

Smernice glede iznosa osebnih podatkov v tretje države



INFORMACIJSKI
POOBlašČENEC

Namen dokumenta:	Smernice podajajo odgovore na najpogosteje zastavljena vprašanja o iznosu osebnih podatkov v tretje države z vidika zahtev Zakona o varstvu osebnih podatkov: kdaj govorimo o iznosu osebnih podatkov v tretje države, kakšne so pravne podlage, kdaj mora in kako lahko upravljavec pridobi dovoljenje Informacijskega pooblaščenca, kdaj vnaprejšnjega dovoljenja ne potrebuje, zagotavljanje ustrezne ravni varstva osebnih podatkov.
Ciljne javnosti:	Upravljalci osebnih podatkov; posamezniki, katerih podatki se prenašajo v tretje države.
Status:	Javno
Verzija:	1.0
Datum izdaje:	15.4.2012
Avtorji:	Informacijski pooblaščenec
Ključne besede:	Smernice, iznos osebnih podatkov v tretje države, ustrezna raven varstva osebnih podatkov, standardne pogodbene klavzule, BCR, računalništvo v oblaku.

Kazalo vsebine

- 4** O smernicah Informacijskega pooblaščenca
- 4** Uvod
- 5** Splošno o iznosu podatkov v tretje države
- 5** *Kdaj gre za iznos podatkov v tretje države?*
- 6** *Pravne podlage za iznos podatkov v tretje države*
- 6** *Kdaj dovoljenje Informacijskega pooblaščenca ni potrebno?*
- 8** *Kdaj je treba pridobiti dovoljenje Informacijskega pooblaščenca in kako ga pridobimo?*
- 8** Ugotavljanje ustrezne ravni varstva za tretjo državo kot celoto
- 9** Ugotavljanje ustrezne ravni varstva za točno določeno organizacijo
- 10** *Iznos na podlagi standardnih pogodbenih klavzul (SPK)*
- 11** *Iznos na podlagi zavezujočih poslovnih pravil (Binding Corporate Rules)*
- 12** Pogosto zastavljena vprašanja ali situacije in kako v njih ravnati?
- 16** Zaključek



1 O smernicah Informacijskega pooblaščenca

Namen smernic IP je podati praktične in razumljive napotke za posameznike, katerih osebni podatki (OP) se obdelujejo, ter za pravne in druge osebe, ki upravljajo z zbirkami osebnih podatkov glede na določbe Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljevanju ZVOP-I).

Pravno podlago za izdajo smernic Pooblaščenca daje 49. člen ZVOP-I, ki med drugim določa, da Pooblaščenec daje neobvezna mnenja, pojasnila in stališča o vprašanih 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-osebni-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-osebni-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/>



2 Uvod

Upravljalci osebnih podatkov so vse pogosteje soočeni s potrebo, željo ali nujnostjo, da podatke svojih zaposlenih ali strank zaradi tega ali onega razloga zaupajo drugi organizaciji, ki ni nujno v Sloveniji ali v Evropi. Na drugi strani tudi posamezniki vse več posegamo po storitvah ponudnikov, ki ne prihajajo iz Evrope. Najmanjše strežnikov v tretjih državah, ki ponujajo ugodnejše pogoje, uporaba spletnih storitev ponudnikov iz ZDA, multi-nacionalna podjetja, ki delujejo globalno, a želijo centralizirano obdelovati podatke zaposlenih, in to ne v Evropi – vse to so primeri, današnja realnost. V digitaliziranem svetu podatkov ni več treba obdelovati na eni lokaciji, pač pa jih lahko praktično poljubno razpršimo po celem svetu.

Da bi v polni meri izkoristili potenciale elektronske obdelave podatkov in možnosti, ki jih odpira, morajo obstajati varovala za zaščito posameznika pri prenosu podatkov. Evropski pravni okvir, katerega del je Slovenija, zagotavlja relativno visoko raven varovanja posameznikove pravice do varstva osebnih podatkov – izven EU je ta raven različna in marsikje ne dosega evropskih standardov. Zato Direktiva o varstvu osebnih podatkov, v Sloveniji pa Zakon o varstvu osebnih podatkov, predvideva posebne postopke v primerih, ko se osebni podatki posameznikov iz EU prenašajo v tretje države, ki ne zagotavljajo ustrezne ravni varstva osebnih podatkov. **Namen določb o iznosu podatkov v tretje države je zagotavljanje enake ravni varstva osebnih podatkov za podatke, ki se obdelujejo znotraj EU, in tiste, ki so posredovani v tretje države.** V nadaljevanju pojasnujemo ključne določbe zakonodaje, ki jih morajo upoštevati upravljalci osebnih podatkov pri prenosu le teh v tretje države, ter podajamo odgovore na pogosto zastavljena vprašanja.

3 Splošno o iznosu podatkov v tretje države

3.1 Kdaj gre za iznos podatkov v tretje države?

O iznosu podatkov v tretje države govorimo takrat, ko upravljavec iz Slovenije (to je lahko tudi podružnica v Sloveniji) osebne podatke iz takega ali drugačnega razloga **posreduje v države izven Evropske unije (EU) ali Evropskega gospodarskega prostora (EGS)**, ali ko je dostop do podatkov omogočen organizacijam, posameznikom ipd. iz tretjih držav izven EU, pa čeprav so podatki hranjeni znotraj EU. Za prenos osebnih podatkov v države članice Evropske unije in Evropskega gospodarskega prostora namreč velja načelo prostega pretoka osebnih podatkov, saj naj bi vse članice EU zagotavljale enako raven varstva osebnih podatkov, skladno z Direktivo o varstvu osebnih podatkov¹. Zakon o varstvu osebnih podatkov (ZVOP-1) tako v 62. členu določa, da se določbe o iznosu osebnih podatkov v tretje države ne uporabljajo, kadar se posredujejo osebni podatki upravljavcu osebnih podatkov, pogodbenemu obdelovalcu ali uporabniku osebnih podatkov, ki je ustanovljen, ima sedež ali je registriran v državi članici Evropske unije ali Evropskega gospodarskega prostora ali zanj kako drugače velja njen pravni red.



¹ Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov

3.2 Pravne podlage za iznos podatkov v tretje države

Iznos podatkov v tretje države je urejen v 62. do 71. členu ZVOP-1, ki določa, da je iznos podatkov dovoljen, kadar je (1) skladen s tem zakonom in kadar je (2) pri iznosu zagotovljena ustrezna raven varstva osebnih podatkov. Za posredovanje osebnih podatkov upravljavcu osebnih podatkov, pogodbenemu obdelovalcu ali uporabniku osebnih podatkov v tretji državi morata biti torej **hkрати izpolnjena dva pogoja, in sicer:**

PRVI POGOJ: Upravljavec mora imeti pravno podlago, da lahko obdeluje osebne podatke. Pravne podlage so za javni sektor določene v 9. členu ZVOP-1, za zasebni sektor pa v 10. členu ZVOP-1. Pogodbenemu obdelovalcu (pravni ali fizični osebi, ki obdeluje osebne podatke v imenu in na račun upravljavca osebnih podatkov) se lahko osebni podatki posredujejo pod pogoji, določenimi v 11. členu ZVOP-1. To pomeni, da mora imeti upravljavec najprej pravno podlago za (kakršen koli) prenos osebnih podatkov drugi entiteti.

Upravljavec iz javnega sektorja lahko podatke posreduje drugemu, če mu to nalaga zakon, pogodba, sklenjena na pobudo posameznika, če je to nujno za izvrševanje zakonitih pristojnosti, ali pa v redkih primerih na podlagi privolitve posameznika². Upravljavec iz zasebnega sektorja lahko podatke posreduje, če to določa zakon, če ima za posredovanje privolitev posameznika, če to zahteva pogodba, ki jo je sklenil s posameznikom, ali če je posredovanje nujno zaradi zakonitega interesa zasebnega sektorja in ta interes očitno prevlada nad interesom posameznika. Pravna podlaga je lahko tudi pogodba o pogodbeni obdelavi osebnih podatkov – kjer pogodbeni obdelovalec v imenu in za račun upravljavca izvede določeno delo in pri tem obdeluje osebne podatke

Na primeru delodajalčevega posredovanja podatkov svojih zaposlenih zunanjemu računovodskemu servisu (v Sloveniji ali pa v tujini) vidimo, da je treba najprej upoštevati določbo specialnega zakona na tem področju – Zakona o delovnih razmerjih³ – ki določa, da se podatki zaposlenih lahko obdelujejo (torej tudi posredujejo), če je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem (46. člen). Ker je posredovanje podatkov

² 2. odst. 9. člena: Nosilci javnih pooblastil lahko obdelujejo osebne podatke tudi na podlagi osebne privolitve posameznika brez podlage v zakonu, kadar ne gre za izvrševanje njihovih nalog kot nosilcev javnih pooblastil. Zbirke osebnih podatkov, ki nastanejo na tej podlagi, morajo biti ločene od zbirk osebnih podatkov, ki nastanejo na podlagi izvrševanja nalog nosilca javnih pooblastil.

³ Uradni list RS št. 42/2002.

zaposlenih računovodstvu potrebno za obračune plač ipd., v tem primeru delodajalec ima pravno podlago za posredovanje podatkov. Če bi delodajalec želel tretjemu posredovati podatke o svojih strankah, bi za to moral imeti katero od pravnih podlag iz 9. ali 10. člena ZVOP-I in/ali sklenjeno pogodbo o pogodbeni obdelavi osebnih podatkov.

DRUGI POGOJ: Upravitelj mora imeti pravno podlago za prenos podatkov v tretjo državo, glede na pravno podlago pa je odvisno, ali potrebuje za iznos osebnih podatkov dovoljenje Informacijskega pooblaščenca.

3.3 Kdaj dovoljenje Informacijskega pooblaščenca ni potrebno?

Dovoljenje **ni potrebno**:

- če je tretja država na seznamu tistih držav iz 66. člena ZVOP-I, za katere je ugotovljeno, da v celoti zagotavljajo ustrežno raven varstva osebnih podatkov;
- če je tretja država na seznamu tistih držav iz 66. člena ZVOP-I, za katere je ugotovljeno, da delno zagotavljajo ustrežno raven varstva osebnih podatkov, če se posredujejo tisti osebni podatki in za tiste namene, za katere je ugotovljena ustrežna raven varstva.

Katere so te države?

Na spisku držav iz 66. člena ZVOP-I, za katere je Informacijski pooblaščenec že ugotovil, da zagotavljajo ustrežno raven varstva osebnih podatkov so trenutno⁴:

- **Švicarska konfederacija** – v celoti zagotavlja ustrežno raven varstva osebnih podatkov; Odločba št. 071-26/2005-6 (0106) z dne 2. 11.2005.
- **Republika Hrvaška** – v celoti zagotavlja ustrežno raven varstva osebnih podatkov; Odločba št. 0601-1/2009/8 z dne 3.7.2009.
- Združene države Amerike zagotavljajo ustrežno raven varstva osebnih podatkov v delu, ko gre za iznos osebnih podatkov organizacijam, ki delujejo po načelih **Varnega pristanišča (Safe Harbor)**; Odločba št. 0601-2/2010/5 z dne 26.11.2010.
- Makedonija, v celoti zagotavlja ustrežno raven varstva osebnih podatkov; Odločba št. 0601-2/2011, z dne 15. 3.2012

⁴ Spisek držav je dostopen na tej povezavi: <https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/iznos-osebnih-podatkov-v-tretje-drzave/seznam-tretjih-drzav-66-clen-zvop-1/>.

Dovoljenje Informacijskega pooblaščenca za iznos podatkov prav tako ni potrebno, kadar (1. do 6. točka 1. odstavka 70- člena ZVOP-I):

- 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 1. odstavka 70. člena ZVOP-I.

Več o dogovoru Safe Harbor si lahko preberete v posebnem okvirčku.



Neglede na vse našteto, torej takrat, ko ni treba pridobiti odločbe Informacijskega pooblaščenca, mora pa seveda vedno obstajati neka pravna podlaga za iznos. Pooblaščenec tu še posebej opozarja, da kadar iznos poteka na podlagi osebne privolitve posameznika, mora upravljavec posameznika **vneprej seznaniti s posledicami posredovanja**. Šele po tem je privolitev posameznika lahko veljavna.

Iznos podatkov v ZDA na podlagi dogovora »Varni pristan«

Dogovor »Varni pristan« (angl. Safe Harbor) v praksi pomeni, da je organizacija iz Slovenije, ki želi prenesti osebne podatke v organizaciji v ZDA, najprej zavezana nacionalni zakonodaji, da zagotovi, da se podatki obdelujejo pravično in zakonito. Pred prenosom podatkov organizaciji v ZDA, ki se je zavezala spoštovati načela Varne pristana, organizacija iz Slovenije ne potrebuje posebnega dovoljenja Pooblaščenca, saj je ta namreč odločil, da ZDA zagotavljajo ustrezno raven varstva osebnih podatkov v delu, ko gre za iznos osebnih podatkov organizacijam, ki delujejo po načelih Varne pristana, uveljavljenih v skladu z najpogosteje zastavljenimi vprašanji – FAQ, ki jih je 21. julija 2000 izdalo Ministrstvo za trgovino ZDA.

ZDA so torej vključene na seznam tistih držav iz 66. člena ZVOP-I, za katere je ugotovljeno, da delno zagotavljajo ustrezno raven varstva osebnih podatkov. Pooblaščenec poudarja, da navedeno velja zgolj za prenos podatkov organizacijam, ki so se zavezale načelom. Če organizacija v ZDA ni zavezana načelom Varne pristana, potem mora organizacija vseeno pred iznosom podatkov pridobiti dovoljenje Pooblaščenca (razen v primeru zgoraj navedenih izjem iz 1. odstavka 70. člena ZVOP-I).

V primeru iznosa podatkov v ZDA se po odločbi Evropske Komisije 2000/520/ES zavezanost organizacije načelom Varne pristana šteje kot zagotovilo, da organizacija ustrezno varuje osebne podatke. Organizacija iz ZDA se za pridobitev ugodnosti Varne pristana samocertificira pri Ministrstvu za trgovino ZDA, kar pomeni, da se zaveže k spoštovanju načel Varne 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/.

Pooblaščenec opozarja, da vključenost pogodbenega obdelovalca v okvir Varne pristana še ne pomeni, da pri iznosu in obdelavi osebnih podatkov ne bo prišlo do kršitev ZVOP-I, zato upravljavec osebnih podatkov svetuje **posebno previdnost, zlasti pri odločanju o uporabi t.i. storitev računalništva v oblaku**, saj morajo biti upoštewane določbe ZVOP-I glede pogodbene obdelave osebnih podatkov (11. člen), posredovanja osebnih podatkov (22. člen) in določbe glede zavarovanja osebnih podatkov (24. in 25. člen ZVOP-I). **Stališče Pooblaščenca in nekaterih drugih nadzornih organov za varstvo osebnih podatkov je, da (zgolj vključenost v) Safe Harbor za uporabo storitev računalništva v oblaku samo po sebi še ne daje zadostnih zagotovil.**

Kaj določajo načela Varne pristana?

Načela Varne pristana določajo, da mora organizacija posameznike **obvestiti o namenu zbiranja in uporabe njihovih podatkov**. Prav tako mora posameznikom ponuditi **možnost izbire o tem, ali se bodo njihovi osebni podatki razkrili tretji stranki ali se bodo uporabili za namen, ki je različen od tistega, s katerim so bili zbrani**. Prenos podatkov tretjim osebam je tako možen samo ob upoštevanju zgornjih dveh načel. Zavezanost načelom varne pristana tako načeloma ščiti osebne podatke, prenesene v ZDA pred nepooblaščeno uporabo in določa, pod kakšnimi pogoji sme organizacija iz ZDA posredovati osebne podatke tretji osebi.

Kako se preverja spoštovanje načel?

Da organizacija pokaže, da spoštuje načela varne pristana, mora izvajanje načel preverjati ali s samoocenjevanjem ali zunanjim pregledom. Pri samoocenjevanju mora tako preverjanje pokazati, da je objavljena politika organizacije glede zasebnosti osebnih podatkov, prejetih iz EU, točna, celovita, prikazana na vidnem mestu, v celoti izvedena in dostopna. Pokazati mora tudi, da je njena politika zasebnosti v skladu z načeli Varne pristana. Organizacije morajo voditi evidenco o svojem izvajanju prakse zasebnosti Varne pristana in jo v primeru preiskave ali pritožbe zaradi neskladnosti izročiti neodvisnemu organu, ki je pristojen za preiskavo pritožb, ali agenciji, ki je pristojna za obravnavo nepoštenih in goljufivih praks.

Organizacija je ob nespoštovanju načel, h katerim se zaveže, podvržena zakonskim pooblastilom pristojnih organov v ZDA, ki so pooblaščenici za preiskave pritožb v primeru nepoštenih. Nacionalnim nadzornim telesom v državah članicah EU (torej tudi Informacijskemu pooblaščenca v Sloveniji)

pa daje 3. člen Odločbe Komisije 2000/520/ES pooblastilo, da ob ugotovitvi pristojnega organa iz ZDA ali pri utemeljeni podlagi, ki kaže na to, da se kršijo določila Varne pristana, prekinajo prenos podatkov v organizacijo iz ZDA, tako da naslovijo zahtevo po prenehanju prenosa podatkov na organizacijo, ki izvaža podatke. Prekinitev preneha takoj, ko je ugotovljeno, da organizacija iz ZDA zopet spoštuje načela Varne pristana⁵.

3.4 Kdaj je treba pridobiti dovoljenje Informacijskega pooblaščenca in kako ga pridobimo?

Kadar torej ne gre za prenos podatkov v **državo, ki je že na seznamu Pooblaščenca**, organizaciji, ki se je zavezala načelom »**Varni pristan**« ali za prenos na podlagi katere od **izjem iz 70⁶ člena ZVOP-I I**, upravljavec pred iznosom podatkov **potrebuje dovoljenje Pooblaščenca**.

V upravni zadevi lahko upravljavec zahteva, da Pooblaščenec odloči:

- **ali država**, v katero naj bi se podatki iznašali, zagotavlja ustrezno raven varstva osebnih podatkov (1. odstavek 63. člena ZVOP-I), oziroma
- **ali točno določena organizacija v tretji državi** zagotavlja ustrezne ukrepe zavarovanja osebnih podatkov ter temeljnih pravic in svoboščin posameznikov in navede možnosti njihovega uresničevanja ali varstva, predvsem v določbah pogodb ali v splošnih pogojih poslovanja (7. točka 1. odstavka 70. člena ZVOP-I).

Za uvedbo postopka ugotavljanja ustrezne ravni varstva osebnih podatkov mora fizična ali pravna oseba izkazati pravni interes. **Vzorec vloge za iznos osebnih podatkov v tretje države je na voljo na spletni strani Pooblaščenca**⁷. V vlogi mora upravljavec navesti svoje podatke, podatke o uvozniku osebnih podatkov, o načinih obdelave, kategorijah osebnih podatkov, osebah, na katere se nanašajo, ter ostale podatke, ki jih vzorec vloge predvideva. Vlogi je potrebno priložiti vsa navedena dokazila.

⁵ Odločbo komisije s priložo načel varnega pristana in s tem povezanih pogosto zastavljenih vprašanj najdete na naslovu: eur-lex.europa.eu/LexUriServ/LexUriServ.do.

⁶ Osebna privolitve, zakonsko določilo, izpolnitev pogodbe, zavarovanje življenja, prenos iz javnih evidenc.

⁷ Vloga za iznos je dostopna na tej povezavi: https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/Vloga_za_iznos_osebni_podatkov_v_tretje_drzave_Obrazec_IZNOS_doc.

4 Ugotavljanje ustrezne ravni varstva za tretjo državo kot celoto

Upravljavec lahko, kot rečeno, na Pooblaščenca naslovi vlogo, da odloči, ali država, v katero naj bi se podatki iznašali, v celoti ali delno zagotavlja ustrezno raven varstva osebnih podatkov. Pri odločanju je Pooblaščenec vezan na odločitve pristojnega organa EU – Evropske komisije, ki ima na svoji spletni strani objavljen seznam držav, za katere je že ugotovila, da zagotavljajo ustrezno raven varstva osebnih podatkov. Trenutno so na tem seznamu naslednje države: Andora, Argentina, Avstralija, Kanada, Švica, Ferski otoki, Guernsey, Izrael, Isle of man, Jersey, ZDA (samo v določenem delu: Varni pristan in podatki potnikov)⁸. V primeru, da gre za državo, za katero je Evropska komisija že ugotovila, da zagotavlja ustrezno varstvo osebnih podatkov, po prejemu vloge Pooblaščenec upravljavcu izda dovoljenje **po hitrem postopku** in državo umesti na svoj seznam iz 66. člena ZVOP-I. **Ko Pooblaščenec državo umesti na svoj seznam, nadaljnja dovoljenja za iznos podatkov v to državo niso več potrebna.**

V postopku presoje ustreznosti ravni varstva osebnih podatkov v določni državi Pooblaščenec za pridobitev potrebnih podatkov naslovi zahtevo na Ministrstvo za zunanje zadeve – to pa pridobi podatke od pristojnega organa v tretji državi, kot to določa Pravilnik o pridobivanju potrebnih informacij za odločanje o iznosu osebnih podatkov v tretje države (Uradni list RS, št. 79/2005). Informacijski pooblaščenec izda odločbo v 2 mesecih od prejema popolnih informacij.



⁸ Spisek je dostopen preko http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

Podatki, ključni za odločanje, so:

1. ali se izneseni osebni podatki uporabljajo le za namen, za katerega so bili izneseni, ali se namen lahko spremeni le na podlagi dovoljenja upravljavca osebnih podatkov, ki jih je posredoval, ali na podlagi osebne privolitve posameznika, na katerega se osebni podatki nanašajo;
2. ali ima posameznik možnost izvedeti, za kakšen namen so se njegovi osebni podatki uporabljali, komu so bili posredovani ter možnost popravka ali izbrisa netočnih ali neažurnih osebnih podatkov;
3. ali tuj upravljavec izvaja ustrezne organizacijske in tehnične postopke ter ukrepe;
4. ali je določena kontaktna oseba, ki je pooblaščenca podati informacije posamezniku ali državnemu nadzornemu organu o obdelavi osebnih podatkov, ki so bili izneseni;
5. ali lahko tuj uporabnik iznese osebne podatke le pod pogojem, če je pri drugem tujem uporabniku, ki mu bodo posredovani osebni podatki, zagotovljeno ustrezno varstvo osebnih podatkov tudi za tuje državljane;
6. ali je zagotovljeno učinkovito pravno varstvo posameznikom, katerih osebni podatki so bili izneseni.

Pri odločanju o ustrezni ravni varstva osebnih podatkov v tretji državi je Pooblaščenec dolžan ugotoviti vse okoliščine v zvezi z iznosom osebnih podatkov. Predvsem mora upoštevati vrsto osebnih podatkov, namen in trajanje predlagane obdelave, pravno ureditev v državi izvora in v državi prejemnici, vključno z ureditvijo varstva osebnih podatkov tujih državljanov, ter ukrepe zavarovanja osebnih podatkov, ki se v njih uporabljajo (68. člen ZVOP-1). Informacije za odločanje lahko vsebujejo določbe Ustave RS, zakonov in podzakonskih aktov, seznam obvezujočih mednarodnih pogodb s področja varstva osebnih podatkov, ki obvezujejo tretjo državo, besedila strokovnih člankov, izpisov iz strokovnih monografij, vodilnih primerov iz sodne prakse, ustavnosodne prakse ter upravne ali inšpekcijske prakse s področja varstva osebnih podatkov v tretji državi, letnih poročil pristojnega organa tretje države, itd.

5 Ugotavljanje ustrezne ravni varstva za točno določeno organizacijo

Osebni podatki se lahko posredujejo v tretjo državo, ki ne zagotavlja ustrezne ravni varstva osebnih podatkov, tudi, če upravljavec osebnih podatkov zagotovi ustrezne ukrepe zavarovanja osebnih podatkov ter temeljnih pravic in svoboščin posameznikov in navede možnosti njihovega uresničevanja ali varstva, predvsem v določbah pogodb ali v splošnih pogojih poslovanja (7. točka 1. odstavek 70. člena ZVOP-1).

To pomeni, da upravljavec in organizacija iz tretje države (uvoznik podatkov) z določili v pogodbah ali pogojih poslovanja zagotovita varovanje osebnih podatkov za posamezen prenos podatkov.



Upravljavcem so na voljo:

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** (Binding Corporate Rules - BCR), oziroma sestavijo
3. **druge pogodbe ali pogoji poslovanja**, ki zadovoljijo pogoje ustreznega varstva osebnih podatkov.

V tem primeru upravljavec na Pooblaščenca naslovi **vlogo⁹ za izdajo posebne odločbe**, osebne podatke pa sme prenesti šele **po prejemu dovoljenja**. Pooblaščenec o vlogi odloči v 2 mesecih. Upravljavec v vlogi opredeli vrste osebnih podatkov, namen obdelave, posameznike, na katere se podatki nanašajo, uporabnike, čas hrambe. Upravljavec mora prav tako izkazati (1) pravno podlago za obdelavo osebnih podatkov in (2) pravno podlago za prenos podatkov - priložiti mora dokumente, ki so podlaga za iznos (standardne pogodbene klavzule, zavezujoča poslovna pravila, drugo).

Če upravljavec ne uporabi zgoraj navedenih tipskih pogodb ali BCR, pač pa z določili v drugih vrstah pogodb ali pogojev poslovanja zagotavlja ukrepe zavarovanja osebnih podatkov za posamezen prenos podatkov, mora vlogi za izdajo dovoljenja posredovati vse relevantne pogodbe in določila, Pooblaščenec pa nato presodi, ali zagotavljajo ustrezno varstvo osebnih podatkov, v skladu z mnenjem¹⁰ Delovne skupine iz člena 29, št. 12/98. **Postopek presoje je v tem primeru daljši, zato Pooblaščenec priporoča uporabo SPK.**

5.1 Iznos na podlagi standardnih pogodbenih klavzul (SPK)

V pomoč upravljavcem, ki želijo osebne podatke prenesti **točno določeni organizaciji** iz tretje države, ki ne zagotavlja ustreznega varstva osebnih podatkov, je Evropska komisija oblikovala **tipske pogodbe**, ki jih **izpolnita in skleneta upravljavec in uvoznik podatkov**.

Uporabljene standardne pogodbene klavzule veljajo za takšne, ki zagotavljajo primerne zaščitne ukrepe glede varstva zasebnosti ter temeljnih pravic in svoboščin posameznikov in glede uresničevanja ustreznih pravic. Sprejete standardne pogodbene klavzule hkrati zadostijo tudi vsem zahtevam iz 11. člena ZVOP-I, 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-I.

Obstajata dva modela SPK (glede na to, ali podatke posredujete pogodbenemu obdelovalcu, ki dela v vašem imenu in za vaš račun, ali pa drugemu upravljavcu, ⁹ https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/Vloga_za_iznos_osebnih_podatkov_v_tretje_drzave_Obrazec_IZNOS_.doc
¹⁰ Mnenje je dostopno na povezavi: http://ec.europa.eu/justice/policies/privacy/docs/wp-docs/1998/wp12_en.pdf

ki bo podatke uporabljal za svoje namene).

Prvi model SPK je namenjen prenosu podatkov od upravljavca k pogodbenemu obdelovalcu v tretji državi¹¹. V SPK podpisnici določita pogoje zavarovanja, odgovornosti in obveznosti, ki veljajo za obdelavo osebnih podatkov. Leta 2010 je bil model posodobljen, tako da sedaj vsebuje tudi določbo o pod-obdelavi osebnih podatkov, kar pomeni, da pogodbeni obdelovalec v tretji državi **lahko podatke zaupa v pod-obdelavo naslednjemu pogodbenemu obdelovalcu**, vendar mora pod-obdelovalec spoštovati enake standarde varovanja osebnih podatkov kot pogodbeni obdelovalec. **Pogodbeni obdelovalec je odgovoren za aktivnosti pod-obdelovalca, upravljavec pa mora imeti natančen seznam vseh pod-obdelovalcev.** Ključno je, da podpisnika natančno določita ukrepe za zavarovanje osebnih podatkov in izpolnita oba dodatka SPK.

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>.

Drugi model SPK je namenjen prenosu podatkov od upravljavca k drugemu upravljavcu v tretji državi, ki ne zagotavlja ustreznega varstva osebnih podatkov. Enako, kot v prvem modelu, tudi v tem podpisnici določita medsebojne obveznosti in dolžnosti glede varstva osebnih podatkov in predpišeta ukrepe za zavarovanje osebnih podatkov. Ključno je, da podpisnika natančno določita ukrepe za zavarovanje osebnih podatkov in izpolnita tudi dodatek SPK.

Pri takem prenosu podatkov drugi upravljavec dobljenih osebnih podatkov ne bo obdeloval v imenu in za račun prvotnega upravljavca (izvoznika podatkov), pač pa jih bo obdeloval oziroma uporabljal **za svoje lastne namene**. Zato mora imeti za tako obdelavo, za svoj lastni namen, pravno podlago (9. oziroma 10. člen ZVOP-I). V primeru takšnega prenosa podatkov torej zgolj sklenitev SPK ni dovolj – za takšno posredovanje osebnih podatkov mora obstajati tudi ustrezna

¹¹ Pogodbeni obdelovalec lahko obdeluje osebne podatke le v okviru upravljavčevega pooblastila in za noben drug namen.

pravna podlaga, podobno kot to velja za posredovanje osebnih podatkov k upravljavcem znotraj Republike Slovenije oz. Evropske unije.

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 so dostopni na tej povezavi: https://www.ip-rs.si/fileadmin/user_upload/Pdf/Contractual_clauses__slo.pdf.

5. 2 Iznos na podlagi zavezujočih poslovnih pravil (Binding Corporate Rules)

Binding Corporate Rules (BCR) 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. 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 pridobiti posebnega dovoljenja nadzornega organa. BCR mora sprejeti nadzorni organ, potem pa korporacija na podlagi sprejetih BCR zaprosi za dovoljenje za iznos 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 ustrežno 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.** 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.

Postopek sprejema BCR:

- Korporacija se najprej obrne na nacionalni nadzorni organ (v Sloveniji je to Informacijski pooblaščenec) in mu posreduje svoj osnutek BCR ter predlog, da nadzorni organ postane vodilni organ v postopku sprejema BCR (kriteriji, po katerih se korporacija odloči, na kateri organ v kateri državi naj se obrne, so opisani v mnenju WP107, dostopnem na tej povezavi -http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp108_en.pdf).

- Nadzorni organ v sodelovanju s korporacijo uskladi tekst BCR ter ga, ko oceni, da zagotavlja primerno raven varstva osebnih podatkov, pošlje v pregled ostalim nadzornim organom v drugih državah članicah EU. Ko na tekst ni pripomb, se šteje, da BCR zagotavljajo ustrežno raven varstva osebnih podatkov.
- **Korporacija nato zaprosi nadzorne organe iz vseh držav članic, v katerih ima svoja podjetja, za dovoljenje za iznos podatkov na podlagi že avtoriziranih BCR¹².**

V BCR je lahko zajeto vse posredovanje osebnih podatkov, vendar mora biti natančno opredeljeno. Postopek sprejema je enoten (kot je opisano zgoraj).

Vodila za sestavo teksta BCR so dostopna na naslednjih povezavah:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_en.pdf
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp108_en.pdf
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153_en.pdf

V primeru večjih sprememb BCR se mora korporacija znova obrniti na nadzorni organ, saj se šteje, da le tekst BCR, ki ga je nadzorni organ skupaj z nadzornimi organi iz drugih držav članic sprejel, zagotavlja ustrežno varstvo osebnih podatkov.

Če ima organizacija sprejete BCR, mora v Sloveniji za pridobitev dovoljenja za iznos Pooblaščenecu posredovati:

- obrazec WP 133 (standardni obrazec predpisan s strani Delovne skupine iz člena 29, s katerim korporacija prične postopek izbite vodilnega organa) – dostopen na tej povezavi http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2007_en.htm;
- tekst BCR;
- opis iznosa osebnih podatkov, namena iznosa, prejemnikov podatkov – obrazec Informacijskega pooblaščenca, dostopen na <http://www.ip-rs.si/obrazci/varstvo-osebni-podatkov/>.

¹² Podrobneje je postopek opisan v naslednjem mnenju Delovne skupine iz člena 29: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp107_en.pdf.

6 Pogosto zastavljena vprašanja ali situacije in kako v njih ravnati?

6.1 Kaj vse štejeemo za iznos osebnih podatkov v tretje države?

V to kategorijo spada kakršna koli obdelava osebnih podatkov s strani entitete v tretji državi, to je v državi, ki ni članica Evropske unije ali del Evropskega gospodarskega prostora. Obdelava pomeni **kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki**, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje (3. točka 6. člena ZVOP-1). Tako sem spadajo tudi hramba podatkov na strežnikih v državah izven EU, izvajanje analize obiska spletnih strani s pomočjo analitičnih orodij, ki jih ponujajo podjetja izven EU (npr. Google Analytics), shranjevanje podatkov v oblaku izven EU (sem spadajo mnoge aplikacije, ki jih posameznik uporablja na mobilnem telefonu, na računalniku, za urejanje pisarniških poslov, koledarji, poštni strežniki, ipd.). Za iznos v tretje države gre tudi, ko ima entiteta iz tretje države zgolj dostop do podatkov, ki se fizično hranijo v Sloveniji ali EU (npr. tehnična pomoč, svetovanje pri incidentih).



6.2 V katere države lahko prenašamo podatke, ne da bi za to potrebovali dovoljenje Pooblaščenca?

V vse **tiste države izven EU/EGS**, za katere je Pooblaščenec že ugotovil, da v celoti ali delno zagotavljajo ustrezno raven varstva osebnih podatkov. Te države so Švica, Hrvaška, Makedonija in ZDA v delu, ko gre za podpisnike dogovora »Varni pristan«. Seznam držav, za katere je bilo ugotovljeno, da zagotavljajo ustrezno raven varstva osebnih podatkov, vodi tudi Evropska komisija. Na njenem seznamu so Andora, Argentina, Avstralija, Kanada, Švica, Ferski otoki, Guernsey, Izrael, Isle of Man in Jersey. Za iznos osebnih podatkov v države, za katere **je Pooblaščenec ugotovil**, da zagotavljajo ustrezno raven varstva osebnih podatkov in se vodijo na njegovem seznamu, odločba Pooblaščenca ni več potrebna, za iznos osebnih podatkov v države, za katere je ustrezno raven varstva osebnih podatkov ugotovila Evropska komisija in se vodijo na njenem seznamu, pa je odločba Pooblaščenca vseeno potrebna, pri čemer pa Pooblaščenec v primeru takšnih držav izda pozitivno odločbo po skrajšanem postopku, saj je pri odločanju vezan na odločitve Evropske komisije.

6.3 S podjetjem iz Črne Gore podpisujete pogodbo o vzdrževanju baze podatkov. Podatki se fizično ne bodo izvažali, pač pa bodo sodelavci iz Črne Gore za potrebe vzdrževanja dostopali do strežnika v Sloveniji. Ali gre tu za iznos podatkov?

Kljub dejstvu, da bodo sodelavci do strežnika dostopali le za potrebe vzdrževanja in ob tem osebnih podatkov ne bodo odjemali ali jih kopirali in kljub temu, da bodo podatki hranjeni v Sloveniji, se že sam dostop šteje za obdelavo osebnih podatkov – torej tu gre za iznos podatkov v tretje države.

6.4 Podjetje iz Slovenije, katerega materinska družba je v tretji državi, za katero Pooblaščenec še ni ugotovil ustrezne ravni varstva osebnih podatkov, želi prenesti materinski družbi podatke svojih zaposlenih (za namen kadrovskih opravil) in strank. Ali za to potrebuje dovoljenje Pooblaščenca?

Če štejeemo podjetje iz Slovenije za upravljavca (naj bo to podružnica ali samostojna pravna oseba v okviru skupine povezanih družb) mora imeti za posredo vanje podatkov pravno podlago. Ko gre za podatke zaposlenih, lahko v primeru,

da je posredovanje oz. obdelava osebnih podatkov potrebna zaradi uresničevanja pravic in obveznosti iz delovnega razmerja, za pravno podlago štejemo Zakon o delovnih razmerjih. Podatke o strankah podjetje lahko obdeluje, torej tudi posreduje, pod pogojem, da ima za to katero od pravnih podlag iz 10. člena ZVOP-I. Če npr. podjetje podatke strank obdeluje na podlagi njihove privolitve, mora stranke vnaprej seznaniti s tem, komu bodo podatki posredovani – šele potem je privolitev veljavna.

Podjetje lahko podatke o zaposlenih in strankah, ki jih obdeluje v skladu s prejšnjim odstavkom, **brez dovoljenja Pooblaščenca**, posreduje materinski družbi v tretjo državo, pod pogojem da (1. do 6. točka 1. odstavka 70. člena ZVOP-I):

- 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.

Najbolj običajno bi se tak prenos lahko izvršil na podlagi osebne privolitve posameznika, na katerega se nanašajo osebni podatki in je seznanjen s posledicami takšnega posredovanja, ali pa, ker je iznos potreben za izpolnitev pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem osebnih podatkov, sprejetih kot odgovor na zahtevo posameznika oziroma, ker je iznos potreben za sklenitev ali izvršitev pogodbe s tretjo stranko, ki je v korist posameznika.

Če nobeden od zgoraj navedenih pogojev ni izpolnjen, lahko podjetje ma terinski družbi posreduje osebne podatke le kot pogodbenemu obdelovalcu,

pri čemer mora z materinsko družbo skleniti dogovor, v katerem zagotovi ustrezne ukrepe zavarovanja osebnih podatkov ter temeljnih pravic in svoboščin posameznikov in navede možnosti njihovega uresničevanja ali varstva (npr. med-družbeni sporazum, SPK, itd.). V takšnih primerih materinska družba dobljenih osebnih podatkov ne sme uporabljati za svoje lastne potrebe, pač pa jih kot pogodbeni obdelovalec lahko obdeluje le v imenu in za račun slovenskega podjetja.

6.5 Smo družba s poslovalnicami po celotni Evropi. Podatki naših zaposlenih bodo po novem shranjeni na centralnem strežniku na Nizozemskem. Ali potrebujemo dovoljenje Pooblaščenca?

Ker bodo podatki hranjeni na Nizozemskem, torej v okviru EU, tu **ne gre za iznos podatkov v tretje države**. Vsak upravljavec znotraj družbe pa mora vseeno spoštovati nacionalno zakonodajo glede obdelave osebnih podatkov zaposlenih – v Sloveniji je to tudi zakonodaja s področja delovnih razmerij (kot pojasnjeno v prejšnjem odgovoru). V primeru, da centralni strežnik na Nizozemskem ni v lasti slovenskega upravljavca osebnih podatkov, pač pa je v lasti druge pravne osebe, ki bo osebne podatke na njem za slovenskega upravljavca osebnih podatkov hranila kot pogodbeni obdelovalec, mora slovenski upravljavec s takšno pravno osebo skleniti pogodbo iz 11. člena ZVOP-I.

6.6 Naše kadrovske evidence bo obdeloval pogodbeni partner iz ZDA. Kaj je treba storiti?

Najprej je treba preveriti, ali je pogodbeni partner na seznamu organizacij, ki so se zavezale spoštovati načela »Varnega pristana« (www.export.gov/safeharbor/). Če je organizacija na seznamu, dovoljenje Pooblaščenca ni potrebno, kljub temu pa tu **opozarjamo**, da zgolj zavezanost organizacije »Varnemu pristanu« ne zadosti vedno zahtevam ZVOP-I po zavarovanju osebnih podatkov (več si lahko preberete v odgovoru pod točko 6.11).

Preveriti je treba, ali gre za katero izmed situacij iz 1. odstavka 70. člena ZVOP-I, pri kateri dovoljenje Pooblaščenca prav tako ni potrebno (npr. osebna privolitev posameznikov).

Če pogodbeni partner iz ZDA ni zavezan načelom varnega pristana

oziroma je v kaki drugi tretji državi (npr. v Indiji), prav tako pa ne gre za katero izmed zgornjih situacij, potem imate dve možnosti:

1. Na Pooblaščenca lahko naslovite vlogo, da bo presodil, ali celotna država zagotavlja ustrezno raven varstva osebnih podatkov – ta postopek je dolgotrajen, poleg tega pa se lahko v postopku ugotovi, da določena država ne zagotavlja ustrezne ravni varstva osebnih podatkov, zaradi česar takšen postopek za posamezne prenose podatkov običajno ni primeren.
2. Na Pooblaščenca naslovite vlogo za izdajo posebne odločbe na podlagi 70. člena ZVOP-I – vlogi priložite pogodbe, v katerih ste s pogodbenim partnerjem zagotovili varstvo osebnih podatkov in njihovo zavarovanje. Najenostavnejša pot je, da uporabite model standardnih pogodbenih klavzul, dostopnih na: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:SL:PDF> (prenos k pogodbenemu obdelovalcu) https://www.ip-rs.si/fileadmin/user_upload/Pdf/Contractual_clauses__slo.pdf (prenos k drugemu upravljavcu)

6.7 Razmišljamo o tem, da bi najeli prostor za naše podatke na strežnikih v Indiji. Kaj naj storimo?

Indija ni na seznamu držav, ki zagotavljajo ustrezno varstvo osebnih podatkov. Shranjevanje podatkov pa prav tako pomeni obdelavo – torej gre tu za iznos podatkov v tretjo državo.

Preveriti je treba, ali gre za katero izmed situacij iz 1. odstavka 70. člena ZVOP-I, pri kateri dovoljenje Pooblaščenca ni potrebno, v nasprotnem primeru pa:

1. Na Pooblaščenca lahko naslovite vlogo, da bo presodil, ali celotna država zagotavlja ustrezno raven varstva osebnih podatkov – ta postopek je dolgotrajen, poleg tega pa se lahko v postopku ugotovi, da država ne zagotavlja ustrezne ravni varstva osebnih podatkov, zaradi česar takšen postopek za posamezne prenose podatkov običajno ni primeren.
2. Na Pooblaščenca naslovite vlogo za izdajo posebne odločbe na podlagi 70. člena ZVOP-I – vlogi priložite pogodbe, v katerih ste s pogodbenim partnerjem zagotovili varstvo osebnih podatkov in njihovo zavarovanje. Najenostavnejša pot je, da uporabite model standardnih pogodbenih klavzul, dostopnih na: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:SL:PDF> (prenos k pogodbenemu obdelovalcu);

6.8 Smo turistična agencija – za rezervacijo hotela na željo stranke moramo na Kitajsko poslati strankine podatke. Kako to storimo zakonito?

Ena od situacij, pri katerih dovoljenje Pooblaščenca za iznos podatkov ni potrebno, je, kadar je **iznos potreben za izpolnitev pogodbe** med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem osebnih podatkov ali **za izvršitev pred-pogodbenih ukrepov, sprejetih kot odgovor na zahtevo posameznika**, na katerega se nanašajo osebni podatki. V tem primeru torej agencija ne bi mogla izpolniti pogodbe, ki jo ima s stranko, ne da posreduje njene osebne podatke v tretjo državo. Podatke strank bi lahko posredovali tudi na podlagi njihove privolitve, pod pogojem, da bi jih seznanili s posledicami takega posredovanja.

6.9 Klienti nam na podlagi pogodbe zaupajo v hrambo njihove podatke, mi pa bi, namesto na strežnikih v Sloveniji, najeli prostor na strežnikih v Indiji, saj je to ugodneje. Kaj storiti?

Vaše podjetje je pogodbeni obdelovalec, ki v imenu in za račun stranke (upravljavca) hrani njene podatke. **ZVOP-I pogodbenemu obdelovalcu ne dovoljuje, da samovoljno podatke posreduje v obdelavo tretji stranki (upravljavcu strežnika v Indiji)**. V tem primeru mora upravljavec, torej vaša stranka, z upravljavcem strežnika v Indiji skleniti pogodbo o pogodbeni obdelavi osebnih podatkov (kot jo je z vami) ter prenos podatkov izvesti v skladu z zgoraj opisanimi postopki glede iznosa osebnih podatkov (vprašanje št. 6. 7) in če je treba, pridobiti dovoljenje Pooblaščenca.

6.10 Naš pogodbeni partner iz Srbije hrani naše podatke na svojih strežnikih. Ima mrežo svojih partnerjev v Črni Gori in Bosni (pod-obdelava), kjer prav tako hrani podatke, ki so mu zaupani. Naše podatke bi torej zaupal v nadaljnjo pod-obdelavo svojim partnerjem. Ali je to dovoljeno? Kako se zavarujemo?

V opisanem primeru morate s pogodbenim partnerjem podpisati **standardne pogodbene klavzule, ki vsebujejo določilo o pod-obdelavi v tretji državi, ter za dovoljenje zaprositi Pooblaščenca**. Pogodbeni obdelovalec osebnih podatkov v tretji državi lahko posreduje osebne podatke podobdelovalcu v tretji državi, pod naslednjimi pogoji:

1. Upravljavec osebnih podatkov, ki je ustanovljen, ima sedež ali je registriran v Republiki Sloveniji (izvoznik podatkov), mora pred iznosom oz. posredovanjem osebnih podatkov s pogodbenim obdelovalcem osebnih podatkov v tretji državi (uvoznik podatkov) skleniti pisno pogodbo, v katero mora v celoti vključiti standardne pogodbene klavzule.
2. Upravljavec oz. izvoznik osebnih podatkov mora po sklenitvi pogodbe, še pred iznosom osebnih podatkov in posredovanjem le teh pogodbenemu obdelovalcu v tretji državi, pridobiti posebno odločbo Pooblaščenca iz drugega odstavka 70. člena ZVOP-I, ki dovoljuje takšen iznos osebnih podatkov.
3. Pogodbeni obdelovalec v tretji državi lahko zatem po prejemu osebnih podatkov od upravljavca oz. izvoznika podatkov odda izvajanje postopkov obdelave osebnih podatkov podobdelovalcu pod pogoji, ki jih določa klavzula I I. Skladno z navedeno klavzulo mora pogodbeni obdelovalec pred oddajo izvajanja postopkov obdelave pod-obdelovalcu pridobiti predhodno pisno soglasje upravljavca (izvoznika) osebnih podatkov, poleg tega pa mora pogodbeni obdelovalec v tretji državi s pod-obdelovalcem še pred oddajo izvajanja postopkov obdelave, ki se bo izvajala v imenu izvoznika, skleniti pisno pogodbo, ki podobdelovalcu nalaga enake obveznosti, kot jih ima uvoznik podatkov po sprejetih klavzulah. Tej zadevi je lahko zadoščeno, če pod-obdelovalec sopodpiše pogodbo, ki sta jo sklenila upravljavec in pogodbeni obdelovalec osebnih podatkov, oziroma se pod-obdelovalec v pisni pogodbi, ki jo sklene s pogodbenim obdelovalcem, zaveže, da bo izpolnjeval vse obveznosti, ki jih glede varstva osebnih podatkov vsebuje pogodba med upravljavcem in pogodbenim obdelovalcem.
4. Pogodbeni upravljavec mora upravljavcu osebnih podatkov poslati izvod pogodbe o pod-obdelavi, upravljavec osebnih podatkov pa mora voditi seznam takšnih pogodb.

6.11 Kdaj gre za iznos podatkov pri računalništvu v oblaku? Na kaj moramo biti pozorni pri ponudnikih oblčnih storitev iz tretjih držav?

Ena od temeljnih značilnosti (zlasti t.i. javnih oblik) računalništva v oblaku je **odsotnost vezave podatkov na natančno opredeljeno fizično lokacijo**. Do obdelave osebnih podatkov lahko pride v vseh tistih državah, v katerih se osebni podatki hranijo. To pomeni, da gre dejansko za prenos osebnih podatkov v vse države, kjer poteka katerokoli ravnanje z osebnimi podatki. Če med te države spadajo tudi države, ki niso članice Evropske unije ali Evropskega gospodarskega prostora, govorimo o iznosu v tretje države.

Če bi recimo ponudnik storitve računalništva v oblaku, ki je sicer ustanovljen in registriran v ZDA, uporabljal svoje podatkovne centre še v Indiji in v Avstraliji, osebni podatki pa bi se prenašali tudi v te države, bi moral upravljavec v Sloveniji s ponudnikom storitev računalništva v oblaku v ZDA skleniti tako pogodbo, v kateri bi bilo jasno določeno, ali in pod kakšnimi pogoji bo ponudnik storitev računalništva v oblaku podatke zaupal v hrambo (ki je tudi obdelava) svojim pod-obdelovalcem (angl. Sub-processors), kamor lahko prištevamo podatkovne centre v Indiji in Avstraliji. Upravljavec osebnih podatkov v Sloveniji mora imeti na podlagi pogodbe s ponudnikom storitev računalništva v oblaku iz ZDA natančen pregled nad tem, kje se bodo podatki hranili, torej ne zgolj to, da bodo hranjeni v oblaku v ZDA, pač pa tudi, ali bo ponudnik oblaka podatke hranil drugje in kje.

Treba je poudariti, da pogodbe oziroma splošni pogoji uporabe, ki jih običajno pripravijo ponudniki storitev računalništva v oblaku, ne zagotavljajo standardov, ki jih glede take vrste iznosa vzpostavlja ZVOP-I in Direktiva o varstvu osebnih podatkov, zato **Pooblaščenec priporoča, da upravljavec iz Slovenije v tem primeru s ponudnikom storitev računalništva v oblaku iz ZDA sklene standardne pogodbene klavzule, ki vsebujejo tudi dogovore v zvezi s »pod-obdelavo« osebnih podatkov s strani ponudnika oblaka**. Pooblaščenec posebej opozarja, da je sestavni del tovrstnih klavzul (Dodatek 2) tudi konkretiziran dogovor o postopkih in ukrepih za zavarovanje osebnih podatkov, ki mora zagotavljati raven, kot jo zahtevata 24. in 25. člen ZVOP-I. **V tem primeru bi upravljavec moral zaprositi za dovoljenje Pooblaščenca**.

Če upravljavec ne sklene standardnih pogodbenih klavzul, pač pa kakšno drugo obliko pogodbe, in če bo ponudnik storitev računalništva v oblaku podatke hranil tudi v drugih državah, ne samo tam, kjer je registriran, mora biti v pogodbi opredeljeno tudi omenjeno vprašanje pod-obdelave in obveznosti pogodbenega obdelovalca v zvezi s tem.

Pooblaščenec na tem mestu posebej opozarja na ponudnike oblaka iz ZDA, ki so zavezani načelom »Varnega pristana«. V tem primeru dovoljenje Pooblaščenca ni potrebno, kar pa ne pomeni, da zgolj načela »Varnega pristana« zagotavljajo, da je obdela podatkov in njihov prenos ponudniku oblaka skluden z ZVOP-I.

Konkretno storitev lahko uporabljate zakonito, če s ponudnikom (pogodbenim obdelovalcem osebnih podatkov) uredite pogodbeno obdelavo osebnih podatkov

skladno z določbami 11. člena ZVOP-1, brez zadostnih informacij glede zavarovanja, ki ga nudi ponudnik te storitve, pa tvegate, da bo prišlo do kršitve določb o zavarovanju osebnih podatkov (14., 24. in 25. člen ZVOP-1), kar lahko pomeni vašo odgovornost za kršitev ZVOP-1 v primeru zlorabe osebnih podatkov (npr. razkritja, izgube, nepooblaščen seznamitve ipd). **Informacijski pooblaščenec uporabnikom, ki s strani ponudnikov rešitev računalništva v oblaku ne prejmejo potrebnih informacij, s pomočjo katerih bi lahko (sami ali s pomočjo zaupanja vrednih tretjih strank) sprejeli ustrezne analize tveganja, do nadaljnjega ne more svetovati uporabe takšnih storitev.**

Več si lahko preberete v mnenjih Pooblaščenca:

- [https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1\[showUId\]=2139&tx_jzvopdecisions_pi1\[highlightWord\]=iznos&cHash=71ca08361a8e5943f8d4000e0f2b9f2e](https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1[showUId]=2139&tx_jzvopdecisions_pi1[highlightWord]=iznos&cHash=71ca08361a8e5943f8d4000e0f2b9f2e)
- [https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1\[showUId\]=2076&tx_jzvopdecisions_pi1\[highlightWord\]=iznos&cHash=106dafa8e41c837ea55cb48cc2d3fb8](https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1[showUId]=2076&tx_jzvopdecisions_pi1[highlightWord]=iznos&cHash=106dafa8e41c837ea55cb48cc2d3fb8)

Računalništvo v oblaku obravnavajo posebne smernice pooblaščenca¹³: <https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/>.

7 Zaključek

Prenos osebnih podatkov v tretje države izven Evropske unije, pa naj bo to s strani upravljavcev osebnih podatkov ali pa s strani uporabnikov storitev, je danes praktično vsakodnevna aktivnost. V evropskem pravnem okviru so za zaščito posameznikov pri takem prenosu predvidena varovala, ki posameznikom zagotavljajo enako raven varstva osebnih podatkov za podatke, ki jih upravljavci obdelujejo znotraj EU, in tiste, ki jih posredujejo v tretje države.

V smernicah smo zato na jasn in pregleden način skušali pojasniti pravne podlage za prenos podatkov v tretje države, ki jih morajo spoštovati upravljavci osebnih podatkov, med drugim tudi obveznost, kdaj je za iznos podatkov potrebno dovoljenje Pooblaščenca in kako ga upravljavci pridobijo. Pojasnili smo tudi, na kakšen način je mogoče podatke iznašati brez vnaprejšnjega dovoljenja Pooblaščenca, ter odgovorili na nekatere najpogostejše dileme, s katerimi se srečujejo upravljavci osebnih podatkov: kako je s hrambo podatkov na strežnikih v tujini, na kaj je treba paziti, če tehnična podpora dostopa do podatkov, ki se hranijo v Sloveniji, kdaj je dobro z uvoznikom skleniti standardne pogodbene klavzule, kaj pomeni dogovor »Varni pristan«, predvsem v okviru računalništva v oblaku, kako je s pod-obdelavo osebnih podatkov s strani pogodbenega partnerja in posredovanjem podatkov materinski družbi.

¹³ Objava v drugi polovici 2012.