INFORMACIJSKI
POOBLAŠČENEC

Smernice glede prenosa osebnih podatkov

v tretje države in mednarodne organizacije po Splošni uredbi o varstvu podatkov

Namen dokumenta:	Smernice podajajo odgovore na najpogosteje zastavljena vprašanja o prenosu osebnih podatkov v tretje države in mednarodne organizacije z vidika zahtev Splošne uredbe o varstvu podatkov: kdaj govorimo o prenosu 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:	Upravljavci osebnih podatkov; obdelovalci osebnih podatkov; posamezniki, katerih podatki se prenašajo v tretje države in mednarodne organizacije.
Status:	Javno
Verzija:	1.4
Datum izdaje:	
Avtorji:	Informacijski pooblaščenec
Spremembe	1.1. Popravki zaradi sodbe Sodišča Evropske unije (C-362/14 z dne 6. 10. 2015) v zvezi z razveljavitvijo podlage za prenos osebnih podatkov v ZDA v okviru 'varnega pristana' ('*Safe Harbor*'). Popravki v skladu z Uredbo (EU) 2016/679 (Splošna uredba o varstvu podatkov). 1.2. Nova definicija prenosa (tč. 3.1.) in odgovor »*Kaj vse štejemo za prenos osebnih podatkov v tretje države?*« (tč. 7.1). 1.3 Popravki zaradi sodbe Sodišča Evropske unije (C-311/18 z dne 16. 7. 2020) v zvezi z razveljavitvijo podlage za prenos osebnih podatkov v ZDA v okviru 'zasebnostnega ščita' ('*Privacy Shield*') in zaostritve. 1.4 Popravki in dopolnitve zaradi novega EDPB Priporočila 1/2020 o ukrepih, ki dopolnjujejo orodja za prenos, da se zagotovi skladnost z v EU zagotovljenim varstvom osebnih podatkov in Priporočila 2/2020 Evropskega odbora za varstvo podatkov glede evropskih bistvenih jamstev; novih EDPB Smernic št. 2/2020 o členu 46(2)(a) in (3)(b) Uredbe 2016/679 glede prenosov osebnih podatkov med javnimi organi in telesi v EGP in zunaj EGP; in novih Standardnih pogodbenih klavzul za prenos podatkov v tretje države sprejetih s strani Evropske komisije.

Ključne besede:	Smernice, prenos oz. iznos osebnih podatkov v tretje države in mednarodne organizacije, ustrezna raven varstva osebnih podatkov, standardne pogodbene klavzule, zavezujoča poslovna pravila (ang. BCR), računalništvo v oblaku.

KAZALO

1. O smernicah Informacijskega pooblaščenca

Namen smernic Informacijskega pooblaščenca je podati skupne praktične napotke za upravljavce zbirk osebnih podatkov na jasen, razumljiv in uporaben način ter s tem odgovoriti na najpogosteje zastavljena vprašanja s področja varstva osebnih podatkov, s katerimi se srečujejo posamezni upravljavci zbirk osebnih podatkov. S pomočjo smernic naj bi upravljavci dobili priporočila, kako naj v praksi zadostijo zahtevam zakonodaje o varstvu osebnih podatkov.

Pravno podlago za izdajo smernic Informacijskemu pooblaščencu daje 3(b) odstavek 58. člena Splošne Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov; ang. GDPR), ki določa, da ima vsak nadzorni organ pooblastila v zvezi z dovoljenji in svetovalnimi pristojnostmi, med drugim, da na lastno pobudo ali na zahtevo izdaja mnenja za nacionalni parlament, vlado države članice ali, v skladu s pravom države članice, druge institucije in telesa, pa tudi za javnost, o vseh vprašanjih v zvezi z varstvom osebnih podatkov. Podobno določa tudi 27. člen Direktive (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (za njen prenos v slovenski pravni red naj bi poskrbel nov Zakon o varstvu osebnih podatkov).

Vse smernice, ki jih je izdal Informacijski pooblaščenec, so objavljene na spletni strani: https://www.ip-rs.si/publikacije/prirocniki-in-smernice/.

Informacijski pooblaščenec priporoča, da si ogledate tudi:

- mnenja na: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/ in
- brošure na: http://www.ip-rs.si/publikacije/prirocniki/.

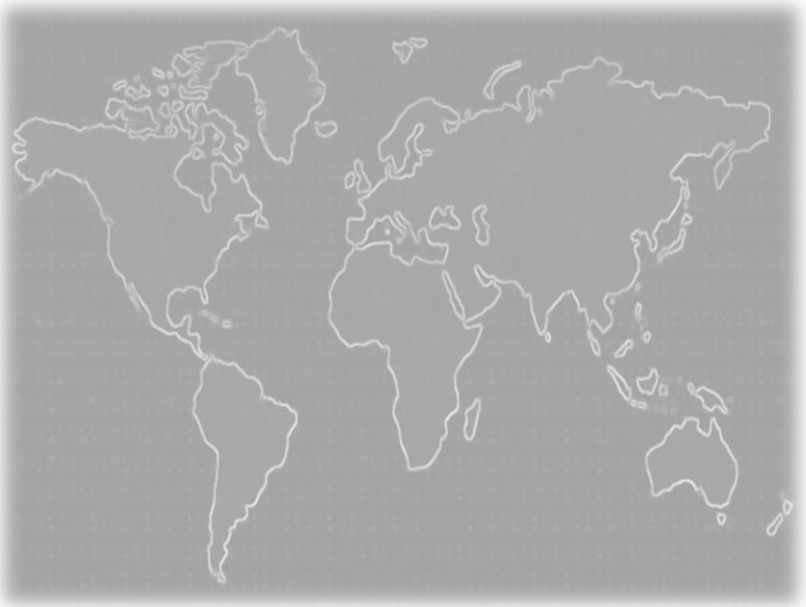
2. Uvod

Upravljavci 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 Evropski uniji (EU). Prav tako obdelovalci osebnih podatkov prenašajo svoje naloge na druge pod-obdelovalce, ki podatke analizirajo, strukturirajo, hranijo in na druge načine obdelujejo, izven evropskih meja. Na drugi strani pa tudi posamezniki vse več posegamo po storitvah ponudnikov, ki ne prihajajo iz EU. Najemanje 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 prenosov podatkov, ki predstavljajo današnjo realnost. Podatki se iz EU prenašajo tudi številnim mednarodnim organizacijam, kot so Združeni narodi, Svetovni antidopinški agenciji (WADA) ipd. 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 Splošna uredba o varstvu podatkov predvideva posebne postopke oz. varovalke v primerih, ko se osebni podatki posameznikov iz EU prenašajo v tretje države, ki ne zagotavljajo ustrezne ravni varstva osebnih podatkov. **Namen določb o prenosu podatkov v tretje države in mednarodne organizacije je zagotavljanje enake ravni varstva osebnih podatkov za podatke, ki se obdelujejo znotraj EU, in tiste, ki so posredovani v tretje države, ter tudi tiste, ki so nadalje posredovani iz tretje države ali mednarodne organizacije v druge tretje države in v druge mednarodne organizacije.** Namen pravil glede prenosov osebnih podatkov je v tem, da zagotovila in varovalni mehanizmi varstva osebnih podatkov sledijo osebnim podatkom.

V nadaljevanju pojasnjujemo ključne določbe zakonodaje, ki jih morajo upoštevati upravljavci in obdelovalci osebnih podatkov pri prenosu le teh v tretje države in mednarodne organizacije (v nadaljevanju zavoljo enostavnosti: tretje države), ter podajamo odgovore na pogosto zastavljena vprašanja.

Ob tem izpostavljamo, da za upravljavce (npr. policija), za katere ne velja Splošna uredba o varstvu podatkov, ampak Direktiva (EU) 2016/680, ki ureja varstvo podatkov pri obdelavah za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov, veljajo določbe **Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj** (Uradni list RS, št. 177/20; ZVOPOKD), ki posebej ureja prenose podatkov v tretje države in mednarodne organizacije.



3. Splošno o prenosu podatkov v tretje države po Splošni uredbi o varstvu podatkov

3.1. Kdaj gre za prenos podatkov v tretje države?

O prenosu oz. iznosu osebnih podatkov v tretje države govorimo takrat, ko upravljavec ali obdelovalec iz Slovenije ali druge države znotraj Evropskega gospodarskega prostora (to je lahko tudi podružnica) osebne podatke iz takega ali drugačnega razloga **posreduje v države izven Evropske unije (EU) ali Evropskega gospodarskega prostora** (**EGP**; sem sodijo poleg EU držav še: Islandija, Norveška in Lihtenštajn) **ali mednarodni organizaciji**. O prenosu govorimo tudi takrat, ko je **dostop do osebnih podatkov** omogočen organizacijam, podjetjem, posameznikom ali drugim subjektom iz tretjih držav izven EGP, pa čeprav so podatki hranjeni znotraj EGP.

3.2. Pogoja za prenos podatkov v tretje države

Prenos podatkov v tretje države je urejen v členih 44 do 49 Splošne uredbe o varstvu podatkov. Člen 44 določa, da je prenos podatkov dovoljen le:

(a) ob upoštevanju drugih določb Splošne uredbe o varstvu podatkov in

(b) se lahko izvede le, kadar upravljavec in obdelovalec ravnata v skladu s V. poglavjem te uredbe (kar velja tudi za nadaljnje prenose iz tretje države ali mednarodne organizacije v drugo tretjo državo ali mednarodno organizacijo), ter

(c) kadar je pri prenosu zagotovljena ustrezna raven varstva osebnih podatkov. Namen pravil glede prenosa podatkov v tretje države je v zagotovitvi, da ni ogrožena raven varstva posameznikov, ki jo zagotavlja Splošna uredba o varstvu podatkov.

Za posredovanje osebnih podatkov upravljavcu osebnih podatkov, pogodbenemu obdelovalcu ali uporabniku osebnih podatkov v tretji državi morata biti **hkrati izpolnjena dva pogoja, in sicer:**

PRVI POGOJ: Upravljavec oz. obdelovalec (izvoznik podatkov) mora imeti pravno podlago, da lahko obdeluje osebne podatke. Splošne pravne podlage so urejene v členu 6 Splošne uredbe o varstvu podatkov. Ta določa, da lahko upravljavec obdeluje osebne podatke naprej zgolj v naslednjih primerih:

(a) posameznik je v to privolil,[1]

(b) obdelava je potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik,

(c) mu to nalaga ali dovoljuje zakon,

(d) obdelava je potrebna za zaščito življenjskih interesov posameznika,

(e) obdelava je potrebna zaradi opravljanja nalog v javnem interesu ali pri izvajanju javne oblasti,

(f) obdelava je potrebna zaradi zakonitih interesov, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika.

Pravne podlage v primeru obdelave posebnih vrst osebnih podatkov pa konkretneje določa člen 9. Poleg tega morajo upravljavci v javnem sektorju še vedno upoštevati tudi določbe 1., 2. in 4. odstavka 9. člena ZVOP-1 (dokler ne stopi v veljavo in se prične uporabljati ZVOP-2). **Upravljavec mora torej najprej zagotoviti pravno podlago za (kakršen koli) prenos osebnih podatkov drugi entiteti.**

Pravna podlaga je lahko tudi **pogodba o obdelavi osebnih podatkov** – kjer obdelovalec v imenu in za račun upravljavca izvede določeno delo in pri tem

[1] Za več informacij o veljavni privolitvi vas napotujemo na spletno stran Informacijskega pooblaščenca: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/privolitev/.

obdeluje osebne podatke. Obdelovalcu se lahko osebni podatki posredujejo pod pogoji, določenimi v členu 28 Splošne uredbe o varstvu podatkov.

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 razmerjih[2] – ki določa, da se podatki zaposlenih lahko obdelujejo (torej tudi posredujejo, če je o pogodbeni obdelavi sklenjena pogodba), če je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem (48. člen). Posredovanje podatkov zaposlenih računovodstvu, kot pogodbenemu obdelovalcu, je namreč potrebno za obračun plač. Če bi delodajalec želel tretjemu posredovati podatke o svojih strankah, bi za to moral imeti katero od pravnih podlag iz člena 6 Splošne uredbe o varstvu podatkov in sklenjeno pogodbo o obdelavi osebnih podatkov (28. člen Splošne uredbe o varstvu podatkov).

DRUGI POGOJ: Po prenosu podatkov v tretjo državo je zagotovljena ustrezna raven varstva podatkov. Od tega načina zagotavljanja ustrezne ravni varstva podatkov po prenosu pa je odvisno, ali potrebuje upravljavec oziroma obdelovalec za prenos osebnih podatkov tudi dovoljenje Informacijskega pooblaščenca. Ob izpolnjenem prvem pogoju je posredovanje osebnih podatkov upravljavcu ali obdelovalcu v tretji državi ali mednarodni organizaciji dopustno pod pogoji, ki jih ureja 5. poglavje Uredbe, in sicer:

(1) če Evropska komisija odloči, da država, ozemlje, določen sektor v državi ali mednarodna organizacija, v katero se prenašajo, zagotavlja ustrezno raven varstva osebnih podatkov;

(2) če izvoznik podatkov zagotovi ustrezne zaščitne ukrepe ter posameznikom zagotovi izvršljive pravice in učinkovita pravna sredstva na podlagi členov 46 in 47 Splošne uredbe o varstvu podatkov;

(3) če gre za posebne primere, ki so določeni v členu 49 Splošne uredbe o varstvu podatkov, v katerih so mogoča odstopanja.

Posamezne oblike zagotavljanja varstva podatkov po prenosu podatkov v tretje države so podrobneje predstavljene v nadaljevanju smernic.

3.3. Kdaj je potrebno posebno dovoljenje Informacijskega pooblaščenca in kako ga pridobiti?

Po Splošni uredbi o varstvu podatkov **dovoljenje Informacijskega pooblaščenca** za prenos podatkov v tretje države ali mednarodne organizacije **v večini primerov ni (več) potrebno**. V določenih primerih pa je še zmeraj treba pridobiti dovoljenje oz. odločbo glede ustreznosti zaščitnih ukrepov, ki predstavljajo podlago za prenos podatkov.

Dovoljenje **je potrebno:**

- ko gre za prenos podatkov v tretjo državo **na podlagi pogodbenih določil, ki jih kot ustrezne zaščitne ukrepe sama določita** izvoznik in uvoznik podatkov (točka a tretjega odstavka člena 46);
- ko gre za prenos podatkov **med javnimi organi ali telesi** na podlagi **določb, ki se vstavijo v upravne dogovore** in v katere so vključene izvršljive in učinkovite pravice za posameznike (točka b tretjega odstavka člena 46).

Dovoljenje s strani vodilnega nadzornega organa je potrebno tudi pri prenosu podatkov na podlagi **zavezujočih poslovnih pravil (BCR)**. Pred prenosom podatkov je treba dati zavezujoča poslovna pravila v odobritev vodilnemu nadzornemu organu, ki nato postopa v skladu z mehanizmom za skladnost iz člena 63 Splošne uredbe o varstvu podatkov. Odobrena so lahko le pod pogojem,

(1) da so pravno zavezujoča za vsakega člana povezane družbe ali skupine podjetij, tudi za zaposlene,

[2] Uradni list RS, št. 21/13, 78/13 – popr., 47/15 – ZZSDT, 33/16 – PZ-F, 52/16 in 15/17 – odl. US.

(2) da posameznikom izrecno podeljujejo izvršljive pravice v zvezi z obdelavo njihovih podatkov in

(3) da izpolnjujejo zahteve iz člena 47(2) Splošne uredbe o varstvu podatkov, ki določa minimalno vsebino zavezujočih poslovnih pravil.

Po odobritvi s strani nadzornega organa, lahko podjetja znotraj multinacionalne skupine podjetij poljubno (vendar v mejah potrjenih zavezujočih poslovnih pravil) prenašajo podatke med seboj. To pomeni, da ni potrebno pridobiti dovoljenja za prenos na podlagi zavezujočih poslovnih pravil od drugih nadzornih organov.

Kako pridobiti dovoljenje Informacijskega pooblaščenca?

V upravni zadevi lahko upravljavec ali obdelovalec zahteva, da Informacijski pooblaščenec odobri pogodbena določila (iz točke a tretjega odstavka člena 46), da odobri upravne dogovore (iz točke b tretjega odstavka člena 46) ali da odobri zavezujoča poslovna pravila (v skladu s členom 47).

Za uvedbo postopka ugotavljanja ustrezne ravni varstva osebnih podatkov mora izvoznik podatkov na Informacijskega pooblaščenca nasloviti **vlogo**. V vlogi mora navesti svoje podatke, podatke o uvozniku osebnih podatkov, o načinih in namenih obdelave, kategorijah osebnih podatkov, osebah, na katere se nanašajo, uporabnike podatkov, čas hrambe ter ostale podatke, ki so relevantni za konkretni prenos. Upravljavec mora prav tako izkazati pravno podlago za obdelavo in prenos osebnih podatkov ter pojasniti način za zagotavljanje ustrezne ravni varstva podatkov po prenosu podatkov - priložiti mora dokumente, v katerih je to opredeljeno (npr. vse relevantne pogodbe in določila). Informacijski pooblaščenec pa nato presodi, ali je izkazano, da bo po prenosu zagotovljena ustrezna raven varstva osebnih podatkov. O vlogi odloči v dveh mesecih. Postopek za prenos podatkov, ki zahteva pridobivanje odločbe Informacijskega pooblaščenca, je vsekakor daljši kot postopek, za katerega takšno dovoljenje ni potrebno.

3.4. Kdaj posebno dovoljenje Informacijskega pooblaščenca ni potrebno?

Dovoljenje Informacijskega pooblaščenca po Splošni uredbi o varstvu podatkov ni potrebno za prenos podatkov v tretje države ali mednarodne organizacije v naslednjih primerih:

- **kadar obstaja sklep o ustreznosti Evropske komisije** o tem, da določena država, ozemlje, določen sektor v državi ali mednarodna organizacija zagotavlja ustrezno raven varstva osebnih podatkov;
- **kadar obstaja pravno zavezujoč in izvršljiv inštrument**, ki ga sprejmejo **javni organi ali telesa** (gre za mehanizem, ki pride v poštev zgolj za prenos podatkov med javnimi organi ali telesi),
- **ob uporabi zavezujočih poslovnih pravil**, s katerimi se multi-nacionalna podjetja zavežejo k ustrezni ravni varstva osebnih podatkov (ang. *Binding Corporate Rules, BCR*),
- **ob uporabi tipskega besedila pogodb**, ki jih je pripravila Evropska komisija – standardne pogodbene klavzule (SPK),
- **kadar obstaja odobren kodeks ravnanja** v skladu s členom 40, skupaj z zavezujočimi in izvršljivimi zavezami uvoznika podatkov, da bo uporabljal ustrezne zaščitne ukrepe,
- **kadar obstaja odobren mehanizem potrjevanja**[3] v skladu s členom 42, skupaj z zavezujočimi in izvršljivimi zavezami uvoznika podatkov, da bo uporabljal ustrezne zaščitne ukrepe.

Pri prenosu podatkov **od upravljavca k obdelovalcu** je treba upoštevati tudi pogoje iz člena 28 Splošne uredbe o varstvu podatkov ter v skladu s tem skleniti pogodbo o obdelavi osebnih podatkov.

[3] Trenutno v Evropski uniji še ni razvit in potrjen noben mehanizem certificiranja po členu 42 Splošne uredbe o varstvu podatkov.

4. Prenos v države in mednarodne organizacije, ki zagotavljajo ustrezno raven varstva osebnih podatkov

4.1. Kdaj se lahko prenaša podatke v tretje države in mednarodne organizacije brez dovoljenja Informacijskega pooblaščenca in brez ustreznih zaščitnih ukrepov?

Če je tretja država, ozemlje, eden ali več določenih sektorjev v tej tretji državi ali mednarodni organizaciji na seznamu iz člena 45 Splošne uredbe o varstvu podatkov, za katere je **Evropska komisija ugotovila, da zagotavljajo ustrezno raven varstva osebnih podatkov**.

Spisek držav, za katere je Evropska komisija ugotovila, da zagotavljajo ustrezno raven varstva osebnih podatkov se nahaja tu: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Evropska komisija pri ocenjevanju ustreznosti ravni varstva osebnih podatkov v tretji državi ali mednarodni organizaciji upošteva med drugim elemente kot so: načelo pravne države, spoštovanje človekovih pravic in temeljnih svoboščin, pravni okvir za varstvo osebnih podatkov in udejanjanje v praksi, obstoj učinkovito delujočih neodvisnih nadzornih organov, mednarodne zaveze tretje države.

Odločbe, s katerimi je Informacijski pooblaščenec pred 25. 5. 2018 skladno s takrat veljavnim 66. členom ZVOP-1 ugotovil, da določene tretje države ali mednarodne organizacije zagotavljajo ustrezno raven varstva osebnih podatkov (to so bile Švicarska konfederacija, Makedonija in Izrael v delu, kjer gre za avtomatizirane prenose osebnih podatkov iz EU ali neavtomatizirane prenose, pri katerih se v Izraelu izvaja nadaljnja avtomatizirana obdelava) ostajajo v veljavi tudi po navedenem datumu vse dokler se jih ne spremeni, nadomesti ali razveljavi, kar bo moral urediti ZVOP-2.

5. Prenos na podlagi ustreznih zaščitnih ukrepov

Osebni podatki se lahko posredujejo v tretjo državo, ki ne zagotavlja ustrezne ravni varstva osebnih podatkov tudi, če upravljavec osebnih podatkov **zagotovi ustrezne zaščitne ukrepe** in pod pogojem, da imajo posamezniki, na katere se nanašajo osebni podatki, **na voljo izvršljive pravice in učinkovita pravna sredstva** (člen 46 Splošne uredbe o varstvu podatkov). Za prenos podatkov v tretjo državo z uporabo ustreznih zaščitnih ukrepov v večini primerov ne potrebujete dovoljenja Informacijskega pooblaščenca, v določenih primerih pa je takšno dovoljenje pogoj za zakonit prenos.

(1) Izvozniki podatkov lahko **brez predhodnega dovoljenja Informacijskega pooblaščenca** zagotovijo ustrezne zaščitne ukrepe za prenos s:

- pravno zavezujočim in izvršljivim inštrumentom, ki ga sprejmejo javni organi ali telesa,
- **zavezujočimi poslovnimi pravili**, s katerimi se multi-nacionalna podjetja zavežejo k ustrezni ravni varstva osebnih podatkov (ang. Binding Corporate Rules, BCR),
- **uporabo tipskega besedila pogodb**, ki jih je pripravila Evropska komisija – standardne pogodbene klavzule (SPK),
- **uporabo tipskega besedila pogodb**, ki bi jih pripravil Informacijski pooblaščenec in odobrila Evropska komisija – standardne pogodbene klavzule (SPK),[4]
- **uporabo odobrenega kodeksa ravnanja** v skladu s členom 40, skupaj z zavezujočimi in izvršljivimi zavezami uvoznika podatkov, da bo uporabljal ustrezne zaščitne ukrepe,
- **uporabo odobrenega mehanizma potrjevanja**[5] v skladu s členom 42, skupaj z zavezujočimi in izvršljivimi zavezami uvoznika podatkov, da bo uporabljal ustrezne zaščitne ukrepe.

(2) Ustrezni zaščitni ukrepi se lahko **z dovoljenjem Informacijskega pooblaščenca** zagotovijo tudi s:

- **pogodbenimi določili**, ki jih določita izvoznik in uvoznik podatkov,
- **določbami, ki se ustavijo v upravne dogovore med javnimi organi ali telesi** in v katere so vključene izvršljive in učinkovite pravice za posameznike.

V primeru (1) izvoznik ne potrebuje dovoljenja Informacijskega pooblaščenca, kar pomeni, da če zagotovi enega izmed naštetih ustreznih zaščitnih ukrepov (npr. z uvoznikom sklene tipsko pogodbo s standardnimi pogodbenimi klavzulami), lahko na podlagi le-teh prenaša podatke v tretjo državo. Takšen način prenosa podatkov v tretjo državo je **hitrejši in enostavnejši.** V primeru (2) mora izvoznik podatkov na Informacijskega pooblaščenca nasloviti **vlogo za izdajo posebne odločbe**, osebne podatke pa sme prenesti v tretjo državo ali mednarodno organizacijo šele **po prejemu dovoljenja.** Upravljavec v vlogi opredeli vrste osebnih podatkov, namen obdelave, posameznike, na katere se podatki nanašajo, uporabnike, čas hrambe. Upravljavec mora prav tako izkazati pravno podlago za obdelavo osebnih podatkov in uporabo ustreznih mehanizmov za zagotavljanje varstva podatkov po prenosu - priložiti mora dokumente, ki so podlaga za prenos (npr. vse relevantne pogodbe in določila). Informacijski pooblaščenec pa nato presodi, ali je zagotovljeno ustrezno varstvo osebnih podatkov. **Postopek je v tem primeru daljši, zato Informacijski pooblaščenec priporoča uporabo tipskih pogodb in zavezujočih poslovnih pravil.**

V primeru prenosa osebnih podatkov na podlagi ustreznih zaščitnih ukrepov je izvoznik podatkov dolžan po potrebi zagotoviti **dopolnilne zaščitne ukrepe,**

[4] Informacijski pooblaščenec do sedaj ni sprejel svojih standardnih pogodbenih klavzul, kar pomeni, da pridejo v poštev le tiste s strani Evropske komisije.

[5] Trenutno v Evropski uniji še ni razvit in potrjen noben mehanizem certificiranja po členu 42 Splošne uredbe o varstvu podatkov.

ki zagotavljajo varovanje zasebnosti ter temeljnih človekovih pravic na enaki ravni, kot je to zagotovljeno v okviru EU.

5.1. Dopolnilni zaščitni ukrepi

Sodišče Evropske unije (SEU) je v sodbi v zadevi C-311/18 z dne 16. 7. 2021 (Schrems II) poudarilo, da se mora za osebne podatke, ne glede na to, kam se prenesejo, zagotoviti v bistvu enakovredno varstvo, kot se zanje zagotavlja v EGP. S prenosom osebnih podatkov v tretje države se ne sme ogroziti ali zmanjšati varstva, ki se jim zagotavlja v EGP.

V primeru prenosa osebnih podatkov na podlagi ustreznih zaščitnih ukrepov (npr. standardnih pogodbenih klavzul ali zavezujočih poslovnih pravil) **morata zato izvoznik in uvoznik podatkov pred samim prenosom podatkov oceniti, ali se v zadevni tretji državi upošteva raven varstva, ki jo zahteva zakonodaja EU, da bi ugotovila, ali je mogoče tudi v praksi zagotoviti jamstva, ki jih zagotavljajo ustrezni zaščitni ukrepi.** V nasprotnem primeru je treba presoditi, ali je mogoče zagotoviti **dopolnilne zaščitne ukrepe**, s pomočjo katerih bi prenos podatkov izpolnjeval standard v bistvu enakovrednega varstva, ki se zahteva s pravom EU. Dopolnilni zaščitni ukrepi po svoji naravi dopolnjujejo varovalke, ki jih že vsebujejo orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov in druge zahteve glede varnosti podatkov iz uredbe. Ti ukrepi so lahko na primer tehnične narave, organizacijske narave ali v obliki dodatnih pogodbenih zavez.

Za izvedbo konkretne presoje glede prenosov, prava tretje države in orodja, na podlagi katerega se bodo prenašali podatki, so odgovorni izvozniki podatkov. Izvozniki podatkov morajo pri tem ravnati s potrebno skrbnostjo in **temeljito dokumentirati svoj postopek**, saj so v skladu z načelom odgovornosti iz Splošne uredbe o varstvu podatkov odgovorni za skladnost z uredbo in morajo biti sposobni to skladnost tudi izkazati.

Evropski odbor za varstvo podatkov je v pomoč izvoznikom in uvoznikom podatkov sprejel **Priporočila 01/2020 o ukrepih, ki dopolnjujejo orodja za prenos, da se zagotovi skladnost z v EU zagotovljenim varstvom osebnih podatkov**:

- https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

Priporočila 01/2020 pojasnjujejo šest korakov, ki lahko izvoznikom in uvoznikom pomagajo pri oceni ravni varstva osebnih podatkov v tretji državi in pri ugotavljanju, ali je za konkretni prenos podatkov treba uvesti tudi dopolnilne zaščitne ukrepe:

Korak 1: Izvoznik mora preučiti svoje prenose podatkov v tretjo državo.

Korak 2: Nato mora opredeliti orodje za prenos podatkov, na katerega se bo oprl.

Korak 3: Ključen je tretji korak, ki izvozniku podatkov pomaga oceniti, ali je orodje **za prenos iz člena 46 Splošne uredbe o varstvu podatkov, na katerega** opira prenos, **učinkovito glede na vse okoliščine prenosa**. Ocena prenosa naj pri tem primarno temelji na javno objavljeni **zakonodaji, ki velja v tretji državi**, ob tem pa je treba preučiti tudi **prakse javnih organov tretje države**. Četudi na primer ustrezna zakonodaja tretje države formalno izpolnjuje standarde EU glede temeljnih pravic in svoboščin ter nujnosti in sorazmernost teh omejitev, se lahko zgodi, da javni organi v praksi navedene zakonodaje ne upoštevajo. V takem primeru je treba pri oceni v okviru tretjega koraka upoštevati prakse teh organov. Na podlagi ocene, ki jo mora izvoznik dokumentirati, slednji sprejme odločitev o tem, da bo podatke prenašal v tretjo državo, da bo prekinil prenos podatkov ali da bo prenašal podatke in ob tem sprejel ustrezne dopolnilne zaščitne ukrepe.

V pomoč pri oceni elementov, **ki jih je treba upoštevati pri oceni prava tretje države, ki obravnava dostop javnih organov do podatkov za namene nadzora,** je Evropski odbor za varstvo podatkov sprejel **Priporočila**

02/2020 Evropskega odbora za varstvo podatkov glede evropskih bistvenih jamstev, ki so dostopna preko povezave:

- https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_sl.pdf.

Korak 4: Če je to mogoče in na podlagi ocene v skladu s korakom 3 potrebno, izvoznik **sprejme ustrezne dopolnilne zaščitne ukrepe**. Z dopolnilnimi ukrepi zagotovi, da bo prenos podatkov izpolnjeval **standard v bistvu enakovrednega varstva, ki se zahteva s pravom EU**, kar pomeni, da je takšen prenos skladen z evropsko zakonodajo**. P**riporočila 01/2020 podajajo nekaj konkretnih primerov dopolnilnih ukrepov z razlago.

Korak 5: Upoštevati je treba postopkovne korake glede dopolnilnih ukrepov, ki se lahko razlikujejo glede na izbrano orodje za prenos podatkov.

Korak 6: Izvoznik mora redno spremljati razvoj v tretji državi, ki bi lahko vplival na oceno glede ravni varstva osebnih podatkov v tretji državi in na odločitev, ki je bila na podlagi tega sprejeta.

5.2. Prenos na podlagi standardnih pogodbenih klavzul (SPK)

V pomoč izvoznikom, 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 izvoznik in uvoznik podatkov.**

Evropska komisija je dne 4. 6. 2021 sprejela nove standardne pogodbene klavzule (v nadaljevanju: SPK ali angl. SCC), na podlagi katerih lahko izvoznik in uvoznik prenašata osebne podatke. Nove klavzule so usklajene s Splošne uredbo o varstvu podatkov in s sodbo SEU v zadevi C-311/18 (Schrems II). **Prejšnje SPK se lahko uporabijo do dne 27. 9. 2021, po tem datumu lahko organizacije sklenejo le še nove SPK. Do dne 27. 12. 2022 morajo biti vse pogodbe prilagojene novim SPK.** V vsakem primeru pa so izvozniki in uvozniki dolžni spoštovati sodbo SEU v zadevi Schrems II in, v kolikor je to potrebno, zagotoviti dopolnilne zaščitne ukrepe, kakor je pojasnjeno v poglavju 5.1 Dopolnilni zaščitni ukrepi.

Upravljavcu ali obdelovalcu, ki prenaša osebne podatke na podlagi SPK, **ni treba pridobiti posebnega dovoljenja Informacijskega pooblaščenca**.

SPK urejajo **prenose podatkov od upravljavca ali obdelovalca, ki te podatke obdeluje v skladu s Splošno uredbo o varstvu podatkov, upravljavcu ali (pod)obdelovalcu, za katerega se pri obdelavi teh podatkov navedena uredba ne uporablja**. S SPK je tako mogoče prenašati podatke od izvoznika podatkov iz EGP uvozniku podatkov izven EGP. Poleg tega pa je z novimi SPK mogoče urediti tudi prenose podatkov med izvoznikom podatkov, ki ima ustanovitev v tretji državi in ga Splošna uredba o varstvu podatkov zavezuje na podlagi člena 3(2), uvozniku podatkov, ki se nahaja izven EGP in zanj Splošna uredba o varstvu podatkov ne velja.

V primerjavi s prejšnjimi SPK nove klavzule pokrivajo tudi prenose podatkov, ko **kot izvoznik podatkov nastopa obdelovalec.** Novo je tudi to, da kadar je uvoznik podatkov obdelovalec ali podobdelovalec, **SPK že vključujejo tudi vse pogodbene zahteve iz člena 28 Splošne uredbe o varstvu podatkov,** zato pogodbenima strankama oziroma strankam ni treba sklepati dveh ločenih pogodb, temveč bo vse pokrila enovita pogodba. Nove klavzule tudi **omogočajo dodajanje več kot dveh strank v pogodbeno ureditev, tako med njenim sklepanjem kot tudi kasneje** (npr. s pogodbo se lahko naknadno zaveže podobdelovalec).

Nove SPK so modularnega značaja, kar pomeni, da vključujejo različne scenarije obdelave osebnih podatkov, ki jih pogodbeni stranki izbereta glede na konkretne okoliščine prenosa oziroma glede na to, kdo sta stranki pogodbe:

- Modul 1: upravljavec prenaša podatke upravljavcu,
- Modul 2: upravljavec prenaša podatke obdelovalcu,
- Modul 3: obdelovalec prenaša podatke obdelovalcu,
- Modul 4: obdelovalec prenaša podlage upravljavcu.

Do vseh **štirih modulov standardnih pogodbenih klavzul** oziroma do Izvedbenega sklepa Komisije (EU) 2021/914 z dne 4. junija 2021 o standardnih pogodbenih določilih za prenos osebnih podatkov v tretje države v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta lahko dostopate prek povezave:

- https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=uriserv%3AOJ.L_.2021.199.01.0031.01.SLV&toc=OJ%3AL%3A2021%3A199%3ATOC.

Stranke lahko SPK vključijo v širšo pogodbo, lahko dodajo druga določila ali dodatne zaščitne ukrepe, vendar le pod pogojem, da ta določila ne nasprotujejo SPK ali posegajo v temeljne pravice in svoboščine posameznikov, na katere se podatki nanašajo.

V skladu s sodbo SEU v zadevi Schrems II **se prenos in obdelava osebnih podatkov na podlagi SPK ne bi smela izvajati, če zakoni in prakse namembne tretje države uvozniku podatkov preprečujejo, da bi spoštoval določila**.[6] Izvoznik in uvoznik podatkov zato s sklenitvijo SPK na podlagi določila 14 jamčita, da »nimata razloga za domnevo, da zakoni in prakse v namembni tretji državi … uvozniku podatkov preprečujejo izpolnjevanje obveznosti iz teh določil«. To jamstvo mora temeljiti na oceni, ki jo je treba dokumentirati in katere predložitev lahko zahteva nacionalni nadzorni organi za varstvo osebnih podatkov, v Sloveniji je to Informacijski pooblaščenec.

Na podlagi SPK je uvoznik podatkov dolžan izvoznika nemudoma obvestiti, če iz kakršnega koli razloga ne more spoštovati SPK. V takem primeru mora izvoznik nemudoma opredeliti ustrezne zaščitne ukrepe (npr. tehnične ali organizacijske ukrepe za zagotovitev varnosti in zaupnosti) oziroma ustaviti prenos podatkov, v posebej resnih primerih kršitev oziroma nezmožnosti spoštovanja SPK pa ima izvoznik pravico do odpovedi pogodbe.

[6] Glej poglavje 5.1 Dopolnilni zaščitni ukrepi.

Ključno je, da stranki oz. stranke pogodbe natančno in jasno določijo tehnične in organizacijske ukrepe, s katerimi bodo zagotavljale varnost osebnih podatkov, in ukrepe, s katerimi bo uvoznik podatkov zagotovil pomoč izvozniku (npr. pomoč pri obvestilu o kršitvi varnosti podatkov). Priloga II k SPK našteva nekaj možnih ukrepov.

Nove SPK krepijo pravice posameznikov, in sicer jim med drugim zagotavljajo, da so obveščeni o postopkih obdelave njihovih podatkov, da imajo možnost, da vzpostavijo stik s tujimi upravljavci in obdelovalci, da prejmejo kopijo sklenjenih klavzul, lahko zahtevajo odškodnino za škodo, povzročeno v zvezi z njihovimi osebnimi podatki itd. Posamezniki se lahko kot tretje upravičene osebe glede svojih pravic sklicujejo neposredno na SPK in svoje pravice (tudi zoper uvoznika) uveljavljajo pri nadzornemu organu za varstvo podatkov v EGP in na evropskih sodiščih.

5.3. Prenos na podlagi zavezujočih poslovnih pravil (ang. *Binding Corporate Rules, BCR*)

Zavezujoča poslovna pravila predstavljajo interni akt multi-nacionalne korporacije – skupine podjetij, od katerih so določena podjetja locirana zunaj EU/EGP, v tretjih državah, ki ne zagotavljajo ustreznega varstva osebnih podatkov. Namen zavezujočih poslovnih pravil je, da je v korporaciji, ki ima lahko člane tudi v tretjih državah, omogočen prost pretok osebnih podatkov in da ni potrebno za vsak prenos podatkov v tretje države pridobiti posebnega dovoljenja nadzornega organa. Podrobneje so urejena v členu 47 Splošne uredbe o varstvu podatkov.

Predpogoj za prenos podatkov v tretjo državo na podlagi zavezujočih poslovnih pravil **je predhodna odobritev zavezujočih poslovnih pravil s strani vodilnega nadzornega organa** v skladu z mehanizmom za skladnost iz člena 63 Splošne uredbe o varstvu podatkov. To pomeni, da vlogo za odobritev zavezujočih poslovnih pravil z vso potrebno dokumentacijo naslovite na vodilni nadzorni organ. **Vodilni nadzorni organ je običajno tisti nadzorni organ, ki se nahaja, kjer je (glavni) sedež upravljavca ali obdelovalca**. Ni pa nujno vedno tako. Za določitev vodilnega nadzornega

organa v postopku odobritve zavezujočih poslovnih pravil si lahko pomagate z dokumentom Evropske komisije z naslovom »*Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR*«.[7]

Zavezujoča poslovna pravila so lahko odobrena le pod pogojem, da:

(1) so pravno zavezujoča za vsakega člana povezane družbe ali skupine podjetij, tudi za zaposlene,

(2) posameznikom izrecno podeljujejo izvršljive pravice v zvezi z obdelavo njihovih podatkov in

(3) izpolnjujejo zahteve iz člena 47/II Splošne uredbe o varstvu podatkov. **Člen 47/II določa minimalno vsebino zavezujočih poslovnih pravil.**

Ko so zavezujoča poslovna pravila odobrena s strani vodilnega nadzornega organa, se šteje, da zagotavljajo ustrezno raven varstva za posredovanje podatkov znotraj skupine podjetij/korporacije, ki so se zavezala k spoštovanju teh pravil. Postopek je zasnovan na način, da se korporacije izognejo temu, da bi morale komunicirati in pridobiti dovoljenja s strani več nadzornih organov, temveč v tem postopku sodelujejo le z vodilnim nadzornim organom.

Tudi pri prenosu podatkov na podlagi zavezujočih poslovnih pravil morajo organizacije zagotoviti, da se osebnim podatkom ne glede na to, kam se prenesejo, zagotovi **v bistvu enakovredno varstvo, kot se zanje zagotavlja v EGP**. Več o tem, kako oceniti raven varstva podatkov v tretji državi in glede dopolnilnih zaščitnih ukrepov, si preberite v poglavju 5.1 Dopolnilni zaščitni ukrepi.

Na podlagi zavezujočih poslovnih pravil ni mogoč prenos podatkov podjetjem zunaj korporacije. Če bi želela korporacija podatke iznašati zunanjemu obdelovalcu v tretji državi, bi morala za to imeti drugo pravno podlago (npr. sklenjene standardne pogodbene klavzule).

V zavezujočih poslovnih pravilih je lahko zajeto celotno posredovanje osebnih podatkov, vendar mora biti to natančno opredeljeno. **Vodila za sestavo teksta zavezujočih poslovnih pravil** so dostopna na naslednjih povezavah:

- https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48799 (zavezujoča poslovna pravila za obdelovalce),
- https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48798 (zavezujoča poslovna pravila za upravljavce).

V primeru večjih sprememb zavezujočih poslovnih pravil se mora korporacija znova obrniti na vodilni nadzorni organ, saj se šteje, da le tekst zavezujočih poslovnih pravil, ki ga je nadzorni organ skupaj z nadzornimi organi iz drugih držav članic v skladu z mehanizmom za skladnost sprejel, zagotavlja ustrezno varstvo osebnih podatkov.

Organizacija mora vodilnemu nadzornemu organu za odobritev zavezujočih poslovnih pravil za namen prenosa podatkov v tretje države posredovati:

- obrazec WP 264 za zavezujoča poslovna pravila za upravljavce (standardni obrazec predpisan s strani Delovne skupine iz člena 29, s katerim korporacija prične postopek izbire vodilnega organa) – dostopen na tej povezavi:
  - https://edpb.europa.eu/our-work-tools/our-documents/recommendation-standard-application-form-approval-controller-binding_en;
- obrazec WP 265 za zavezujoča poslovna pravila za obdelovalce – dostopen na tej povezavi:
  - http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623848;
- tekst zavezujočih poslovnih pravil (ang. BCR).

[7] Dokument je za zdaj dostopen zgolj v angleškem jeziku: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056.

6. Prenos podatkov na podlagi odstopanj v posebnih primerih

Če sklep o ustreznosti zagotovljene ravni varstva osebnih podatkov za določeno državo oz. mednarodno organizacijo iz člena 45 Splošne uredbe o varstvu podatkov ni sprejet in če ni mogoče sprejeti ustreznih zaščitnih ukrepov v skladu s členom 46, se lahko prenos izvede le v določenih posebnih primerih, kakor to določa člen 49. Prenos se na podlagi teh pogojev lahko izvede zgolj **izjemoma**, **če prenos v tretjo državo ali mednarodno organizacijo z uporabo drugih mehanizmov varstva na podlagi člena 45 ali člena 46 resnično ni možen (oz. vse dokler ni možen).** Gre za odstopanja, ki so mogoča, če je izpolnjen eden izmed sledečih pogojev:

(a) posameznik, na katerega se nanašajo osebni podatki, je **izrecno privolil** v predlagani prenos, potem ko je bil **obveščen o morebitnih tveganjih**, ki jih zaradi nesprejetja sklepa o ustreznosti in ustreznih zaščitnih ukrepov takšni prenosi pomenijo zanj (npr. da v tretji državi morda ne bo lokalnega nadzornega organa, na katerega bi se lahko obrnil za izvrševanje svojih pravic);[8]

(b) (b) prenos je potreben **za izvajanje pogodbe** med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem ali **za izvajanje predpogodbenih ukrepov**, sprejetih na zahtevo posameznika, na katerega se nanašajo osebni podatki (npr. napotitev delavca na usposabljanje v tretjo državo);

(c) prenos je potreben **za sklenitev ali izvajanje pogodbe** med upravljavcem in drugo fizično ali pravno osebo, ki je **v interesu posameznika**, na katerega se nanašajo osebni podatki;

(d) prenos je potreben zaradi **pomembnih razlogov javnega interesa**;

(e) prenos je potreben **za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov**;

(f) prenos je potreben **za zaščito življenjskih interesov posameznika**, na katerega se nanašajo osebni podatki, ali drugih oseb, kadar posameznik, na katerega se nanašajo osebni podatki, fizično ali pravno **ni sposoben dati privolitve**;

(g) prenos se opravi **iz registra, ki je po pravu EU ali pravu države članice namenjen zagotavljanju informacij javnosti** in je na voljo za vpogled bodisi javnosti na splošno bodisi kateri koli osebi, ki lahko izkaže zakonit interes, vendar le, če so v posameznem primeru izpolnjeni pogoji za tak vpogled, določeni s pravom EU ali pravom države članice.

6.1. Odstopanja od odstopanj

V kolikor prenos ni možen na podlagi zgoraj navedenih pogojev, se lahko izvede le v strogo določenih primerih, in sicer je tak prenos možen zgolj, **če:**

- **ni ponovljiv,**
- **zadeva le omejeno število posameznikov, na katere se nanašajo osebni podatki,**
- **je potreben zaradi nujnih zakonitih interesov, za katere si prizadeva upravljavec in ki ne prevladajo nad interesi ali pravicami in svoboščinami posameznika, ter če**
- **je upravljavec predhodno ocenil vse okoliščine v zvezi s prenosom podatkov in na podlagi te ocene predvidel ustrezne zaščitne ukrepe v zvezi z varstvom osebnih podatkov.**

Oceno in predvidene ukrepe mora upravljavec oz. obdelovalec **dokumentirati v evidenci o obdelavi podatkov** skladno s členom 30 Splošne uredbe o varstvu podatkov. Poleg tega mora upravljavec o tem **obvestiti**

[8] Glede pogojev za veljavno izrecno privolitev vas napotujemo na spletno stran Informacijskega pooblaščenca: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/privolitev/.

nadzorni organ, torej Informacijskega pooblaščenca, posameznikom pa zagotoviti informacije iz členov 13 in 14 Splošne uredbe o varstvu podatkov ter informacije o zadevnem prenosu in nujnih zakonitih interesih, zaradi katerih je prenos potreben.

Za več informacij o prenosu podatkov na podlagi odstopanj v posebnih primerih, si preberite **Smernice št. 2/2018 o odstopanjih iz člena 49 v skladu s Splošno uredbo o varstvu podatkov**, ki so dostopne na spletni povezavi:

- https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_sl.

Podrobnejše informacije glede tega, kdo so javni organi in kaj morajo takšni pravno zavezujoči in izvršljivi inštrumenti ter upravni dogovori vsebovati, lahko pridobite v **Smernicah št. 2/2020 o členu 46(2)(a) in (3)(b) Uredbe 2016/679 glede prenosov osebnih podatkov med javnimi organi in telesi v EGP in zunaj EGP**, ki jih je sprejel Evropski odbor za varstvo podatkov. Smernice so dostopne na povezavi:

- https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_sl.

7. Prenos podatkov med javnimi organi

Če želi javni organ ali telo iz EGP prenašati podatke drugemu javnemu organu v tretjo državo ali mednarodni organizaciji, ki niso bile zajete s sklepom o ustreznosti Evropske komisije, mora za to predhodno zagotoviti ustrezen mehanizem za prenos podatkov. Splošna uredba o varstvu podatkov predvideva dva mehanizma, ki sta najbolj primerna za takšne prenose podatkov:

- Prenos podatkov **na podlagi pravno zavezujočega in izvršljivega inštrumenta**, ki ga sprejmejo **javni organi ali telesa** (točka a člena 46(2)). Dovoljenje vodilnega nadzornega organa v tem primeru ni potrebno.
- Prenos podatkov med javnimi organi ali telesi na podlagi **določb, ki se vstavijo v upravne dogovore** in v katere so vključene izvršljive in učinkovite pravice za posameznike (točka b člena 46(3)). V takem primeru je **predhodno dovoljenje vodilnega nadzornega organa obvezno.**

8. Pogosto zastavljena vprašanja ali situacije in kako v njih ravnati?

8.1. Kaj vse štejemo za prenos 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 EGP (sem sodijo poleg vseh držav EU še države: Islandija, Norveška in Lihtenštajn), ali s strani mednarodne organizacije. Obdelava osebnih podatkov pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, zlasti zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje. 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 prenos 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).

8.2. V katere države lahko prenašamo podatke, ne da bi za to morali zagotoviti ustrezne zaščitne ukrepe ali pridobiti dovoljenje Informacijskega pooblaščenca?

Osebne podatke se lahko posreduje v vsako izmed držav članic EU in v države EGP. V takem primeru ne gre za prenos podatkov v tretjo državo. Prenos podatkov brez zagotovljenih ustreznih zaščitnih ukrepov in brez dovoljenja Informacijskega pooblaščenca pa je možen v vse tiste države izven EU/EGP, za katere je Evropska komisija že ugotovila, da v celoti ali delno zagotavljajo ustrezno raven varstva osebnih podatkov. Spisek držav, za katere je Evropska komisija ugotovila, da zagotavljajo ustrezno raven varstva osebnih podatkov se nahaja tu: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Za prenos osebnih podatkov v navedene države ni potrebno zagotoviti ustreznih zaščitnih ukrepov (člen 46 Splošne uredbe o varstvu podatkov) niti ni potrebno pridobiti odločbe Informacijskega pooblaščenca.

8.3. 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 prenos 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 prenos podatkov v tretje države.

8.4. Podjetje iz Slovenije, katerega materinska družba je v tretji državi, za katero Informacijski 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 Informacijskega pooblaščenca?

Če štejemo podjetje iz Slovenije za upravljavca (naj bo to podružnica ali samostojna pravna oseba v okviru skupine povezanih družb) mora imeti za posredovanje podatkov najprej 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 6. člena Splošne uredbe o varstvu podatkov. 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.[9]

Podjetja lahko za prenos podatkov o zaposlenih in strankah, ki jih obdeluje v skladu s prejšnjim odstavkom, **brez predhodnega dovoljenja Informacijskega pooblaščenca** zagotovijo ustrezne zaščitne ukrepe z:

- **zavezujočimi poslovnimi pravili**, s katerimi se multi-nacionalna podjetja zavežejo k ustrezni ravni varstva osebnih podatkov za prenose znotraj skupine podjetij,
- **tipskimi pogodbami**, ki jih je pripravila Evropska komisija – standardne pogodbene klavzule (SPK),
- **odobrenim kodeksom ravnanja** v skladu s členom 40, skupaj z zavezujočimi in izvršljivimi zavezami uvoznika podatkov, da bo uporabljal ustrezne zaščitne ukrepe,
- **odobrenim mehanizmom potrjevanja** v skladu s členom 42, skupaj z zavezujočimi in izvršljivimi zavezami uvoznika podatkov, da bo uporabljal ustrezne zaščitne ukrepe (mehanizmi potrjevanja v EU trenutno še niso razviti, posledično te podlage sedaj še ni mogoče koristiti).

Materinsko podjetje v tretji državi lahko predstavlja **upravljavca osebnih podatkov**. V takem primeru je za zakoniti prenos in obdelavo podatkov potrebno zagotoviti eno izmed **pravnih podlag za obdelavo** iz člena 6 Splošne uredbe o varstvu podatkov oz. člena 9 v primeru obdelave posebnih vrst osebnih podatkov. Prenos upravljavcu v tretji državi je skladno s členom 6 možen, če:

- je podana osebna privolitev posameznika, na katerega se nanašajo osebni podatki,
- obdelava je potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik,
- mu to nalaga zakon,
- obdelava je potrebna za zaščito življenjskih interesov posameznika,
- obdelava je potrebna zaradi opravljanja nalog v javnem interesu ali pri izvajanju javne oblasti,
- obdelava je potrebna zaradi zakonitih interesov, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika.

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 prenos potreben za izpolnitev pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem osebnih podatkov, oziroma, ker je prenos potreben za sklenitev ali izvršitev pogodbe s tretjo stranko, ki je v korist posameznika.

[9] Za več informacij o veljavni privolitvi vas napotujemo na svojo spletno stran: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/privolitev.

Če nobeden od zgoraj navedenih pogojev ni izpolnjen, lahko podjetje materinski družbi posreduje osebne podatke le kot **obdelovalcu,** pri čemer mora z materinsko družbo skleniti pogodbo o obdelavi iz člena 28 Splošne uredbe o varstvu podatkov, v kateri upravljavec in obdelovalec uredita svoje razmerje ter določita medsebojne obveznosti in dolžnosti glede obdelave osebnih podatkov. 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.

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

Ker bodo podatki hranjeni na Nizozemskem, torej v okviru EGP, tu **ne gre za prenos 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. 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 obdelovalec, mora slovenski upravljavec s takšno pravno osebo skleniti pogodbo iz člena 28 Splošne uredbe o varstvu podatkov.

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

Združene države Amerike so bile sicer leta 2016 na podlagi sklepa Evropske Komisije uvrščene na listo tretjih držav, ki zagotavljajo ustrezno raven varstva osebnih podatkov, in sicer ko gre za osebne podatke, ki se prenašajo v okviru zasebnostnega ščita EU-ZDA (*Privacy Shield*), vendar pa je bil ta sklep na podlagi sodbe Sodišča EU v zadevi Schrems II (C-311/18 z dne 16. 7. 2020)[10] razveljavljen, zato velja, da **ZDA v celoti ponovno sodijo med tretje države**. To pomeni, da se lahko prenosi podatkov v ZDA vršijo le na podlagi ustreznih zaščitnih ukrepov iz člena 46 Splošne uredbe o varstvu podatkov (npr. na podlagi standardnih pogodbenih klavzul ali zavezujočih poslovnih pravil), oziroma če je to ustrezno tudi na podlagi katerih od izjem iz člena 49 Splošne uredbe o varstvu podatkov.

Ob tem je izvoznik podatkov dolžan oceniti, ali bo prenesenim podatkom zagotovljena **v bistvu enakovredna raven varstva podatkov tej v EU**. Izvoznik podatkov mora preučiti relevantno zakonodajo in prakso javnih organov v ZDA in oceniti, ali morebitni dostopi javnih organov do prenesenih podatkov presegajo to, kar je sprejemljivo po pravu EU. V takem primeru lahko izvoznik prenese podatke le pod pogojem, da je mogoče z **dopolnilnimi zaščitnimi ukrepi** zagotoviti enakovredno raven varstva podatkov. Kako opraviti navedeno oceno in kaj so dopolnilni zaščitni ukrepi, si preberite v *Priporočilih 01/2020 o ukrepih, ki dopolnjujejo orodja za prenos, da se zagotovi skladnost z v EU zagotovljenim varstvom osebnih podatkov*:

- https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en;

in v *Priporočilih 02/2020 Evropskega odbora za varstvo podatkov glede evropskih bistvenih jamstev*:

- https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_sl.pdf.

[10] Sodba Sodišča EU v zadevi Schrems II z dne 16. 7. 2020: http://curia.europa.eu/juris/document/document.jsf;jsessionid=93A4164B11548C6349307CAAFB9860AC?text=&docid=228677&pageIndex=0&doclang=sl&mode=lst&dir=&occ=first&part=1&cid=9823840.

8.7. 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 prenos podatkov v tretjo državo.

Prenos lahko opravite na podlagi ustreznih zaščitnih ukrepov (člen 46 Splošne uredbe o varstvu podatkov), lahko npr. uporabite standardne pogodbene klavzule (glej odgovor na prejšnje vprašanje). Lahko pa sestavite tudi svojo pogodbo med izvoznikom in uvoznikom podatkov (točka a člena 46(3) Splošne uredbe o varstvu podatkov), vendar je v takem primeru potrebno pridobiti predhodno dovoljenje Informacijskega pooblaščenca. Ob tem je treba tudi oceniti, ali relevantna zakonodaja in praksa javnih organov v Indiji predstavlja v bistvu enakovredno raven varstva podatkov tej v EU (glej odgovor na prejšnje vprašanje).

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

Kitajska ni na seznamu držav Evropske komisije ali Informacijskega pooblaščenca, ki zagotavljajo ustrezno raven varstva osebnih podatkov, kar pomeni, da se je za prenos podatkov potrebno poslužiti ustreznih zaščitnih ukrepov iz člena 46 Splošne uredbe o varstvu podatkov. V konkretnem primeru bi vam svetovali, da kot turistična agencija s hotelom na Kitajskem sklenete pogodbo, ki je sestavljena iz **splošnih pogodbenih klavzul**. Na takšen način lahko uredite medsebojna razmerja glede varstva osebnih podatkov in na podlagi pogodbe (in v mejah pogodbenih določil) prenašate podatke svojih strank hotelu na Kitajskem. Vse to lahko storite **brez posebnega dovoljenja Informacijskega pooblaščenca**. Ob tem je treba tudi oceniti, ali relevantna zakonodaja in praksa javnih organov na Kitajskem predstavlja v bistvu enakovredno raven varstva podatkov tej v EU (glej odgovor na vprašanje pod št. 8.6).

Druga možnost pa je prenos podatkov v tretjo državo v skladu z določbami člena 49 Splošne uredbe o varstvu podatkov, ki ureja **odstopanja v posebnih primerih**.

V konkretnem primeru bi pravno podlago lahko prestavljala točka b člena 49, ki omogoča odstopanje, če je prenos potreben **za izvajanje pogodbe** med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem ali **za izvajanje predpogodbenih ukrepov**, sprejetih na zahtevo posameznika, na katerega se nanašajo osebni podatki. Ta opcija bi prišla v poštev v primeru, da gre za **občasen prenos** med subjektoma, ki sicer nimata vzpostavljenega poslovnega odnosa, ter mora biti tak prenos **nujen za izvajanje pogodbe oz. pred-pogodbenih ukrepov**. 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 **izrecne privolitve**, pod pogojem, da bi jih seznanili s posledicami in z morebitnimi tveganji takega posredovanja (točka a člena 49).

Vsekakor pa je treba poudariti, da lahko pravno podlago za prenos predstavljajo določbe člena 49 **le pod pogojem, da v konkretnem primeru ni mogoče zagotoviti ustreznih zaščitnih ukrepov iz člena 46**, saj gre za odstopanja v posebnih primerih. Napotujemo vas, da si preberete **smernice o odstopanjih iz člena 49**, ki jih je sprejel Evropski odbor za varstvo podatkov:

- https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_sl.pdf.

8.9. 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 (za vaše kliente), ki v imenu in za račun stranke (upravljavca) hrani njene podatke. **Splošna uredba o varstvu podatkov obdelovalcu ne dovoljuje, da samovoljno podatke posreduje v obdelavo tretji stranki – podobdelovalcu (torej upravljavcu strežnika v Indiji), temveč mora to s splošnim ali posebnim pisnim dovoljenjem odobriti upravljavec.** Kot obdelovalec morate skleniti pogodbo o obdelavi podatkov po členu 28 Splošne uredbe o varstvu podatkov z upravljavcem. Poleg tega pa vaše podjetje v opisanem primeru prenaša podatke v Indijo in je zato potrebno zagotoviti ustrezne zaščitne ukrepe za takšen prenos. Ena izmed opcij je, da vaše podjetje kot obdelovalec podatkov sklene standardne pogodbene klavzule s podobdelovalcem v Indiji, namreč klavzule lahko po novem sklene tudi obdelovalec kot izvoznik podatkov.

Za več informacij glej vprašanja št. 8.6, 8.7, več informacij glede pogodbene obdelave pa lahko pridobite v Smernicah IP o pogodbeni obdelavi:

- https://www.ip-rs.si/publikacije/priro%C4%8Dniki-in-smernice/smernice-po-splo%C5%A1ni-uredbi-o-varstvu-podatkov-gdpr/smernice-o-pogodbeni-obdelavi.

8.10. 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 svetujemo, da s pogodbenim partnerjem podpišete **standardne pogodbene klavzule, ki vsebujejo določilo o pod-obdelavi v tretji državi. Druga opcija pa je, da vse tri stranke podpišete standardne pogodbene klavzule**, namreč s pogodbo se lahko zaveže več strank in to tudi kasneje.

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 prenosom oz. posredovanjem osebnih podatkov z obdelovalcem osebnih podatkov v tretji državi (uvoznik podatkov) skleniti **standardne pogodbene klavzule** (Modul 2: prenos od upravljavca obdelovalcu), **v katere so že vključene vse pogodbene zahteve v zvezi z obdelavo podatkov iz člena 28(3)**.

1.1) Pogodbeni obdelovalec v tretji državi lahko zatem po prejemu osebnih podatkov od upravljavca oz. izvoznika podatkov odda izvajanje postopkov obdelave osebnih podatkov podobdelovalcu le pod pogoji Iz določila 9 novih Standardnih pogodbenih klavzul. Skladno z navedeno klavzulo mora pogodbeni obdelovalec pred oddajo izvajanja postopkov obdelave pod-obdelovalcu pridobiti **predhodno posebno ali splošno 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**. Obdelovalec mora upravljavcu osebnih podatkov na njegovo zahtevo posredovati poslati izvod pogodbe o pod-obdelavi.

- ALI -

1.2) Druga možnost pa je, da se namesto točke 1.1) **vse tri stranke zavežejo s standardnimi pogodbenimi klavzulami**. Klavzule omogočajo, da se z njimi zaveže več strank in da se lahko stranke tudi kasneje pridružijo na strani uvoznika ali izvoznika podatkov (določilo 7).

8.11. Kdaj gre za prenos podatkov pri računalništvu v oblaku? Na kaj moramo biti pozorni pri ponudnikih oblačnih 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 EU ali EGP, govorimo o prenosu v tretje države.

Če bi recimo ponudnik storitve računalništva v oblaku, ki je sicer ustanovljen in registriran v Kanadi, 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 Kanadi 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 natančen pregled nad tem, kje se bodo podatki hranili, torej ne zgolj to, da bodo hranjeni v oblaku, pač pa tudi, ali bo ponudnik oblaka podatke hranil drugje in kje.

Treba je poudariti, da pogodbe oz. splošni pogoji uporabe, ki jih običajno pripravijo ponudniki storitev računalništva v oblaku, ne zagotavljajo standardov, ki jih glede take vrste prenosa vzpostavlja Splošna uredba o varstvu podatkov, zato **Informacijski pooblaščenec priporoča, da upravljavec iz Slovenije v tem primeru s ponudnikom storitev računalništva v oblaku sklene standardne pogodbene klavzule, ki vsebujejo tudi dogovore v zvezi s »pod-obdelavo« osebnih podatkov s strani ponudnika oblaka**. Informacijski pooblaščenec posebej opozarja, da je sestavni del tovrstnih klavzul (Dodatek 2) tudi konkretiziran dogovor o postopkih in ukrepih za zavarovanje osebnih podatkov. Standardne pogodbene klavzule je potrebno sprejeti v celoti in se jih ne sme spreminjati. **V takšnem primeru upravljavec ne potrebuje posebnega dovoljenja s strani Informacijskega pooblaščenca**. Ob tem pa se je upravljavec predhodno dolžan prepričati, ali zakonodaja in praksa javnih organov v namembni tretji državi zagotavlja **v bistvu enakovredno raven varstva podatkov tej v EGP** oz. ali je treba v ta namen sprejeti **dopolnilne zaščitne ukrepe** (glej poglavje 5.1).

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. V takem primeru je za prenos podatkov potrebno **pridobiti predhodno dovoljenje Informacijskega pooblaščenca.**

Polega tega morate s ponudnikom storitve računalništva v oblaku, ki predstavlja obdelovalca podatkov, skleniti pogodbo o obdelavi iz člena 28 Splošne uredbe o varstvu podatkov in ob tem upoštevati tudi druge pogoje iz navedenega člena. Nove standardne pogodbene klavzule med upravljavcem in obdelovalec že vsebujejo vse pogodbene zahteve iz člena 28(3), kar pomeni, da se lahko to uredi v enoviti pogodbi.

Brez zadostnih informacij glede obdelave osebnih podatkov in zavarovanja, ki ga nudi ponudnik te storitve, tvegate, da bo prišlo do kršitve določb o varstvu osebnih podatkov, kar lahko pomeni vašo odgovornost za kršitev v primeru zlorabe osebnih podatkov (npr. razkritja, izgube, nepooblaščene seznanitve 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.

Računalništvo v oblaku obravnavajo posebne smernice Informacijskega pooblaščenca:

https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_Varstvo_osebnih_podatkov_in_racunalnistvo_v_oblaku_2016.pdf.

9. Zaključek

Prenos osebnih podatkov v tretje države izven EU, pa naj bo to s strani upravljavcev osebnih podatkov ali pa s strani obdelovalcev, 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 ali EGP, in tiste, ki jih posredujejo v tretje države.

V smernicah smo zato na jasen in pregleden način skušali pojasniti ureditev in mehanizme varovanja pri prenosu podatkov v tretje države, ki jih morajo v skladu s Splošno uredbo o varstvu podatkov spoštovati upravljavci osebnih podatkov, med drugim tudi obveznost, kdaj je za prenos podatkov potrebno dovoljenje Informacijskega pooblaščenca in kako ga upravljavci pridobijo. Pojasnili smo tudi, na kakšen način je mogoče podatke prenašati brez vnaprejšnjega dovoljenja Informacijskega 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, kako je s pod-obdelavo osebnih podatkov s strani pogodbenega partnerja in posredovanjem podatkov materinski družbi.

Ob tem izpostavljamo, da za upravljavce (npr. policija), za katere ne velja Splošna uredba o varstvu podatkov, ampak Direktiva (EU) 2016/680, ki ureja varstvo podatkov pri obdelavah za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov, do sprejema novega Zakona o varstvu podatkov v celoti veljajo določbe ZVOP-1.