	x		Naročnik mora razpolagati s pravno podlago (npr. privolitev posameznika ali podlaga v zakonu) za obdelavo osebnih podatkov, da sploh lahko obdeluje in posreduje osebne podatke (še preden se torej odloči za uporabo storitev računalništva v oblaku). Pravne podlage, kot so npr. privolitev posameznika ali podlaga v zakonu, opredeljujejo 8., 9., 10. člen ZVOP-1.	8., 9., 10. člen ZVOP-1
2	Naročnik ve, katere kategorije osebnih podatkov bo iznašal v oblak.	☐	☐	x	x	Naročnik mora v vsakem trenutku vedeti, katere kategorije osebnih podatkov iznaša v oblak; to lahko predstavlja katalog zbirke osebnih podatkov, podatkovni model. Naročnik mora od ponudnika pridobiti natančne informacije o tem, katere kategorije osebnih podatkov zbira oziroma dalje obdeluje njegov informacijski sistem (velja predvsem za model SaaS - Programska oprema kot storitev), kjer bi se naročnik lahko šele z uporabo rešitve seznanil s tem, da bo prišlo do obdelave določenih kategorij osebnih podatkov).	
3	Ponudnik ustreza vsem pogojem uporabe storitve, ki jih je postavil naročnik.	☐	☐	x	x	Smernico lahko izpolnijo tudi tipske pogodbe in splošni pogoji, če ustrezajo vsem zahtevam naročnika. Upoštevati je treba tudi možnost, da ponudnik sicer ne omogoča prilagajanja, da pa izpolnjuje vse pogoje (tako naročnika kot npr. zakonske). Naročnik mora biti pozoren na pogodbena določila glede možnosti spreminjanja pogojev tekom obdelave podatkov s strani ponudnika in	2. odst. 11. člena ZVOP-1 (obdelava samo v okviru naročnikovih pooblastil)

Zap.št.	Kontrolna točka	DA	NE	N	P	Smernice za izpolnitev	Zakonska referenca
						mora biti pripravljen na morebitno potrebo po zamenjavi ponudnika. Naročnik mora biti o spremembah vnaprej obveščen, da lahko, če se z njimi ne strinja, prekine sodelovanje s ponudnikom.	
Pogodbena obdelava osebnih podatkov							
4	S ponudnikom računalništva v oblaku smo sklenili pisno pogodbo.	☐	☐	x	x	Pogodba je lahko sklenjena tudi v elektronski obliki, ki je zakonsko dopustna in enakovredna pisni (npr. ZEPEP). Pogodba naj vsebuje priporočene varovalke (glej mnenje Delovne skupine iz člena 29).	2. odst. 11. člena ZVOP-1
5	Pisna pogodba s ponudnikom računalništva v oblaku vključuje konkretiziran dogovor o postopkih in ukrepih za zavarovanje osebnih podatkov.	☐	☐	x	x	Dogovor o zavarovanju je lahko sestavni del pogodbe oz. splošnih pogojev, ali pa drug dokument, priložen pogodbi (npr. aneks) ali sklic na obstoječe pravilnike in druge dokumente, ki to opredeljujejo (varnostne politike ipd.) Zgolj sklic na določen člen zakona ne izpolnjuje kontrolne točke. Konkretiziran dogovor pomeni, da so postopki in ukrepi natančno opisani, npr.: varnostna služba, protivirusni sistem, protipožarni sistemi. Opozorilo: ponudnik iz tretje države mora spoštovati določbe ZVOP-1 o postopkih in	2. odst. 11. člena ZVOP-1

Zap.št.	Kontrolna točka	DA	NE	N	P	Smernice za izpolnitev	Zakonska referenca
						ukrepih za zavarovanje osebnih podatkov, posebej opozarjamo na zahtevo po sledljivosti obdelave osebnih podatkov[19].	
6	V pogodbi s ponudnikom računalništva v oblaku je opredeljeno, katere obdelave osebnih podatkov izvaja ponudnik in kakšna so njegova pooblastila.	☐	☐	x	x	Pogodba (oz. ustrezni pripadajoči dokument kot sestavni del pogodbe) med naročnikom in ponudnikom mora jasno navajati, kakšno obdelavo osebnih podatkov *sme* oz.*mora* izvajati ponudnik – obseg pooblastil, ki jih naročnik predaja ponudniku storitev mora biti jasno opisan. Življenjski cikel zagotavlja varnost podatkov od zajema, uporabe do uničenja in ima definirane in dokumentirane postopke in procese. Primer: Naročnik mora vedeti, ali ponudnik izdeluje (tudi) varnostne kopije. V nekaterih primerih je pomembno opredeliti tudi, česa NE SME izvajati ponudnik (npr. izdelovati kopij podatkov za lastne namene).	2. odst. 11. člena ZVOP-1
7	Naročnik mora biti v vsakem trenutku seznanjen z vsemi podizvajalci, ki v imenu in za račun ponudnika izvajajo obdelavo osebnih podatkov naročnika ter katere obdelave	☐	☐	x	x	Smernica je izpolnjena npr. na način, da ponudnik svojim naročnikom zagotavlja ažuren in dostopen seznam vseh svojih podizvajalcev z opisom storitev, ki jih ti opravljajo za	8. člen ZVOP-1

[19] Sledljivost obdelave osebnih podatkov pomeni, da je mogoče poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil.

Zap.št.	Kontrolna točka	DA	NE	N	P	Smernice za izpolnitev	Zakonska referenca
	izvajajo (načelo transparentnosti). Ponudnik mora naročniku dati razumen rok pred uporabo storitev novega podizvajalca, v katerem se lahko naročnik odloči, da bo odstopil od pogodbe, če se z uporabo storitev novega podizvajalca ne bo strinjal. Prenos osebnih podatkov podizvajalcu, s katerim se naročnik ne strinja, ni dopusten.					ponudnika. Podizvajalci morajo zagotavljati enako raven zavarovanja kot ponudniki – prenos pooblastil s ponudnika na podizvajalca ne sme pomeniti znižanja ravni zavarovanja osebnih podatkov. V primeru, da ponudnik in naročnik ne najdeta skupnega jezika glede določenega podizvajalca, mora ponudnik naročniku omogočiti ustrezen čas pred prekinitvijo pogodbenega razmerja, v katerem lahko k sebi prenese osebne podatke.	
8	Po preteku pogodbe ali na zahtevo naročnika bo ponudnik storitev računalništva v oblaku uničil vse osebne podatke, vključno z morebitnimi kopijami.	☐	☐	x	x	Naročnik mora biti natančno seznanjen, kdaj bodo osebni podatki, ki jih je zaupa ponudniku, dejansko izbrisani in na kakšen način. Ponudniki, ki naročnikom ne znajo resnično in pošteno[20] predstaviti, kdaj in kako bodo podatki dejansko uničeni ne izpolnijo tega pogoja. Naročnik naj se zaveda, da si mora zagotoviti uporabnost podatkov tudi po preteku pogodbene obdelave, zato mora ponudnik naročniku omogočati pridobitev kopije osebnih podatkov v strukturiranemu elektronskemu formatu, ki naročniku omogoča nadaljnjo	21. člen ZVOP-1

[20] Pošteno se nanaša na dolžnost, da se pomembne informacije ne zamolčijo.

Zap.št.	Kontrolna točka	DA	NE	N	P	Smernice za izpolnitev	Zakonska referenca
						obdelavo podatkov. Naročnik se mora zavedati, da k podatkom sodijo tudi dnevniki, ki izkazujejo sledljivost obdelave osebnih podatkov.	
Informacijska varnost (zavarovanje osebnih podatkov) - skladnost in revizija							
9	Pred uporabo storitev računalništva v oblaku je naročnik sam ali s pomočjo zaupanja vredne tretje stranke izvedel analizo tveganja.	☐	☐	x		Pri pripravi analize tveganja naj upravljavci upoštevajo sorazmernost z vidika obsega osebnih podatkov, kategorij osebnih podatkov ter občutljivosti osebnih podatkov, ki se bodo obdelovali v oblaku. (glej praktične primere v posebnih okvirčkih). Priporočamo, da se analize tveganja izvedejo skladno z uveljavljenimi metodologijami, kot npr. ISO/IEC 27005:2008, ENISA Cloud Computing Security Risk Assesment ali drugimi uveljavljenimi standardi.	24. člen ZVOP-1
10	Fizična lokacija osebnih podatkov je znana v vseh fazah obdelave osebnih podatkov.	☐	☐	x	x	Naročnik pozna lokacijo (točen naslov) vseh podatkovnih centrov, kjer bo potekala katerakoli faza obdelave osebnih podatkov, kar velja tudi za lokacije podizvajalcev. Ponudnik mora naročniku podati resnično in pošteno predstavitev vseh informacij o tem, kje in kako bo obdeloval osebne podatke	24. člen ZVOP-1

Zap.št.	Kontrolna točka	DA	NE	N	P	Smernice za izpolnitev	Zakonska referenca
						(naročniku npr. ne sme zamolčati, da v določeni fazi prihaja do iznosa osebnih podatkov v tretje države.) Naročnik lahko o tem zahteva izjavo od ponudnika.	
11	Naročnik ima pogodbeno pravico do revizije informacijskega sistema ponudnika oziroma ponudnik redno izvaja zunanje neodvisne revizije celotnega informacijskega sistema. Ponudnik strankam objavlja rezultate revizij informacijskega sistema in varnostnih pregledov v skladu z zakonodajo in varnostnimi standardi.	☐	☐	x	x	Priporočamo, da ponudnik vsaj enkrat letno izvede zunanji revizijski pregled celotnega informacijskega sistema, ki zajema upravljanje IT, varnost in neprekinjeno poslovanje in pridobi neodvisno mnenje revizorja informacijskih sistemov za vse točke pregleda. Notranja revizija ponudnika ne izpolnjuje te smernice.	2. odst. 11. člena ZVOP-1
12	Ponudnik šifrira osebne podatke, ki se prenašajo v ali znotraj oblaka po nezaščitenih komunikacijskih omrežjih.	☐	☐	x	x	Zaščitena komunikacijska omrežja zagotavljajo zaupnost, avtentičnost in celovitost podatkov. Ne velja za prenos podatkov izven nadzora upravljavca (npr. po internetu), če je med prenosom zagotovljena zaupnost in nespremenljivost podatkov.	24. člen ZVOP-1
13	Naročnik je obveščen o dejanskih incidentih[21] ter o načinih odkrivanja in rokovanja z incidenti, vključno s sredstvi pri ponudniku, ki so načrtovani in opisani v načrtu odziva na	☐	☐	x	x	Incidenti naj se redno beležijo in obravnavajo. Postopki naj bodo vnaprej definirani in naj se redno posodabljajo. Ponudnikov SLA[22] zagotavlja podporo pri rokovanju z incidenti, ki	24. člen ZVOP-1

[21] Bodoča zakonodaja na področju varstva osebnih podatkov bo zelo verjetno zahtevala obveznost obveščanja (prizadetih posameznikov in/ali nadzornih organov) o varnostnih incidentih.
[22] Service Level Agreement – dogovor o ravni storitve.

Zap.št.	Kontrolna točka	DA	NE	N	P	Smernice za izpolnitev	Zakonska referenca
	incidente.					je potrebna za učinkovito izvedbo načrta odziva na incidente za vsako fazo v procesu: - odkrivanje - analiza - obvladovanje - izkoreninjenje - obnovitev Testiranje načrta odziva na incidente naj se izvaja vsaj enkrat letno.	
14	Naročnik mora biti seznanjen s pristopom, ki ga ponudnik uporablja za deljenje virov in s tehničnimi in drugimi ukrepi s katerimi ponudnik naslavlja varnostne vidike večstanovalskosti[23] (angl. multi-tenancy).	☐	☐	x	x	Naročnik mora vedeti, ali ima pri ponudniku zagotovljene svoje fizične vire ali svoje logične vire (s pomočjo virtualizacije), ter ali so njegovi podatki od podatkov drugih stanovalcev samo logično ločeni in shranjeni v skupni podatkovni bazi ali podatkovnih nosilcih ipd. Naročniki naj preverijo, ali sta logično ločevanje in uporaba večstanovalskih sistemov (angl. multi-tenancy) sprejemljiva s strani zakonskih zahtev , ki urejajo njihovo poslovanje. Naročniki naj ocenijo sprejemljivost tveganj, ki jih s sabo prinašajo večstanovalski sistemi (logično ločevanje, superadministratorji, kršitve izolacijeidr.).	24. člen ZVOP-1

[23] Koncept računalniške arhitekture, ki omogoča, da ena instanca programske opreme obdeluje zahteve več uporabnikov oziroma stanovalcev.

15	Ponudnik varuje svojo večstanovalsko infrastrukturo in z načini varovanja seznani naročnika.	☐	☐	x	x	Naročnik naj od ponudnika zahteva opis (ali preverja delovanje) varnostnih kontrol, ki varujejo ponudnikovo večstanovalsko platformo. Med njimi so najpomembnejše: • Načini zagotavljanja ločitve med različnimi stanovalci njegovega informacijskega okolja (npr. ločevanje z omrežje VLAN, procesno /pomnilniško ločevanje virtualnih strojev, aplikativno ločevanje v aplikacijah SaaS, itd.). • Načini zaščite ponudnikove programske opreme večstanovalske platforme pred napadi. • Načini utrjevanja in zagotavljanja odpornosti ponudnikove infrastrukture (npr. hipervizorja, omrežnih naprav, operacijskega sistema, lastne programske opreme) na programske varnostne napake. V to spadajo npr. postopki nameščanja popravkov programske opreme, testiranje in upravljanje sprememb lastne programske opreme ipd. Na podlagi tega naj naročnik oceni dodatna tveganja, ki jim je zaradi večstanovalskosti izpostavljen in potencialno uvede nove/dodatne kontrole.	

Pravice posameznika							
16	Naročnik je preveril, da postopki in infrastruktura ponudnika omogočata enostaven dostop do osebnih podatkov v primeru zahteve posameznika po seznanitvi z lastnimi osebnimi podatki v okviru predpisanih zakonskih rokov.	☐	☐	x	x	Naročnik naj se zaveda, da mora tudi pri uporabi storitev računalništva v oblaku zagotavljati izvrševanja pravice posameznika do seznanitve z lastnimi osebnimi podatki, pri čemer bo verjetno potrebno sodelovanje ponudnika. Postopek in časovni okvir realizacije posameznikove zahteve po seznanitvi z lastnimi osebnimi podatki, ki se obdelujejo v oblaku, naj bo vnaprej predviden in opredeljen.	30.-32. člen ZVOP-1
Iznos osebnih podatkov v tretje države							
17	Naročnik je seznanjen s podatkom, v katere (vse) tretje države se bodo iznašali osebni podatki.	☐	☐	x		Osebni podatki bodo hranjeni in obdelovani izključno v državah EU/EGS oz. osebni podatki se bodo iznašali v tretje države. (izven EU/EGS).	63.-71. člen
18	**Pravne podlage za iznos OP v vsako izmed navedenih tretjih držav**					Naročnik mora imeti v primeru iznosa osebnih podatkov izven EU/EGS eno od možnih pravnih podlag (točke 1 do 7)	
	1. Država, iz katere je ponudnik oblaka, oziroma v kateri bodo (tudi če le za kratek čas) hranjeni podatki, je **na seznamu IP**, v celoti ali delno zagotavlja VOP (Švica Hrvaška, ZDA-varni pristan, Makedonija) - **odločba ni potrebna**	☐	☐	x	x		2. odst. 63. člena

	2. Ponudnik oblaka je zavezan Varnemu pristanu in izpolnjuje vse ostale kontrolne točke (**odločba IP ni potrebna)**.	☐	☐	x	x		3. odstavek 63. člena
	3. Iznos bo opravljen na podlagi ene izmed navedenih izjem (**odločba IP ni potrebna**, tudi če država ne zagotavlja ustrezne ravni varstva OP): — tako določa drug zakon ali obvezujoča mednarodna pogodba; — podana je osebna privolitev posameznika, — iznos je potreben za izpolnitev pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem osebnih podatkov ali za izvršitev predpogodbenih ukrepov, sprejetih kot odgovor na zahtevo posameznika, na katerega se nanašajo osebni podatki; — iznos je potreben za sklenitev ali izvršitev pogodbe, ki je v korist posameznika, na katerega se nanašajo osebni podatki, sklenjeno med upravljavcem osebnih podatkov in tretjo stranko; — iznos je potreben, da se pred hujšim ogrožanjem zavaruje življenje ali telo posameznika, na katerega se nanašajo osebni podatki; — iznos se opravi iz registrov, javnih knjig ali uradnih evidenc, ki so po zakonu namenjene zagotavljanju informacij javnosti in so na voljo za vpogled javnosti na splošno ali katerikoli osebi, ki lahko izkaže pravni interes, da so v posameznem primeru izpolnjeni pogoji, ki jih za vpogled določa zakon	☐	☐	x	x	Samo za iznose, ki niso masovni in pogosti!	1.-6. točka 1. odstavka 70. člena ZVOP-1

	4. Država, v kateri bodo podatki, je **na seznamu Evropske komisije** (**odločba IP je potrebna**!)	☐	☐	x			1. odstavek 63. in 67. člen ZVOP-1
	5. S ponudnikom oblaka, ki mu bomo zaupali OP smo sklenili **standardne pogodbene klavzule** (**odločba IP je potrebna**!)	☐	☐	x	x	Navedite, kateri model: upravljavec-upravljavec/ upravljavec-pogodbeni obdelovalec.	7. točka 1. odstavka 70. člena ZVOP-1
	6. Ponudnik oblaka ima **potrjena Zavezujoča poslovna pravila** - **odločba IP je potrebna**!	☐	☐	x	x		7. točka 1. odstavka 70. člena ZVOP-1
	7. S ponudnikom oblaka smo sklenili **drugo pogodbo, s katero zagotavljamo ustrezno raven varstva OP** (zgled so standardne pogodbene klavzule) **– odločba IP je potrebna**!	☐	☐	x	x		7. točka 1. odstavka 70. člena ZVOP-1

5. PRAKTIČNI PRIMERI

Da bi bile smernice lažje razumljive v tem poglavju podajamo nekaj povsem življenjskih situacij, v katerih se bodo znašli upravljavci osebnih podatkov, ki jih zanima ponudba storitev računalništva v oblaku ter ponudniki teh storitev, ki želijo poslovati skladno z zakonodajo. Na konkretnih primerih je prikazano, kako si pri teh odločitvah pomagati s smernicami.

Primer 1 – malo podjetje in pisarniški programski paket v oblaku

Malo podjetje želi podatke svojih naročnikov na svoje e-novice (fizičnih in pravnih oseb) voditi v oblačni alternativi popularnih pisarniških paketov. S strani ponudnika je dobilo informacijo, da je ponudnik zavezan dogovoru Varni pristan in da je pridobil certifikat SSAE 16 type II ter da tako zagotavlja »zasebnost«. Z uporabo kontrolnega seznama je podjetje ugotovilo, da nima natančnih podatkov o tem, kje se bodo nahajali podatki njihovih naročnikov, ali se bodo iznašali v tretje države (v pogojih uporabe je navedeno, da se bodo podatki hranili v ZDA in v drugih državah, v katerih ima ponudnik svoje zmogljivosti) in kakšna bo sledljivost dostopov do teh podatkov, kdaj bodo popolnoma izbrisani. Pogojev uporabe ni možno spreminjati. Malo podjetje se je zaradi netransparentnosti ponudnika odločilo, da bo preučilo ponudbo drugih ponudnikov in da bo pred končno odločitvijo izvedlo analizo tveganja. Če bi namreč prišlo do izgube ali javne objave osebnih podatkov, bi bilo primarno odgovorno malo podjetje kot upravljavec osebnih podatkov.

Primer 2 – primer upravljavca osebnih podatkov iz javnega sektorja

Osnovna šola bi rada podatke o svojih učencih (vključno z elektronsko redovalnico) hranila in obdelovala pri ponudniku oblačne storitve iz ZDA. Ker osnovna šola spada v javni sektor, mora najprej preveriti, ali ima pravno podlago za obdelavo osebnih podatkov, ki jih želi hraniti v oblaku (da obdelavo podatkov določa zakon). Osnovna šola po uporabi kontrolnika in pregledu ponudbe ugotovi, da ima ponudnik svoje centre, kjer se podatki dejansko hranijo, v ZDA in Indiji. Ponudnik je zavezan načelom Varnega pristana. Prav tako si ponudnik pridržuje pravico, da lahko kadarkoli spremeni pogoje uporabe storitve ali najame nove centre za shranjevanje podatkov, hkrati pa bi bila osnovna šola kljub spremenjenim pogojem po pogodbi zavezana uporabljati storitev še 2 leti. Ponudnik storitve namerava shranjene podatke uporabljati tudi za svoje namene, za izdelavo statistik v šolstvu. Ostale zahteve iz kontrolnika so izpolnjene (npr. glede zavarovanja podatkov, revizije, uporabe certifikatov, itd.). Osnovna šola ugotovi, da ponudba ne ustreza več zahtevam iz kontrolnika, zato se s ponudnikom prične pogajati in na koncu doseže, da ponudnik storitve poleg svoje zavezanosti načelom Varnega pristana ponudi v podpis tudi standardne pogodbene klavzule za prenos podatkov v tretje države. Prav tako pogodba določa, da lahko osnovna šola ob spremembi pogojev ali najemu novega podizvajalca s strani ponudnika takoj in brez posledic odstopi od pogodbe, ponudnik pa ji mora potencialne spremembe sporočiti vnaprej, v takšnem roku, da lahko osnovna šola izbere novega ponudnika in podatke preseli. V pogodbi je tudi jasno zapisano, da ponudnik storitve podatkov NE SME uporabljati za svoje namene, niti za izdelavo statistik. Ker so izpolnjene vse zahteve iz kontrolnika, osnovna šola lahko prične z uporabo storitve v oblaku.

Primer 4 – primer večjega podjetja

Podjetje želi v javni oblak IaaS prenesti informacijsko storitev, ki hrani in obdeluje osebne podatke. Edino odprto vprašanje je še, kako zagotoviti zaščito osebnih podatkov pri prenosu preko zaupanja nevrednih omrežij. Skozi oceno tveganj je podjetje ugotovilo, da se tveganja pojavijo pri prenosu podatkov med podjetjem in ponudnikom javnega oblaka, ter pri internih prenosih znotraj javnega oblaka (prenos virtualnih strojev preko omrežja, replikacija shranjevalnih polj idr.). Podjetje je od vseh potencialnih ponudnikov zahtevalo opis zaščite prenosa znotraj njihovih večstanovalskih sistemov in nato izbralo ponudnika, ki vse interne komunikacije preko zaupanja nevrednih omrežij kriptografsko ščiti v skladu z kriptografsko politiko (algoritmi, dolžina ključev, upravljanja s ključi) podjetja, ter hkrati omogoča vzpostavitev enako ščitene povezave VPN z naročniki. Na zahtevo je ponudnik posredoval svojo varnostno politiko in potrdilo o vključenosti le-te v redne presoje ISO 27001. Izbrani ponudnik je moral naročniku zagotoviti pogodbeno pravico do revizije informacijskega sistema ponudnika oz. zagotoviti, da ponudnik redno izvaja zunanje neodvisne revizije celotnega informacijskega sistema. Poleg tega je podjetje v pogodbi o dogovorjeni ravni storitev (SLA) ponudnika zavezalo k zakonsko ustrezni ravni varovanja osebnih in občutljivih osebnih podatkov. Podjetje je preverilo ali imajo morebiti ponudniki strežnike v tujini (kar pomeni iznos osebnih podatkov v tuje države) in ali je v njihovem primeru iznos zakonsko dopusten.

Primer 5 – primer večjega podjetja

Večje podjetje že ima lasten informacijski sistem. Zaradi uvedbe nove spletne rešitve s potencialom velikega števila uporabnikov se je vodstvo odločilo, da zaradi prilagodljivosti in manjšega začetnega stroška storitev gostuje v oblaku pri zunanjem ponudniku. V podjetju je analiza tveganj že obstajala, vendar so jo morali zaradi uporabe storitev v oblaku temeljito dopolniti. Pri tem so ugotovili, da bo uporaba storitve neposredno vplivala na varnost obstoječega informacijskega sistema, saj nova storitev iz njega bere in vpisuje podatke, med drugim tudi osebne. Pri tem so ugotovili, da podjetje nima usklajenih varnostnih politik in kontrol s ponudnikom storitve v oblaku. Naredili so analizo razkoraka (angl. »gap analysis«) s primerjavo vzpostavljenih kontrol in drugih ukrepov obvladovanja tveganj v podjetju in pri ponudniku. S pogajanji s ponudnikom storitve so dosegli, da bo dodatne kontrole uvedel tudi ponudnik in s tem zagotovili, da se z uporabo storitev v oblaku ne bo zmanjšala raven varnosti osebnih podatkov in da se bo ohranilo ločevanje produkcijskega, testnega in razvojnega okolja. Predvidena rešitev je bila najprej predmet vodstvenega pregleda, pred zasnovo projekta pa se je v nadzor projekta vključila tudi notranje-revizijska služba, ki je s preizkušenim revizorjem informacijskih sistemov sodelovala v vseh fazah projekta (zbiranje zahtev, analiza tveganj, podpis pogodbe, razvoj, testiranje in zagon storitve).

Primer 6 – primer malega podjetja in uporabe oblačne rešitve za upravljanje odnosov s strankami (CRM)

Podjetje želi vpeljati rešitev za upravljanje odnosov s strankami v oblaku. Lokalni ponudnik oblačno storitev izvaja v sodelovanju s ponudnikom iz tujine – podatki so tako hranjeni na različnih lokacijah, predvsem izven EU. Podjetje po pregledu ponudbe ugotovi, da ponudnik NE določa natančnih fizičnih lokacij strežnikov, kjer bi se nahajali podatki. V ponujeni pogodbi tudi ni jasno opredeljeno, kaj se zgodi z osebnimi podatki, če se prekine pogodba. Podjetje ponudnika na to opozori in doseže, da je v novi pogodbi jasno definirana lokacija infrastrukture in podrobneje opisana varnostna politika. V pogodbi je tudi jasno definirano ravnanje z osebnimi podatki za primer odpovedi pogodbe, kjer se ponudnik zaveže, da bo fizično uničil vse podatke, vključno z vsemi varnostnimi kopijami in to v vnaprej določenem času od prekinitve pogodbe. Lokalni ponudnik prav tako izpolnjuje ostale zahteve iz kontrolnika, predvsem glede iznosa podatkov v države izven EU na strežnike tujega partnerja lokalnega ponudnika.

Primer 7 – vidik lokalnega ponudnika računalništva v oblaku

Ponudnik storitve v oblaku (pisarniški programski paketi in orodja za spletno komunikacijo) je lokalno podjetje, ki najema podatkovne centre v Braziliji, Mehiki in Indiji. Na slovenskem trgu želi ponuditi svoje storitve manjšim podjetjem. Ponudnik nudi svojim strankam tipsko pogodbo, v kateri navaja, da si pridržuje pravico do tega, da kadarkoli najame nove podizvajalce v ali izven EU in uporabniku ne ponuja dostopa do seznama svojih podizvajalcev. Pogodba ne vsebuje določb o načinih odkrivanja in rokovanja z incidenti, vključno s sredstvi pri ponudniku, ki so načrtovani in opisani v načrtu odziva na incidente. Glede konkretizacije postopkov in ukrepov za zavarovanje osebnih podatkov pogodbe vsebuje zgolj sklic na določen člen zakona. Glede načinov varovanja svoje večstanovalske infrastrukture pogodbe ne vsebujejo nobenih informacij. Ponudnik s pomočjo kontrolnega seznama pravočasno ugotovi, katere so minimalne zahteve zakonodaje in svojo prakso prilagodi v smeri večje transparentnosti do svojih strank. Prav tako ugotovi, da je kot ponudnik odgovoren za ustrezno zavarovanje osebnih podatkov, ki jih hrani za svoje stranke in da je lahko v primeru neustreznega zavarovanja v okviru inšpekcijskega in prekrškovnega postopka spoznan za odgovornega, s čimer mu grozijo tudi globe.

6. ZAKLJUČEK

Glede na navedeno Informacijski pooblaščenec upravljavcem osebnih podatkov priporoča, da pred odločitvijo o iznosu osebnih podatkov v »oblak« izvedejo **temeljite analize tveganj** in da zlasti občutljivih osebnih podatkov, kot so zdravstveni podatki, in vseh ostalih osebnih podatkov z višjo stopnjo tveganja, do uveljavitve trdnih varovalk ne prenašajo v oblak. Ne gre namreč pozabiti, da je upravljavec osebnih podatkov primarno tisti, ki nosi odgovornost za zlorabe osebnih podatkov, zato mora biti trdno prepričan, da tudi njegovi pogodbeni obdelovalci oziroma ponudniki storitev in rešitev, ki jih uporablja, lahko ponudijo takšna zagotovila. Pooblaščenec posebej glede ponudnikov storitev iz ZDA opozarja, da dopustnost iznosa osebnih podatkov v tretje države ponudniku, ki je sprejel zaveze dogovora Varni pristan, še ne pomeni, da ta izpolnjuje vse zahteve glede zavarovanja osebnih podatkov in ureditve pogodbene obdelave osebnih podatkov, kot to zahteva ZVOP-1. Ponudnik kakršne koli storitve, ki naročniku ne zmore ponuditi zadovoljivih odgovorov in zagotovil glede tega, kako bodo zavarovani njegovi podatki, bi moral pri naročniku, ki zna pravilno oceniti tveganja v povezavi s svojimi podatki, vzbuditi določeno mero previdnosti in zadržanosti. Naročnik oziroma upravljavec osebnih podatkov je kot rečeno tisti, ki mora izvesti analizo tveganja in sprejeti odločitev, ali bo zaupal določenemu ponudniku ali ne in tisti, ki je za obdelavo podatkov odgovoren.

Pooblaščenec zaključno podaja še **splošna priporočila glede računalništva v oblaku**. Pooblaščenec je mnenja, da:

- so potenciali računalništva v oblaku izjemni, vendar pa zaradi tega ne sme priti do nižanja ravni varstva osebnih podatkov kot temeljne človekove pravice;
- morajo biti vloženi nadaljnji napori v raziskave, standardizacijske in certifikacijske sheme in prilagoditve zakonodajnega in regulativnega okvira za dvig stopnje zaupanja v storitve računalništva v oblaku;
- morajo upravljavci osebnih podatkov pred uporabo storitev računalništva v oblaku izvajati potrebne analize tveganja in presoje vplivov na zasebnost, po potrebi s pomočjo zaupanja vrednih tretjih strank;
- morajo ponudniki storitev računalništva v oblaku zagotoviti večjo transparentnost svojih praks, predvsem pa zagotovil s področja informacijske varnosti;
- morajo nadzorni organi na področju varstva osebnih podatkov in zasebnosti nadaljevati z oblikovanjem smernic in ozaveščanjem glede vprašanj varstva osebnih podatkov in zasebnosti.

7. UPORABNI VIRI IN POVEZAVE

- Cloud Computing: Benefits, Risks and Recommendations for Information Security. https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

- CSA Security Guidance v.3, CSA Cloud Controls Matrix, CSA Consensus Assessments Initiative: https://cloudsecurityalliance.org/research/

- Mnenja delovne skupine iz člena 29 (Artice 29 Working Party) http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm

- ENISA Cloud Computing Information Assurance Framework. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework.

- ENISA Security and Resilience in Governmental Clouds. 2011. http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/.

- ENISA Procure Secure: A guide to monitoring of security service levels in cloud contracts: http://www.enisa.europa.eu/activities/application-security/test/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts

- IWGDPT: Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum" - 51st meeting, 23-24 April 2012, Sopot (Poland): http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

- NIST Definition of Cloud Computing - NIST SP 800-145. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

- NIST Cloud Computing Synopsis and Recommendations - NIST SP 800-146. http://csrc.nist.gov/publications/nistpubs/800-146/SP800-146.pdf.

- INDUSTRY RECOMMENDATIONS TO VICE PRESIDENT NEELIE KROES ON THE ORIENTATION OF A EUROPEAN CLOUD COMPUTING STRATEGY - November 2011 http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=7672&utm_campaign=isp&utm_medium=rss&utm_source=newsroom&utm_content=tpa-261