Translations proofread by EDPB Members.
This language version has not yet been proofread.

Priporočila 01/2020 o ukrepih, ki dopolnjujejo orodja za prenos, za zagotovitev skladnosti z ravnjo varstva osebnih podatkov na ravni EU

Sprejeto 10. novembra 2020

Povzetek

Splošna uredba EU o varstvu podatkov (v nadaljnjem besedilu: Splošna uredba o varstvu podatkov) je bila sprejeta z dvojnim namenom: da bi se z njo omogočil lažji prosti pretok osebnih podatkov v Evropski uniji, hkrati pa ohranile temeljne pravice in svoboščine posameznikov, zlasti njihova pravica do varstva osebnih podatkov.

Sodišče Evropske unije (v nadaljnjem besedilu: Sodišče) nas je v nedavni sodbi v zadevi C-311/18 (Schrems II) opozorilo, da se mora za osebne podatke, ne glede na to, kam se prenesejo, zagotoviti enakovredno varstvo, kot se zanje zagotavlja v Evropskem gospodarskem prostoru (EGP). S prenosom osebnih podatkov v tretje države se ne sme ogroziti ali zmanjšati varstvo, ki se jim zagotavlja v EGP. Sodišče to zagovarja tudi s pojasnilom, da se ne zahteva, da je raven varstva v tretjih državah enaka ravni, ki se zagotavlja v EGP, temveč da je v bistvu enakovredna. Zagovarja tudi veljavnost standardnih pogodbenih določil kot orodja za prenos, ki se lahko uporablja za pogodbeno zagotavljanje v bistvu enakovredne ravni varstva podatkov, prenesenih v tretje države.

Standardna pogodbena določila in druga orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov se ne uporabljajo ločeno. Sodišče navaja, da so upravljavci ali obdelovalci kot izvozniki odgovorni, da za vsak primer posebej, po potrebi v sodelovanju z uvoznikom v tretji državi, preverijo, ali pravo ali praksa tretje države posega v učinkovitost ustreznih zaščitnih ukrepov, ki jih vsebujejo orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov. V teh primerih Sodišče še vedno dopušča možnost, da izvozniki izvedejo dopolnilne ukrepe, s katerimi zapolnijo te vrzeli v varstvu in ga zagotovijo na ravni, ki jo zahteva pravo EU. Sodišče ne navaja, kateri ukrepi bi to lahko bili. Poudarja pa, da jih morajo izvozniki opredeliti za vsak primer posebej. To je v skladu z načelom odgovornosti iz člena 5(2) Splošne uredbe o varstvu podatkov, ki določa, da morajo biti upravljavci odgovorni za skladnost z načeli Splošne uredbe o varstvu podatkov, ki se nanašajo na obdelavo osebnih podatkov, ter sposobni to skladnost dokazati.

Evropski odbor za varstvo podatkov (EOVP) je sprejel ta priporočila, da bi pomagal izvoznikom (ki so lahko upravljavci ali obdelovalci, zasebni subjekti ali javni organi, ki obdelujejo osebne podatke v okviru področja uporabe Splošne uredbe o varstvu podatkov) pri kompleksni nalogi ocenjevanja tretjih držav in po potrebi opredelitvi ustreznih dopolnilnih ukrepov. Ta priporočila izvoznikom zagotavljajo zaporedje korakov, ki naj jih izvedejo, morebitne vire informacij in nekaj primerov dopolnilnih ukrepov, ki bi jih bilo mogoče uvesti.

Kot **prvi korak** vam EOVP kot izvoznikom svetuje, da **preučite svoje prenose**. Evidentiranje vseh prenosov osebnih podatkov v tretje države je lahko zahtevna naloga. Da bi se za osebne podatke zagotovila v bistvu enakovredna raven varstva ne glede na to, kje se obdelujejo, je treba vedeti, kam se prenesejo. Preveriti morate tudi, ali so podatki, ki jih prenesete, ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se prenesejo in obdelujejo v tretji državi.

Drugi korak je, da **preverite, ali je orodje za prenos, na katerega se opirate pri svojem prenosu**, navedeno v poglavju V Splošne uredbe o varstvu podatkov. Če je Evropska komisija državo, regijo ali sektor, kamor prenesete podatke, razglasila kot ustrezen v enem od svojih sklepov o ustreznosti v skladu s členom 45 Splošne uredbe o varstvu podatkov ali prejšnjo Direktivo 95/46 in če sklep še velja, vam ni treba izvesti nadaljnjih korakov, razen da spremljate veljavnost sklepa o ustreznosti. Če sklep o ustreznosti ni bil sprejet, se morate za prenose, ki so redni in ponavljajoči, opreti na eno od orodij za prenos iz člena 46 Splošne uredbe o varstvu podatkov. Samo v nekaterih primerih občasnih in neponavljajočih se prenosov se lahko, če izpolnjujete pogoje, oprete na eno od odstopanj iz člena 49 Splošne uredbe o varstvu podatkov.

Tretji korak je, da **ocenite**, ali v okviru vašega konkretnega prenosa morda kar koli v **pravu ali praksi tretje države** posega v učinkovitost ustreznih zaščitnih ukrepov v orodjih za prenos, na katera se opirate. Vaša ocena naj bo v prvi vrsti osredotočena na zakonodajo tretje države, ki je pomembna za vaš prenos in orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov, na katerega se opirate, in ki lahko ogrozi raven njegovega varstva. Za oceno elementov, ki jih je treba upoštevati pri oceni prava tretje države, ki obravnava dostop javnih organov do podatkov za namene nadzora, glej priporočila EOVP iz evropskih bistvenih jamstev. To naj se zlasti skrbno preuči, kadar zakonodaja, ki ureja dostop javnih organov do podatkov, ni jasna ali javno dostopna. Če ni zakonodaje, ki bi urejala okoliščine, v katerih imajo javni organi dostop do osebnih podatkov, in še vedno želite opraviti prenos, preučite druge zadevne in objektivne dejavnike ter se ne opirajte na subjektivne dejavnike, kot je verjetnost dostopa javnih organov do vaših podatkov na način, ki ni v skladu s standardi EU. To oceno opravite s potrebno skrbnostjo in jo temeljito dokumentirajte, ker boste odgovorni za odločitev, ki jo boste morda sprejeli na tej podlagi.

Četrti korak je, da **opredelite in sprejmete dopolnilne ukrepe**, potrebne za zagotovitev ravni varstva prenesenih podatkov, ki je enakovredna standardu EU glede bistvene enakovrednosti. Ta korak je potreben samo, če vaša ocena razkrije, da zakonodaja tretje države posega v učinkovitost orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov, na katerega se opirate ali se nameravate opreti v okviru svojega prenosa. Ta priporočila vsebujejo (v Prilogi 2) neizčrpen seznam primerov dopolnilnih ukrepov z nekaterimi pogoji za njihovo učinkovitost. Tako kot ustrezni zaščitni ukrepi, ki jih vsebujejo orodja za prenos iz člena 46, so lahko tudi nekateri dopolnilni ukrepi učinkoviti v nekaterih državah, ne pa nujno tudi v drugih. Odgovorni ste za oceno njihove učinkovitosti v okviru prenosa ter glede na pravo tretje države in orodja za prenos, na katerega se opirate, prav tako pa ste odgovorni za odločitev, ki jo sprejmete. To lahko od vas zahteva tudi, da združite več dopolnilnih ukrepov. Na koncu boste morda ugotovili, da z nobenim dopolnilnim ukrepom ni mogoče zagotoviti v bistvu enakovredne ravni varstva za vaš konkretni prenos. V primerih, kadar noben dopolnilni ukrep ni primeren, se morate prenosu izogniti, ga začasno ustaviti ali ga prenehati, da preprečite ogrožanje ravni varstva osebnih podatkov. Tudi to oceno dopolnilnih ukrepov morate opraviti s potrebno skrbnostjo in jo dokumentirati.

Peti korak je, da **sprejmete** kateri koli **formalni postopkovni korak**, ki je morda potreben za sprejetje vašega dopolnilnega ukrepa glede na orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov, na katerega se opirate. V teh priporočilih so navedene te formalnosti. O nekaterih od njih se boste morda morali posvetovati s svojimi pristojnimi nadzornimi organi.

Vaš **šesti in končni korak** bo, da v ustreznih časovnih razmikih znova ocenite raven varstva, zagotovljeno za podatke, ki jih prenesete v tretje države, ter spremljate, ali je bil oziroma bo kakršen koli razvoj dogodkov, ki lahko vpliva nanjo. Načelo odgovornosti zahteva stalno pozornost pri spremljanju ravni varstva osebnih podatkov.

Nadzorni organi bodo še naprej izvajali svoja pooblastila za spremljanje uporabe Splošne uredbe o varstvu podatkov in jo uveljavljali. Še naprej bodo ustrezno preučili ukrepe, ki jih izvozniki sprejmejo za zagotovitev, da bi se za podatke, ki jih prenesejo, zagotovila v bistvu enakovredna raven varstva. Kot opozarja Sodišče, bodo nadzorni organi začasno ustavili ali prepovedali prenose podatkov v primerih, kadar bodo po preiskavi ali pritožbi ugotovili, da v bistvu enakovredne ravni varstva ni mogoče zagotoviti.

Nadzorni organi bodo še naprej pripravljali smernice za izvoznike in usklajevali njihove ukrepe v EOVP, da bi se zagotovila skladnost pri uporabi prava EU o varstvu podatkov.

Kazalo

1 Odgovornost pri prenosu podatkov 7

2 Načrt: uporaba načela odgovornosti za prenose podatkov v praksi 8

2.1 Korak 1: Preučite svoje prenose 8

2.2 Korak 2: Opredelite orodja za prenos, na katera se opirate 9

2.3 Korak 3: Ocenite, ali je orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov, na katerega se opirate, učinkovito glede na vse okoliščine prenosa 12

2.4 Korak 4: Sprejmite dopolnilne ukrepe 15

2.5 Korak 5: Postopkovni koraki, če ste opredelili učinkovite dopolnilne ukrepe 17

2.6 Korak 6: Oceno ponovno izvedite v ustreznih časovnih razmikih 19

3 Sklepna ugotovitev 20

PRILOGA 1: OPREDELITEV POJMOV 21

PRILOGA 2: PRIMERI DOPOLNILNIH UKREPOV 22

Tehnični ukrepi 22

Dodatni pogodbeni ukrepi 28

Organizacijski ukrepi 35

PRILOGA 3: MOŽNI VIRI INFORMACIJ ZA OCENO TRETJE DRŽAVE 39

Evropski odbor za varstvo podatkov je –

ob upoštevanju člena 70(1)(e) 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 (v nadaljnjem besedilu: Splošna uredba o varstvu podatkov),

ob upoštevanju Sporazuma o Evropskem gospodarskem prostoru (EGP) ter zlasti Priloge XI in Protokola 37 k Sporazumu, kakor je bil spremenjen s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018[1],

ob upoštevanju členov 12 in 22 svojega poslovnika,

ob upoštevanju naslednjega:

(1) Sodišče Evropske unije (v nadaljnjem besedilu: Sodišče) je v sodbi z dne 16. julija 2020 v zadevi *Data Protection Commissioner proti Facebook Ireland LTD, Maximillian Schrems,* C-311/18, sklenilo, da je treba člen 46(1) in člen 46(2)(c) Splošne uredbe o varstvu podatkov razlagati tako, da je treba z ustreznimi zaščitnimi ukrepi, izvršljivimi pravicami in učinkovitimi pravnimi sredstvi, ki se zahtevajo s tema določbama, zagotoviti, da je osebam, katerih osebni podatki se prenesejo v tretjo državo na podlagi standardnih določil o varstvu podatkov, zagotovljena raven varstva, ki je v bistvu enakovredna ravni varstva, ki se v Evropski uniji zagotavlja s to uredbo v povezavi z Listino Evropske unije o temeljnih pravicah.[2]

(2) Kot je poudarilo Sodišče, je treba posameznikom zagotoviti raven varstva, ki je v bistvu enakovredna ravni, ki se v Evropski uniji zagotavlja s Splošno uredbo o varstvu podatkov v povezavi z Listino, ne glede na določbo poglavja V, na podlagi katere se izvaja prenos osebnih podatkov v tretjo državo. Namen določb poglavja V je zagotavljati kontinuiteto te visoke ravni varstva pri prenosu osebnih podatkov v tretjo državo.[3]

(3) Uvodna izjava 108 in člen 46(1) Splošne uredbe o varstvu podatkov določata, da če sklep EU o ustreznosti ni sprejet, bi moral upravljavec ali obdelovalec sprejeti ukrepe, na podlagi katerih pomanjkanje varstva podatkov v tretji državi nadomesti z ustreznimi zaščitnimi ukrepi za posameznika, na katerega se nanašajo osebni podatki. Upravljavec ali obdelovalec lahko zagotovi ustrezne zaščitne ukrepe, za kar ne potrebuje posebnega dovoljenja nadzornega organa, in sicer z uporabo enega od orodij za prenos iz člena 46(2) Splošne uredbe o varstvu podatkov, kot so standardna določila o varstvu podatkov.

[1] Sklice na „države članice“ v teh priporočilih je treba razumeti kot sklice na „države članice EGP“.
[2] Sodba Sodišča z dne 16. julija 2020, *Data Protection Commissioner proti Facebook Ireland Ltd, Maximillian Schrems (v nadaljnjem besedilu:* C-311/18 (Schrems II)), druga ugotovitev.
[3] C-311/18 (Schrems II), točki 92 in 93.

(4) Sodišče pojasni, da je namen standardnih določil o varstvu podatkov, ki jih je sprejela Komisija, zgolj zagotoviti upravljavcem in obdelovalcem s sedežem v Uniji pogodbena jamstva, ki se enotno uporabljajo v vseh tretjih državah. Iz pogodbene narave standardnih določil o varstvu podatkov izhaja, da ta določila ne morejo zavezovati javnih organov tretjih držav, saj ti niso pogodbena stranka. Izvozniki podatkov morajo zato morda jamstva iz teh standardnih določil o varstvu podatkov dopolniti z dopolnilnimi ukrepi, da zagotovijo skladnost z ravnjo varstva, ki se z vidika prava EU zahteva v določeni tretji državi. Sodišče se sklicuje na uvodno izjavo 109 Splošne uredbe o varstvu podatkov, v kateri je navedena ta možnost, ter upravljavce in obdelovalce spodbuja k njeni uporabi.[4]

(5) Sodišče je navedlo, da mora izvoznik podatkov za vsak primer posebej in po potrebi v sodelovanju z uvoznikom podatkov predvsem preveriti, ali pravo namembne tretje države z vidika prava EU zagotavlja v bistvu enakovredno raven varstva osebnih podatkov, prenesenih na podlagi standardnih določil o varstvu podatkov, pri čemer po potrebi zagotovi dopolnilne ukrepe k ukrepom iz teh določil.[5]

(6) Če upravljavec ali obdelovalec s sedežem v Evropski uniji ne more sprejeti ustreznih dopolnilnih ukrepov za zagotovitev v bistvu enakovredne ravni varstva z vidika prava EU, mora sam ali, podredno, pristojni nadzorni organ začasno ustaviti ali prenehati prenos osebnih podatkov v zadevno tretjo državo.[6]

(7) Splošna uredba o varstvu podatkov in Sodišče ne opredeljujeta ali navajata „dodatnih zaščitnih ukrepov“, „dodatnih ukrepov“ ali „dopolnilnih ukrepov“ k zaščitnim ukrepom v orodjih za prenos iz člena 46(2) Splošne uredbe o varstvu podatkov, ki jih lahko upravljavci in obdelovalci sprejmejo za zagotovitev skladnosti z ravnjo varstva, ki se z vidika prava EU zahteva v določeni tretji državi.

(8) EOVP se je na svojo pobudo odločil, da preuči to vprašanje ter za upravljavce in obdelovalce kot izvoznike pripravi priporočila o postopku, po katerem lahko opredelijo in sprejmejo dopolnilne ukrepe. Namen teh priporočil je izvoznikom zagotoviti metodologijo, po kateri določijo, ali bi morali za svoje prenose uvesti dodatne ukrepe in katere. Primarna odgovornost izvoznikov je zagotoviti, da se za prenesene podatke v tretji državi zagotavlja raven varstva, ki je v bistvu enakovredna ravni, ki se zanje zagotavlja v EU. S temi priporočili želi EOVP v skladu s svojimi pooblastili spodbuditi dosledno uporabo Splošne uredbe o varstvu podatkov in sodbe Sodišča[7] –

SPREJEL NASLEDNJE PRIPOROČILO:

[4] C-311/18 (Schrems II), točki 132 in 133.
[5] C-311/18 (Schrems II), točka 134.
[6] C-311/18 (Schrems II), točka 135.
[7] Člen 70(1)(e) Splošne uredbe o varstvu podatkov.

1 ODGOVORNOST PRI PRENOSU PODATKOV

1. Primarno pravo EU obravnava pravico do varstva podatkov kot temeljno pravico.[8] Pravici do varstva podatkov se zato zagotavlja visoka raven zaščite, omejitve pa so dovoljene samo, če jih predvideva zakonodaja, če spoštujejo bistvo pravice ter če so sorazmerne, potrebne in dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali če so potrebne zaradi zaščite pravic in svoboščin drugih.[9] Pravica do varstva osebnih podatkov ni absolutna pravica; v skladu z načelom sorazmernosti jo je treba obravnavati glede na vlogo, ki jo ima v družbi, in jo uravnotežiti z drugimi temeljnimi pravicami.[10]

2. Z podatke, ki se prenesejo v tretje države zunaj EGP, je treba zagotoviti raven varstva, ki je v bistvu enakovredna ravni varstva, zagotovljeni v EU, s čimer se zagotovi, da ni ogrožena raven varstva, ki jo zagotavlja Splošna uredba o varstvu podatkov.

3. Pravica do varstva osebnih podatkov je aktivna pravica. Od izvoznikov in uvoznikov (kot upravljavcev in/ali obdelovalcev) zahteva več kot samo njeno priznanje ali pasivno spoštovanje.[11] Upravljavci in obdelovalci si morajo dejavno in nenehno prizadevati za spoštovanje pravice do varstva podatkov z izvajanjem pravnih, tehničnih in organizacijskih ukrepov, ki zagotavljajo njegovo učinkovitost. Poleg tega morajo biti sposobni ta prizadevanja dokazati posameznikom, na katere se nanašajo osebni podatki, splošni javnosti in nadzornim organom za varstvo podatkov. To je tako imenovano načelo odgovornosti.[12]

4. Načelo odgovornosti, potrebno za zagotavljanje učinkovite uporabe ravni varstva, ki ga podeljuje Splošna uredba o varstvu podatkov, se uporablja tudi za prenose podatkov v tretje države[13], ker so ti sami po sebi oblika obdelave podatkov.[14] Kot je v sodbi poudarilo Sodišče, je treba zagotoviti raven varstva, ki je v bistvu enakovredna rani varstva, ki se v Evropski uniji zagotavlja s Splošno uredbo o varstvu podatkov v povezavi z Listino, in sicer ne glede na določbo navedenega poglavja, na podlagi katere se izvaja prenos osebnih podatkov v tretjo državo.[15]

5. V sodbi Schrems II Sodišče poudarja odgovornosti izvoznikov in uvoznikov, da zagotovijo, da se je obdelava osebnih podatkov izvajala in se bo še naprej izvajala v skladu z ravnjo varstva, ki jo določa pravo EU o varstvu podatkov, ter da začasno ustavijo prenos podatkov in/ali odstopijo od pogodbe, če uvoznik podatkov ni ali ni več sposoben spoštovati standardnih določil o varstvu podatkov, vključenih v zadevno pogodbo med izvoznikom in uvoznikom.[16] Upravljavec ali obdelovalec mora kot izvoznik zagotoviti, da uvozniki pri izpolnjevanju teh odgovornosti po potrebi sodelujejo z izvoznikom, tako da ga sproti obveščajo na primer o vsakem razvoju dogodkov, ki vpliva na raven varstva prejetih osebnih

[8] Člen 8(1) Listine o temeljnih pravicah in člen 16(1) PDEU, uvodna izjava 1, člen 1(2) Splošne uredbe o varstvu podatkov.
[9] Člen 52(1) Listine EU o temeljnih pravicah.
[10] Uvodna izjava 4 Splošne uredbe o varstvu podatkov in sodba v zadevi Google LLC, successor in law to Google Inc. proti Commission nationale de l'informatique et des libertés (CNIL), C-507/17, točka 60.
[11] C-92/09 in C-93/02, Volker und Markus Schecke GbR proti Land Hessen, mnenje generalne pravobranilke Eleanor Sharpston z dne 17. junija 2010, točka 71.
[12] Člen 5(2) in člen 28(3)(h) Splošne uredbe o varstvu podatkov.
[13] Člen 44, uvodna izjava 101 in člen 47(2)(d) Splošne uredbe o varstvu podatkov.
[14] Sodba Sodišča z dne 6. oktobra 2015, *Maximillian Schrems proti Data Commissioner (v nadaljnjem besedilu:* C-362/14, (Schrems I)), točka 45.
[15] C-311/18 (Schrems II), točki 92 in 93.
[16] C-311/18 (Schrems II), točke 134, 135, 139, 140, 141, 142.

podatkov v državi uvoznika.[17] Te odgovornosti pomenijo uporabo načela odgovornosti iz Splošne uredbe o varstvu podatkov za prenose podatkov.[18]

2 NAČRT: UPORABA NAČELA ODGOVORNOSTI ZA PRENOSE PODATKOV V PRAKSI

6. V nadaljevanju je naveden načrt korakov, ki jih morate izvesti, da bi ugotovili, ali morate (kot izvoznik podatkov) uvesti dopolnilne ukrepe, da boste lahko podatke zakonito prenesli iz EGP. „Vi“ v tem dokumentu pomeni upravljavca ali obdelovalca kot izvoznika podatkov, ki obdeluje osebne podatke v okviru področja uporabe Splošne uredbe o varstvu podatkov – vključno z obdelavo s strani zasebnih subjektov in javnih organov pri prenosu podatkov zasebnim organom.[19] Tako kot za prenose osebnih podatkov med javnimi organi, so tudi *za prenose osebnih podatkov med javnimi organi v EGP in zunaj EGP v Smernicah 2/2020 o členu 46(2)(a) in členu 46(3)(b) Uredbe 2016/679 na voljo posebne smernice*.[20]

7. To oceno ter dopolnilne ukrepe, ki jih izberete in izvedete, morate ustrezno dokumentirati in to dokumentacijo pa na zahtevo dati na voljo pristojnemu nadzornemu organu.[21]

2.1 Korak 1: Preučite svoje prenose

8. Da bi vedeli, kaj se lahko zahteva za vas (kot izvoznika podatkov), da bi lahko še naprej prenašali osebne podatke ali izvajali nove prenose osebnih podatkov[22], je prvi korak, da zagotovite, da ste v celoti seznanjeni s svojimi prenosi (preučite svoje prenose). Beleženje in evidentiranje vseh prenosov je lahko kompleksna naloga za subjekte, ki izvajajo večkratne, različne in redne prenose v tretje države ter uporabljajo več obdelovalcev in podobdelovalcev. Preučitev svojih prenosov je v bistvu vaš prvi korak za izpolnitev obveznosti v skladu z načelom odgovornosti.

9. Za zagotovitev popolne seznanjenosti s svojimi prenosi se lahko oprete na evidenco dejavnosti obdelave, ki jo morate kot upravljavec ali obdelovalec morda voditi v skladu s členom 30 Splošne uredbe o varstvu podatkov.[23] Pomagajo vam lahko tudi predhodni ukrepi za izpolnitev obveznosti obveščanja posameznikov, na katere se nanašajo osebni podatki, v skladu s členom 13(1)(f) in

[17] C-311/18 (Schrems II), točka 134.
[18] Člen 5(2) in člen 28(3)(h) Splošne uredbe o varstvu podatkov.
[19] Glej Smernice 3/2018 Evropskega odbora za varstvo podatkov o ozemeljski veljavnosti Splošne uredbe o varstvu podatkov (člen 3); https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_sl.
[20] Smernice 2/2020 Evropskega odbora za varstvo podatkov o členu 46(2)(a) in členu 46(3)(b) Uredbe 2016/679 za prenose osebnih podatkov med javnimi organi v EGP in zunaj EGP; glej https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_sl.
[21] Člen 5(2) in člen 24(1) Splošne uredbe o varstvu podatkov.
[22] Upoštevajte, da se oddaljeni dostop do podatkov v EGP s strani subjekta iz tretje države prav tako šteje za prenos.
[23] Glej člen 30 Splošne uredbe o varstvu podatkov, zlasti odstavka 1(e) in 2(c). Vaša evidenca obdelave naj vsebuje tudi opis vaših dejavnosti obdelave (med drugim vključno s kategorijami posameznikov, na katere se nanašajo osebni podatki, kategorijami osebnih podatkov in nameni obdelave ter specifičnimi informacijami o prenosih podatkov). Nekateri upravljavci in obdelovalci so izvzeti iz obveznosti vodenja evidence obdelave (člen 30(5) Splošne uredbe o varstvu podatkov). Za smernice o tej izjemi glej dokument o stališču Delovne skupine iz člena 29 o odstopanjih od obveznosti vodenja evidence dejavnosti obdelave v skladu s členom 30(5) Splošne uredbe o varstvu podatkov (potrdil EOVP 25. maja 2018).

členom 14(1)(f) Splošne uredbe o varstvu podatkov o vaših prenosih njihovih osebnih podatkov v tretje države.[24]

10. Pri evidentiranju prenosov ne pozabite upoštevati tudi nadaljnjih prenosov, na primer, ali vaši obdelovalci zunaj EGP prenesejo osebne podatke, ki ste jim jih zaupali, podobdelovalcu v drugi tretji državi ali isti tretji državi[25].

11. V skladu z načelom „najmanjšega obsega podatkov“ iz Splošne uredbe o varstvu podatkov[26] morate tudi preveriti, ali so podatki, ki jih prenesete, ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se prenesejo in obdelujejo v tretji državi.

12. Te dejavnosti se morajo izvesti pred vsakim prenosom in posodobiti pred nadaljevanjem prenosov po začasni ustavitvi prenosov podatkov: vedeti morate, kje so lahko osebni podatki, ki ste jih izvozili, oziroma kje jih uvozniki lahko obdelujejo (zemljevid namembnih krajev).

13. Upoštevajte, da se tudi oddaljeni dostop iz tretje države (npr. v podpornih primerih) in/ali hramba v oblaku zunaj EGP štejeta za prenos.[27] Konkretneje, če uporabljate mednarodno infrastrukturo v oblaku, morate oceniti, ali se bodo vaši podatki prenesli v tretje države in kam, razen če ponudnik storitev v oblaku v pogodbi jasno navede, da se podatki v tretjih državah sploh ne bodo obdelovali.

2.2 Korak 2: Opredelite orodja za prenos, na katera se opirate

14. V drugem koraku, ki ga morate izvesti, med orodji za prenos, navedenimi in predvidenimi v poglavju V Splošne uredbe o varstvu podatkov, opredelite tista, na katera se opirate.

Sklepi o ustreznosti

15. Evropska komisija lahko s **sklepi o ustreznosti**, ki se nanašajo na nekatere ali vse tretje države, v katere prenesete osebne podatke, prizna, da zagotavljajo ustrezno raven varstva osebnih podatkov.[28]

16. S takim sklepom o ustreznosti se omogoči pretok osebnih podatkov iz EGP v zadevno tretjo državo, ne da bi bilo potrebno orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov.

[24] V skladu s pravili o preglednosti iz Splošne uredbe o varstvu podatkov morate posameznike, na katere se nanašajo osebni podatki, obvestiti o prenosih osebnih podatkov v tretje države (člen 13(1)(f) in člen 14(1)(f) Splošne uredbe o varstvu podatkov). Obvestiti jih morate zlasti, ali je Evropska komisija sprejela sklep o ustreznosti ali ne, pri prenosih iz člena 46, 47 ali drugega pododstavka člena 49(1) Splošne uredbe o varstvu podatkov pa se morate sklicevati na ustrezne ali primerne zaščitne ukrepe in sredstva za pridobitev njihove kopije ali navesti, kje so bila dana na voljo. Informacije, zagotovljene posamezniku, na katerega se nanašajo osebni podatki, morajo biti točne in veljavne, zlasti ob upoštevanju sodne prakse Sodišča v zvezi s prenosi.

[25] Če je upravljavec izdal predhodno posebno ali splošno pisno dovoljenje v skladu s členom 28(2) Splošne uredbe o varstvu podatkov.

[26] Člen 5(1)(c) Splošne uredbe o varstvu podatkov.

[27] Glej pogosto zastavljena vprašanja, št. 11 „*opozoriti je treba, da tudi zagotovitev dostopa do podatkov iz tretje države, na primer za upravne namene, pomeni prenos*“, EOVP, Pogosto zastavljena vprašanja v zvezi s sodbo Sodišča Evropske unije z dne 23. julija 2020, Data Protection Commissioner proti Facebook Ireland Ltd in Maximillianu Schremsu, C-311/18.

[28] Evropska komisija je pooblaščena, da v skladu s členom 45 Splošne uredbe o varstvu podatkov presodi, ali država zunaj EU zagotavlja ustrezno raven varstva podatkov. Prav tako je pooblaščena, da presodi, ali mednarodna organizacija zagotavlja ustrezno raven varstva.

17. Sklepi o ustreznosti lahko zajemajo državo kot celoto ali pa so omejeni na njen del. Zajemajo lahko vse prenose podatkov v neko državo ali pa so omejeni na nekatere vrste prenosov (npr. v en sektor).[29]

18. Evropska komisija objavi seznam svojih sklepov o ustreznosti na svojem spletišču.[30]

19. Če prenesete osebne podatke v tretje države, regije ali sektorje, ki jih zajema sklep Komisije o ustreznosti (v veljavnem obsegu), **vam ni treba opraviti nobenih nadaljnjih korakov, kot so opisani v teh priporočilih.**[31] Še vedno pa morate spremljati, ali so bili sklepi o ustreznosti, ki veljajo za vaše prenose, preklicani ali razveljavljeni.[32]

20. Vendar sklepi o ustreznosti posameznikom, na katere se nanašajo osebni podatki, ne preprečujejo vložitve pritožbe. Prav tako nadzornim organom ne preprečujejo, da pri nacionalnem sodišču vložijo tožbo, če imajo pomisleke glede veljavnosti sklepa, tako da lahko nacionalno sodišče pred Sodiščem sproži postopek predhodnega odločanja za preučitev te veljavnosti.[33]

Primer: Maximilian Schrems, državljan EU, je junija 2013 pri irski komisiji za varstvo podatkov vložil pritožbo, v kateri je temu nadzornemu organu predlagal, naj prepove ali začasno ustavi prenos njegovih osebnih podatkov iz družbe Facebook Ireland v Združene države, ker je menil, da zakonodaja in praksa v Združenih državah ne zagotavljata zadostnega varstva osebnih podatkov, ki se hranijo na njenem ozemlju, pred dejavnostmi nadzora, ki jih tam izvajajo javni organi. Komisija za varstvo podatkov je pritožbo zavrnila zlasti zato, ker je Evropska komisija v Odločbi 2000/520 menila, da Združene države na podlagi sheme javnega pristana zagotavljajo ustrezno raven varstva prenesenih osebnih podatkov (odločba o varnem pristanu). Maximilian Schrems je odločitev komisije za varstvo podatkov izpodbijal, irsko višje sodišče pa je pred Sodiščem Evropske unije sprožilo postopek za ugotavljanje veljavnosti Odločbe 2000/520. Sodišče se je pozneje odločilo razveljaviti Odločbo Komisije 2000/520/ES o primernosti zaščite, ki jo zagotavljajo načela zasebnosti varnega pristana.[34]

[29] Člen 45(1) Splošne uredbe o varstvu podatkov.

[30] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_sl.

[31] Če ste vi in uvoznik podatkov izvedla ukrepe za izpolnitev drugih obveznosti iz Splošne uredbe o varstvu podatkov; v nasprotnem primeru izvedite navedene ukrepe.

[32] Evropska komisija mora vse sklepe o ustreznosti redno pregledovati in spremljati, ali tretje države, v korist katerih so bili sprejeti sklepi o ustreznosti, še naprej zagotavljajo ustrezno raven varstva (glej člen 45(3) in (4) Splošne uredbe o varstvu podatkov). Sodišče lahko sklepe o ustreznosti tudi razveljavi (glej njegovi sodbi v zadevah C-362/14 (Schrems I) in C-311/18 (Schrems II)).

[33] C-311/18 (Schrems II), točke 118–120. Nadzorni organi ne smejo odločiti za neupoštevanje sklepa o ustreznosti ter začasno ustaviti ali prepovedati prenose osebnih podatkov v take države, pri tem pa navesti samo neustreznost ravni varstva. Svoja pooblastila za začasno ustavitev ali prepoved prenosov osebnih podatkov v zadevno tretjo državo lahko izvajajo samo na podlagi drugih razlogov (npr. zaradi nezadostnih varnostnih ukrepov v nasprotju s členom 32 Splošne uredbe o varstvu podatkov, neobstoja pravne podlage, ki bi veljavno podpirala obdelavo podatkov kot tako, v nasprotju s členom 6 Splošne uredbe o varstvu podatkov). Nadzorni organi lahko popolnoma neodvisno preučijo, ali se pri prenosu teh podatkov izpolnjujejo zahteve iz Splošne uredbe o varstvu podatkov, in po potrebi pri nacionalnih sodiščih vložijo tožbo, zato da ta sodišča, če se strinjajo s pomisleki tega organa glede veljavnosti sklepa Komisije o ustreznosti, pred Evropskim sodiščem sprožijo postopek predhodnega odločanja za preučitev njegove veljavnosti.

[34] Zadeva C-362/14 (Schrems I).

Orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov

21. V členu 46 Splošne uredbe o varstvu podatkov je navedena vrsta orodij za prenos, ki vsebujejo „*ustrezne zaščitne ukrepe*“, ki jih lahko izvozniki uporabljajo pri prenosu osebnih podatkov v tretje države, če niso bili sprejeti sklepi o ustreznosti. Glavne vrste orodij za prenos iz člena 46 Splošne uredbe o varstvu podatkov so:

- standardna določila o varstvu podatkov;
- zavezujoča poslovna pravila;
- kodeksi ravnanja;
- mehanizmi potrjevanja;
- ad hoc pogodbena določila.

22. Ne glede na izbrano orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov morate zagotoviti, da se bo za prenesene osebne podatke na splošno zagotavljala v bistvu enakovredna raven varstva.

23. Orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov vsebujejo v glavnem ustrezne pogodbene zaščitne ukrepe, ki se lahko uporabljajo za prenose v vse tretje države. Zaradi razmer v tretji državi, kamor prenesete podatke, morate morda ta orodja za prenos in zaščitne ukrepe, ki jih vsebujejo, dopolniti še z dodatnimi ukrepi („dopolnilni ukrepi“), da zagotovite v bistvu enakovredno raven varstva.[35]

Odstopanja

24. Splošna uredba o varstvu podatkov poleg sklepov o ustreznosti in orodij za prenos iz člena 46 vsebuje še tretjo možnost, ki dovoljuje prenose osebnih podatkov v nekaterih primerih. Pod določenimi pogoji še vedno lahko prenesete osebne podatke na podlagi odstopanja iz člena 49 Splošne uredbe o varstvu podatkov.

25. Člen 49 Splošne uredbe o varstvu podatkov se uporablja v izjemnih primerih. Odstopanja, ki jih vsebuje, je treba razlagati restriktivno, nanašajo pa se v glavnem na dejavnosti obdelave, ki so občasne in se ne ponavljajo. EOVP je izdal Smernice št. 2/2018 o odstopanjih iz člena 49 v skladu z Uredbo 2016/679. [36]

26. Preden se oprete na odstopanje iz člena 49 Splošne uredbe o varstvu podatkov, morate preveriti, ali vaš prenos izpolnjuje stroge pogoje, ki jih ta določba določa za vsakega od njih.

***

27. Če vašega prenosa ni mogoče pravno utemeljiti na podlagi sklepa o ustreznosti ali odstopanja iz člena 49, morate nadaljevati s korakom 3.

[35] C-311/18 (Schrems II), točki 130 in 133. Glej tudi točko 2.3 v nadaljevanju.
[36] Dodatne smernice o tem so na voljo na spletnem naslovu https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_sl.

2.3 Korak 3: Ocenite, ali je orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov, na katerega se opirate, učinkovito glede na vse okoliščine prenosa

28. Izbira orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov morda ne bo zadostovala. Z orodjem za prenos je treba zagotoviti, da se s prenosom ne ogrozi raven varstva, ki jo zagotavlja Splošna uredba o varstvu podatkov.[37] Z drugimi besedami, vaše orodje za prenos mora biti učinkovito v praksi.

29. Učinkovito pomeni, da se za prenesene osebne podatke v tretji državi zagotavlja raven varstva, ki je v bistvu enakovredna ravni, ki se zagotavlja v EGP.[38] To ne velja, če uvozniku podatkov preprečujejo izpolnitev obveznosti na podlagi izbranega orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov zaradi zakonodaje in praks tretje države, ki se v njej uporabljajo za prenos.

30. Zato morate po potrebi v sodelovanju z uvoznikom oceniti, ali v okviru vašega konkretnega prenosa morda kar koli v pravu ali praksi tretje države posega v učinkovitost ustreznih zaščitnih ukrepov, ki jih vsebuje orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov, na katerega se opirate. Po potrebi naj vam uvoznik vaših podatkov zagotovi ustrezne vire in informacije o tretji državi, v kateri ima sedež, in pravu, ki se uporablja za prenos. Sklicujete se lahko tudi na druge vire informacij, kot so informacije, ki so neizčrpno navedene v Prilogi 3.[39]

31. Pri oceni upoštevajte vse akterje, ki sodelujejo pri prenosu (npr. upravljavce, obdelovalce in podobdelovalce, ki obdelujejo podatke v tretji državi), kot so opredeljeni v evidenci prenosov. Več upravljavcev, obdelovalcev ali uvoznikov kot je vključenih, kompleksnejša bo vaša ocena. V tej oceni morate upoštevati tudi vse morebitne nadaljnje prenose.

32. V ta namen morate preučiti značilnosti posameznih prenosov in ugotoviti, kako se nacionalni pravni sistem države, v katero se prenesejo (ali nadalje prenesejo) podatki, uporablja za te prenose.

33. Veljavni pravni okvir je odvisen od okoliščin prenosa, zlasti:

- namenov, za katere se podatki prenesejo in obdelujejo (npr. trženje, človeški viri, hramba, podpora IT, klinično preskušanje);
- vrste subjektov, vključenih v obdelavo (javni/zasebni; upravljavec/obdelovalec);
- sektorja, v katerem se izvaja prenos (npr. oglaševalsko-tehnološki, telekomunikacijski, finančni itd.);
- kategorij prenesenih osebnih podatkov (npr. osebni podatki, ki se nanašajo na otroke, lahko v tretji državi spadajo na področje uporabe posebne zakonodaje);
- ali bodo podatki shranjeni v tretji državi ali je samo zagotovljen oddaljeni dostop do podatkov, shranjenih v EU/EGP;
- oblike podatkov, ki se prenesejo (tj. v obliki navadnega besedila/psevdonimizirani ali šifrirani[40]);
- možnosti, da bodo morda podatki predmet nadaljnjih prenosov iz tretje države v drugo tretjo državo.[41]

[37] Člen 44 Splošne uredbe o varstvu podatkov.
[38] C-311/18 (Schrems II), točka 105 in druga ugotovitev.
[39] Glej tudi točko 43 v nadaljevanju.
[40] Nekatere tretje države ne dovoljujejo uvoza šifriranih podatkov.
[41] Če je upravljavec izdal predhodno posebno ali splošno pisno dovoljenje v skladu s členom 28(2) Splošne uredbe o varstvu podatkov.

34. Oceniti morate, ali kateri od zakonov, ki se uporabljajo, posega v obveznosti, ki jih vsebuje vaše izbrano orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov. Preverite, ali je mogoče obveznosti, ki posameznikom, na katere se nanašajo osebni podatki, omogočajo uveljavljanje pravic v okviru mednarodnih prenosov (kot so zahteve do dostopa, popravka in izbrisa prenesenih podatkov), učinkovito uporabljati v praksi in jih pravo namembne tretje države ne preprečuje.

35. Oceniti morate, ali zadevna splošna pravila vplivajo na učinkovito uporabo zaščitnih ukrepov, ki jih vsebuje orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov, ter na temeljne pravice posameznikov (zlasti na pravico do varstva, zagotovljeno posamezniku, na katerega se nanašajo osebni podatki, v primeru dostopa javnih organov tretje države do prenesenih podatkov).

36. V vsakem primeru posebno pozornost namenite vsej zadevni zakonodaji, zlasti zakonodaji, ki določa zahteve za razkritje osebnih podatkov javnim organom ali tem javnim organom podeljuje pooblastila za dostop do osebnih podatkov (npr. za namene kazenskega pregona, regulativnega nadzora in nacionalne varnosti). Če so te zahteve ali pooblastila omejena na to, kar je potrebno in sorazmerno v demokratični družbi,[42] ne smejo posegati v obveznosti, ki jih vsebuje orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov, na katerega se opirate.

37. Standarde EU, kot sta člena 47 in 52 Listine EU o temeljnih pravicah, je treba uporabiti kot referenco za oceno, ali je tak dostop javnih organov omejen na to, kar je potrebno in sorazmerno v demokratični družbi, in ali je posameznikom, na katere se nanašajo osebni podatki, zagotovljeno učinkovito varstvo.

38. Pri tej oceni je treba upoštevati tudi različne vidike pravnega sistema zadevne tretje države, na primer elemente iz člena 45(2) Splošne uredbe o varstvu podatkov.[43] Na primer, stanje pravne države v tretji državi je lahko pomembno za oceno učinkovitosti razpoložljivih mehanizmov, da posamezniki dobijo (sodno) varstvo pred nezakonitim vladnim dostopom do osebnih podatkov. Obstoj celovite zakonodaje o varstvu podatkov ali neodvisnega organa za varstvo podatkov ter spoštovanje mednarodnih instrumentov, ki zagotavljajo zaščitne ukrepe za varstvo podatkov, lahko prispevata k zagotavljanju sorazmernosti vladnega posredovanja.[44]

***

39. Priporočila Evropskega odbora za varstvo podatkov glede evropskih bistvenih jamstev zagotavljajo elemente, ki jih je treba oceniti za ugotovitev, ali se za pravni okvir, ki ureja dostop javnih organov do osebnih podatkov v tretji državi, ne glede na to, ali so to agencije za nacionalno varnost ali organi kazenskega pregona, lahko šteje, da je poseg upravičen (in zato ne posega v obveznosti, prevzete na podlagi orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov) ali ne. To naj se zlasti skrbno preuči, kadar zakonodaja, ki ureja dostop javnih organov do podatkov, ni jasna ali javno dostopna.

[42] Glej člena 47 in 52 Listine EU o temeljnih pravicah, člen 23(1) Splošne uredbe o varstvu podatkov in Priporočila št. 02/2020 Evropskega odbora za varstvo podatkov glede evropskih bistvenih jamstev za nadzorne ukrepe z dne 10. novembra 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_sl.

[43] C-311/18 (Schrems II), točka 104.

[44] Na primer: Konvencija št. 108 (Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, ETS št. 108) ali Konvencija št. 108+ (Posodobljena konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, CETS št. 223) določa izvršljiva mednarodna pravna sredstva v primeru kršitev pravil o varstvu podatkov ter prispeva k zagotavljanju minimalne ravni varstva osebnih podatkov in spoštovanju zasebnega življenja.

40. Priporočila Evropskega odbora za varstvo podatkov glede evropskih bistvenih jamstev lahko pri prenosih podatkov na podlagi orodij za prenos iz člena 46 usmerjajo izvoznika in uvoznika podatkov pri ocenjevanju, ali taka pooblastila neupravičeno posegajo v obveznosti uvoznika podatkov, da zagotovi v bistvu enakovredno raven.

41. Neobstoj v bistvu enakovredne ravni varstva bo zlasti očiten, kadar zakonodaja ali praksa tretje države, ki se uporablja za vaš prenos, ni v skladu z zahtevami evropskih bistvenih jamstev.

42. Vaša ocena mora v prvi vrsti temeljiti na zakonodaji, ki je javno dostopna. Vendar v nekaterih primerih to morda ne bo zadostovalo, ker morda v tretjih državah nimajo take zakonodaje. Če v tem primeru še vedno želite opraviti prenos, preučite druge zadevne in objektivne dejavnike[45] ter se ne opirajte na subjektivne dejavnike, kot je verjetnost dostopa javnih organov do vaših podatkov na način, ki ni v skladu s standardi EU. To oceno opravite s potrebno skrbnostjo in jo temeljito dokumentirajte, ker boste odgovorni za odločitev, ki jo boste morda sprejeli na tej podlagi.[46]

43. Svojo oceno lahko dopolnite z informacijami, pridobljenimi iz drugih virov[47], kot so:

    - elementi, ki dokazujejo, da bo organ tretje države glede na sporočene precedenčne primere, zakonodajo in prakso poskušal dobiti dostop do podatkov, o čemer bo uvoznik podatkov obveščen ali pa ne;
    - elementi, ki dokazujejo, da bo organ tretje države glede na sporočene precedenčne primere, zakonska pooblastila ter tehnične, finančne in človeške vire, ki jih ima na voljo, lahko dobil dostop do podatkov prek uvoznika podatkov ali z neposrednim prestrezanjem komunikacijske poti.

44. Vaša ocena bo morda na koncu razkrila, da orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov, na katero se opirate, in ustrezni zaščitni ukrepi, ki jih vsebuje:

    - učinkovito zagotavljajo, da se za prenesene osebne podatke v tretji državi zagotavlja raven varstva, ki je v bistvu enakovredna ravni, ki se zagotavlja v EGP. Zakonodaja in prakse tretje države, ki se uporabljajo za prenos, uvozniku podatkov omogočajo izpolnitev njegovih obveznosti na podlagi izbranega orodja za prenos. Oceno izvajajte v ustreznih časovnih razmikih ali če se zgodijo pomembne spremembe (glej korak 6);
    - ne zagotavljajo učinkovito v bistvu enakovredne ravni varstva. Uvoznik podatkov ne more izpolniti svojih obveznosti zaradi zakonodaje in/ali praks tretje države, ki se uporabljajo za prenos. Sodišče je poudarilo, da če z orodji za prenos iz člena 46 Splošne uredbe o varstvu podatkov ni mogoče zagotoviti ustreznega varstva, je odgovornost izvoznika podatkov, da sprejme učinkovite dopolnilne ukrepe ali da osebnih podatkov ne prenese.[48]

[45] Glej točko 43 v nadaljevanju in Prilogo 3.
[46] Člen 5(2) Splošne uredbe o varstvu podatkov.
[47] Glej tudi Prilogo 3.
[48] Sodišče, C-311/18 (Schrems II), točki 134 in 135.

Sodišče je na primer razsodilo, da člen 702 ameriškega zakona o nadzoru tujih obveščevalnih podatkov (FISA) ne upošteva minimalnih zaščitnih ukrepov, ki izhajajo iz načela sorazmernosti v skladu s pravom EU, tako da zanj ni mogoče šteti, da je omejen na tisto, kar je nujno potrebno. To pomeni, da raven varstva programov v skladu s členom 702 FISA v bistvu ni enakovredna zaščitnim ukrepom, ki se zahtevajo v skladu s pravom EU. Posledično velja, da če uvoznik podatkov ali nadaljnji prejemnik, ki mu lahko uvoznik podatkov razkrije podatke, spada pod člen 702 FISA[49], se je mogoče pri takem prenosu na standardna pogodbena določila ali druga orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov opreti samo, če je zaradi dodatnih dopolnilnih tehničnih ukrepov dostop do prenesenih podatkov onemogočen ali neučinkovit.

2.4 Korak 4: Sprejmite dopolnilne ukrepe

45. Če je vaša ocena v okviru koraka 3 razkrila, da vaše orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov ni učinkovito, morate po potrebi v sodelovanju z uvoznikom preučiti, ali so na voljo dopolnilni ukrepi, s katerimi bi se lahko, če bi se dodali zaščitnim ukrepom, ki jih vsebujejo orodja za prenos, zagotovilo, da bi se za prenesene podatke v tretji državi zagotavljala raven varstva, ki je v bistvu enakovredna ravni, ki se zagotavlja v EU.[50] „Dopolnilni ukrepi“ po definiciji dopolnjujejo zaščitne ukrepe, ki jih že zagotavljajo orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov.[51]

46. Za vsak primer posebej morate opredeliti, kateri dopolnilni ukrepi bi lahko bili pri uporabi določenega orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov učinkoviti za niz prenosov v določeno tretjo državo. Svoje predhodne ocene v okviru korakov (1, 2 in 3 zgoraj) boste lahko nadgradili in na podlagi njihovih ugotovitev preverili morebitno učinkovitost dopolnilih ukrepov pri zagotavljanju zahtevane ravni varstva.

47. Dopolnilni ukrepi so načeloma lahko pogodbeni, tehnični ali organizacijski. Z združitvijo različnih ukrepov na način, da se medsebojno podpirajo in nadgrajujejo, se lahko poveča raven varstva in tako prispeva k doseganju standardov EU.

48. Samo s pogodbenimi in organizacijskimi ukrepi se po navadi javnim organom tretje države ne prepreči dostop do osebnih podatkov (kadar to neupravičeno posega v obveznosti uvoznika podatkov glede zagotavljanja v bistvu enakovrednosti). Dejansko bodo primeri, v katerih je mogoče samo s tehničnimi ukrepi ovirati dostop javnih organov v tretjih državam do osebnih podatkov ali zagotoviti njegovo neučinkovitost, zlasti za namene nadzora.[52] V teh primerih lahko pogodbeni ali organizacijski ukrepi

[49] Člen 702 FISA se uporablja, če se podatki pridobijo „od ponudnika elektronskih komunikacijskih storitev ali z njegovo pomočjo“ (člen 702 FISA je člen 1881a naslova 50 zakonodajne zbirke ZDA (USC), pod točko (h)(2)(A)(vi)), ki je bil nato v členu 1881(b)(4) naslova 50 USC opredeljen kot
„(A) izvajalec telekomunikacijskih storitev, kot je ta pojem opredeljen v členu 153 naslova 47;
(B) ponudnik elektronskih komunikacijskih storitev, kot je ta pojem opredeljen v členu 2510 naslova 18;
(C) ponudnik računalniških storitev na daljavo, kot je ta pojem opredeljen v členu 2711 naslova 18;
(D) kateri koli drugi ponudnik komunikacijskih storitev, ki ima dostop do žičnih ali elektronskih komunikacij, ne glede na to, ali se take komunikacije prenesejo ali so shranjene, ali
(E) vodilni delavec, zaposleni ali zastopnik subjekta iz pododstavka (A), (B), (C), ali (D).“

[50] C-311/18 (Schrems II), točka 96.

[51] Uvodna izjava 109 Splošne uredbe o varstvu podatkov in C-311/18 (Schrems II), točka 133.

[52] Kadar tak dostop presega, kar je v demokratični družbi potrebno in sorazmerno; glej člena 47 in 52 Listine EU o temeljnih pravicah, člen 23(1) Splošne uredbe o varstvu podatkov in Priporočila št. 02/2020 Evropskega odbora za varstvo podatkov glede evropskih bistvenih jamstev za nadzorne ukrepe z dne 10. novembra 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_sl.

dopolnjujejo tehnične ukrepe in povečajo splošno raven varstva podatkov, na primer z oviranjem poskusov javnih organov, da bi dobili dostop do podatkov na način, ki ni v skladu s standardi EU.

49. Po potrebi lahko v sodelovanju z uvoznikom podatkov pregledate naslednji (neizčrpni) seznam dejavnikov in opredelite, kateri dopolnilni ukrepi bi bili najučinkovitejši za varstvo prenesenih podatkov:

- oblika podatkov, ki se prenesejo (tj. v obliki navadnega besedila/psevdonimizirani ali šifrirani);
- vrsta podatkov;
- trajanje in kompleksnost poteka dela pri obdelavi podatkov, število akterjev, vključenih v obdelavo, ter njihovo medsebojno razmerje (npr. ali je v prenose vključenih več upravljavcev ali pa so vključeni upravljavci in obdelovalci, vključitev obdelovalcev, ki bodo podatke od vas prenesli uvozniku vaših podatkov (ob upoštevanju ustreznih določb, ki se zanje uporabljajo v skladu z zakonodajo namembne tretje države));[53]
- možnost, da bodo podatki lahko predmet nadaljnjih prenosov znotraj iste tretje države ali celo v druge tretje države (npr. vključitev podobdelovalcev uvoznika podatkov[54]).

Primeri dopolnilnih ukrepov

50. Nekaj primerov tehničnih, pogodbenih in organizacijskih ukrepov, ki bi se lahko preučili, je na voljo v neizčrpnih seznamih iz Priloge 2.

***

51. Če ste uvedli učinkovite dopolnilne ukrepe, s katerimi se skupaj z vašim izbranim orodjem za prenos iz člena 46 Splošne uredbe o varstvu podatkov dosega raven varstva, ki je zdaj v bistvu enakovredna ravni varstva, ki se zagotavlja v EGP, lahko začnete izvajati svoje prenose.

52. Če ne morete najti ali izvesti učinkovitih dopolnilnih ukrepov, s katerimi bi se za prenesene osebne podatke zagotavljala v bistvu enakovredna raven varstva,[55] na podlagi orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov, na katerega se opirate, ne smete začeti prenosov osebnih podatkov v zadevno tretjo državo. Če prenose že izvajate, morate prenos osebnih podatkov začasno ustaviti ali prenehati.[56] V skladu z zaščitnimi ukrepi, ki jih vsebuje orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov, na katerega se opirate, bi vam moral uvoznik podatke, ki ste jih že prenesli v zadevno tretjo državo, in njihove kopije v celoti vrniti ali uničiti.[57]

[53] Splošna uredba o varstvu podatkov dodeljuje upravljavcem in obdelovalcem različne obveznosti. Prenosi so lahko od upravljavca k upravljavcu, med skupnimi upravljavci, od upravljavca k obdelovalcu ter na podlagi dovoljenja upravljavca od obdelovalca k upravljavcu ali od obdelovalca k obdelovalcu.
[54] Glej opombo 25.
[55] Kadar tak dostop presega, kar je v demokratični družbi potrebno in sorazmerno; glej člena 47 in 52 Listine EU o temeljnih pravicah, člen 23(1) Splošne uredbe o varstvu podatkov in Priporočila št. 02/2020 Evropskega odbora za varstvo podatkov glede evropskih bistvenih jamstev za nadzorne ukrepe z dne 10. novembra 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_sl.
[56] C-311/18 (Schrems II), točka 135.
[57] Glej klavzulo 12 iz Priloge k Sklepu 87/2010 o standardnih pogodbenih klavzulah; glej (neobvezno) posebno klavzulo o prenehanju pogodbe iz Priloge B k Odločbi 2004/915/ES o standardnih pogodbenih klavzulah.

Primer: pravo tretje države prepoveduje dopolnilne ukrepe, ki ste jih opredelili (npr. prepoveduje uporabo šifriranja) ali drugače preprečuje njihovo učinkovitost. Prenosov osebnih podatkov v to državo ne smete začeti oziroma morate ustaviti obstoječe prenose v to državo, ki se že izvajajo.

53. Če se odločite, da boste prenos nadaljevali ne glede na dejstvo, da uvoznik ne more izpolniti obveznosti, prevzete na podlagi orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov, morate obvestite pristojni nadzorni organ v skladu s posebnimi določbami, vstavljenimi v zadevno orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov.[58] Pristojni nadzorni organ bo začasno ustavil ali prepovedal prenose podatkov, če bo ugotovil, da v bistvu enakovredne ravni varstva ni mogoče zagotoviti.[59]

54. Pristojni nadzorni organ vam lahko naloži kateri koli drug popravljalni ukrep (npr. globo), če kljub temu, da ne morete dokazati v bistvu enakovredne ravni varstva v tretji državi, začnete izvajati ali še naprej izvajate prenos.

2.5 Korak 5: Postopkovni koraki, če ste opredelili učinkovite dopolnilne ukrepe

55. Postopkovni koraki, ki jih boste morda morali opraviti, če ste opredelili učinkovite dopolnilne ukrepe, ki jih je treba uvesti, so lahko različni glede na orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov, ki ga uporabljate ali ste ga predvideli za uporabo.

2.5.1 Standardna določila o varstvu podatkov (člen 46(2)(c) in (d) Splošne uredbe o varstvu podatkov)

56. Če nameravate poleg standardnih pogodbenih določil uvesti tudi dopolnilne ukrepe, vam ni treba pri pristojnem nadzornem organu zaprositi za dovoljenje za dodajanje takih določil ali dodatnih zaščitnih ukrepov, če opredeljeni dopolnilni ukrepi niso neposredno ali posredno v nasprotju s standardnimi pogodbenimi določili in zadostujejo za preprečitev ogrožanja ravni varstva, ki jo zagotavlja Splošna uredba o varstvu podatkov.[60] Izvoznik in uvoznik podatkov morata zagotoviti, da dodatnih določil ni mogoče razlagati, da kakor koli omejujejo pravice in obveznosti iz standardnih pogodbenih določil ali da kakor koli znižujejo raven varstva podatkov. To bi morali biti sposobni dokazati, vključno z jasnostjo vseh določil, v skladu z načelom odgovornosti in vašo obveznostjo zagotavljanja zadostne ravni varstva podatkov. Pristojni nadzorni organi so pooblaščeni, da po potrebi ta določila o dopolnilnih ukrepih pregledajo (npr. pri pritožbi ali preiskavi na lastno pobudo).

[58] Glej pogosto zastavljena vprašanja Evropskemu nadzoru za varstvo podatkov v zvezi s sodbo Sodišča Evropske unije z dne 23. julija 2020, Data Protection Commissioner proti Facebook Ireland Ltd in Maximillianu Schremsu, C-311/18, zlasti vprašanja 5, 6 in 9. Glej tudi klavzulo 4(g) Sklepa Komisije 2010/87/EU; klavzulo 5(a) Odločbe Komisije 2001/497/ES in klavzulo II(c) „Sklopa II“ Odločbe Komisije 2004/915/ES.

[59] C-311/18 (Schrems II), točki 113 in 121.

[60] V uvodni izjavi 109 Splošne uredbe o varstvu podatkov je navedeno: „Možnost, ki jo ima upravljavec ali obdelovalec glede uporabe standardnih določil Komisije ali nadzornega organa o varstvu podatkov, upravljavcem ali obdelovalcem ne bi smela preprečiti niti, da standardna določila o varstvu podatkov vključijo v obsežnejšo pogodbo, kot je pogodba med obdelovalcem in drugim obdelovalcem, niti da dodajo druga določila ali dodatne zaščitne ukrepe, če ti neposredno ali posredno ne nasprotujejo standardnim pogodbenim določilom Komisije ali nadzornega organa ali posegajo v temeljne pravice ali svoboščine posameznikov, na katere se nanašajo osebni podatki.“ Podobne določbe vsebuje sklop standardnih pogodbenih določil, ki jih je Evropska komisija sprejela na podlagi Direktive 95/45/ES.

57. Če nameravate standardna določila o varstvu podatkov spremeniti ali če so dodani dopolnilni ukrepi neposredno ali posredno „v nasprotju“ s standardnimi pogodbenimi določili, se za vas več ne šteje, da se opirate na standardna pogodbena določila[61], in morate pri pristojnem nadzornem organu zaprositi za dovoljenje v skladu s členom 46(3)(a) Splošne uredbe o varstvu podatkov.

2.5.2 Zavezujoča poslovna pravila (člen 46(2)(b) Splošne uredbe o varstvu podatkov)

58. Trditev iz sodbe v zadevi Schrems II velja tudi za druge instrumente za prenos v skladu s členom 46(2) Splošne uredbe o varstvu podatkov, saj so vsi ti instrumenti v bistvu pogodbeni, zato jamstva, ki so v njih predvidena, in obveznosti, ki jih z njimi prevzamejo pogodbene stranke, ne morejo zavezovati javnih organov tretjih držav.[62]

59. Sodba v zadevi Schrems II se uporablja za prenose osebnih podatkov na podlagi zavezujočih poslovnih pravil, saj lahko zakonodaja tretjih držav vpliva na varstvo, ki ga ti instrumenti zagotavljajo. Glede točnega učinka sodbe v zadevi Schrems II na zavezujoča poslovna pravila še vedno poteka razprava. EOVP bo čim prej zagotovil več podrobnosti o tem, ali bi bilo morda treba v zavezujoča poslovna pravila v referenčnih dokumentih WP 256/257 vključiti kakršne koli dodatne obveznosti.[63]

60. Sodišče je poudarilo, da je odgovornost izvoznika in uvoznika podatkov, da ocenita, ali se v zadevni tretji državi spoštuje raven varstva, ki se zahteva s pravom EU, da bi ugotovila, ali je mogoče v praksi spoštovati jamstva, zagotovljena s standardnimi pogodbenimi določili ali zavezujočimi poslovnimi pravili. Če to ni mogoče, morate oceniti, ali lahko uvedete dopolnilne ukrepe za zagotovitev v bistvu enakovredne ravni varstva, kot se zagotavlja v EGP, in ali pravo ali praksa tretje države ne bo posegala v te dopolnilne ukrepe in preprečila njihove učinkovitosti.

2.5.3 Ad hoc pogodbena določila (člen 46(3)(a) Splošne uredbe o varstvu podatkov)

61. Trditev iz sodbe v zadevi Schrems II velja tudi za druge instrumente za prenos v skladu s členom 46(2) Splošne uredbe o varstvu podatkov, saj so vsi ti instrumenti v bistvu pogodbeni, zato jamstva, ki so v njih predvidena, in obveznosti, ki jih z njimi prevzamejo pogodbene stranke, ne morejo zavezovati javnih organov tretjih držav.[64] Sodba v zadevi Schrems II se zato uporablja za prenose osebnih podatkov na podlagi ad hoc pogodbenih določil, saj lahko pravo tretjih držav vpliva na varstvo, ki ga ti instrumenti zagotavljajo. Glede točnega učinka sodbe v zadevi Schrems II na ad hoc določila še vedno poteka razprava. EOVP bo čim prej zagotovil več podrobnosti.

---

[61] Glej po analogiji Mnenje 17/2020 Evropskega odbora za varstvo podatkov o osnutku standardnih pogodbenih določil, ki jih je predložil slovenski nadzorni organ (člen 28(8) Splošne uredbe o varstvu podatkov) o že sprejetem standardnem pogodbenem določilu iz člena 28 („Odbor poleg tega opozarja, da možnost uporabe standardnih pogodbenih določil, ki jih sprejme nadzorni organ, pogodbenicama ne preprečuje, da dodata druge določbe ali dodatne zaščitne ukrepe, če niso v nasprotju, bodisi posredno bodisi neposredno, s sprejetimi standardnimi pogodbenimi določili ali ne posegajo v temeljne pravice ali svoboščine posameznikov, na katere se osebni podatki nanašajo. Kadar so standardna določila o varstvu podatkov spremenjena, se poleg tega šteje, da pogodbenici ne uporabljata več sprejetih standardnih pogodbenih določil.“), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_sl.pdf.

[62] Sodišče, C-311/18 (Schrems II), točka 132.

[63] Delovni dokument Delovne skupine iz člena 29 o vzpostavitvi preglednice elementov in načel, ki bo vključena v zavezujoča poslovna pravila, kakor je bil nazadnje spremenjen in sprejet 6. februarja 2018, WP 256 rev.01; Delovni dokument Delovne skupine iz člena 29 o vzpostavitvi preglednice elementov in načel, ki bo vključena v zavezujoča poslovna pravila, kakor je bil nazadnje spremenjen in sprejet 6. februarja 2018, WP 257 rev.01.

[64] Sodišče, C-311/18 (Schrems II), točka 132.

2.6 Korak 6: Oceno ponovno izvedite v ustreznih časovnih razmikih

62. Nenehno in po potrebi v sodelovanju z uvozniki podatkov spremljajte razvoj v tretji državi, kamor ste prenesli osebne podatke, ki bi lahko vplival na vašo prvotno oceno ravni varstva in odločitve, ki ste jih morda v skladu z njo sprejeli v zvezi s svojimi prenosi. Odgovornost je stalna obveznost (člen 5(2) Splošne uredbe o varstvu podatkov).

63. Uvesti bi morali dovolj zanesljive mehanizme, ki bi zagotavljali, da se nemudoma ustavi ali preneha prenos, če:

- je uvoznik kršil ali ne more spoštovati obveznosti, ki jih je prevzel na podlagi orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov, ali
- dopolnilni ukrepi v zadevni tretji državi niso več učinkoviti.

3 SKLEPNA UGOTOVITEV

64. Splošna uredba o varstvu podatkov določa pravila o obdelavi osebnih podatkov v EGP in s tem dovoljuje prosti pretok osebnih podatkov znotraj EGP. Poglavje V Splošne uredbe o varstvu podatkov ureja prenose osebnih podatkov v tretje države in določa visok prag: s prenosom se ne sme ogroziti raven varstva, ki jo posameznikom zagotavlja Splošna uredba o varstvu podatkov (člen 44 navedene uredbe). Sodišče v sodbi v zadevi C-311/18 (Schrems II) poudarja potrebo po zagotavljanju kontinuitete ravni varstva, ki se v skladu s Splošno uredbo o varstvu podatkov zagotavlja za osebne podatke, prenesene v tretjo državo.[65]

65. Da bi zagotovili v bistvu enakovredno raven varstva vaših podatkov, morate v prvi vrsti temeljito preučiti svoje prenose. Preveriti morate tudi, ali so podatki, ki jih prenesete, ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se prenesejo in obdelujejo v tretji državi.

66. Opredeliti morate tudi orodje za prenos, na katero se pri prenosih opirate. Če orodje za prenos ni sklep o ustreznosti, morate za vsak primer posebej preveriti, ali v okviru vaših prenosov pravo ali praksa namembne tretje države ogroža zaščitne ukrepe, ki jih vsebuje orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov, ali ne. Če z orodjem za prenos iz člena 46 Splošne uredbe o varstvu podatkov za osebne podatke, ki jih prenesete, ni mogoče doseči v bistvu enakovredne ravni varstva, se vrzel lahko zapolni z dopolnilnimi ukrepi.

67. Če ne morete najti ali izvesti učinkovitih dopolnilnih ukrepov, s katerimi bi se za prenesene osebne podatke zagotavljala v bistvu enakovredna raven varstva, na podlagi vašega izbranega orodja za prenos ne smete začeti prenosov osebnih podatkov v zadevno tretjo državo. Če prenose že izvajate, morate prenos osebnih podatkov nemudoma začasno ustaviti ali prenehati.

68. Pristojni nadzorni organ je pooblaščen, da začasno ustavi ali preneha prenose osebnih podatkov v tretjo državo, če se za prenesene podatke ne zagotavlja varstvo, ki ga zahtevata pravo EU, zlasti člena 45 in 46 Splošne uredbe o varstvu podatkov, ter Listina o temeljnih človekovih pravicah.

Za Evropski odbor za varstvo podatkov

Predsednica

(Andrea Jelinek)

[65] C-311/18 (Schrems II), točka 93.

PRILOGA 1: OPREDELITEV POJMOV

- „Tretja država“ pomeni katero koli državo, ki ni država članica EGP.
- „EGP“ pomeni Evropski gospodarski prostor in vključuje države članice Evropske unije ter Islandijo, Norveško in Lihtenštajn, za katere se Splošna uredba o varstvu podatkov uporablja na podlagi Sporazuma EGP, zlasti njegove Priloge XI in Protokola 37.
- „Splošna uredba o varstvu podatkov“ se nanaša na Uredbo (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.
- „Listina“ se nanaša na Listino Evropske unije o temeljnih pravicah, UL C 326, 26.10.2012, str. 391–407.
- „Sodišče EU“ ali „Sodišče“ se nanaša na Sodišče Evropske unije. To je organ sodne oblasti Evropske unije in v sodelovanju s sodišči in tribunali držav članic zagotavlja enotno uporabo in razlago prava EU.
- „Izvoznik podatkov“ pomeni upravljavca ali obdelovalca v EGP, ki prenese osebne podatke k upravljavcu ali obdelovalcu v tretji državi.
- „Uvoznik podatkov“ pomeni upravljavca ali obdelovalca v tretji državi, ki prejme osebne podatke, prenesene iz EGP, ali dobi dostop do njih.
- „Orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov“ se nanaša na ustrezne zaščitne ukrepe na podlagi člena 46 navedene uredbe, ki jih morajo izvozniki podatkov uvesti pri prenosu osebnih podatkov v tretjo državo, če ni bil sprejet sklep o ustreznosti v skladu s členom 45(3) navedene uredbe. Člen 46(2) in (3) Splošne uredbe o varstvu podatkov vsebuje seznam orodij za prenos iz člena 46 te uredbe, ki jih lahko uporabljajo upravljavci in obdelovalci.
- „Standardna pogodbena določila“ pomenijo standardna določila o varstvu podatkov (ali standardna pogodbena določila), ki jih je Evropska komisija sprejela za prenose osebnih podatkov med upravljavci in obdelovalci v EGP ter upravljavci ali obdelovalci zunaj EGP. Standardna pogodbena določila, ki jih je sprejela Evropska komisija, so v skladu s členom 46(2)(c) in (5) Splošne uredbe o varstvu podatkov orodje za prenos iz Splošne uredbe o varstvu podatkov.

PRILOGA 2: PRIMERI DOPOLNILNIH UKREPOV

69. Naslednji ukrepi so primeri dopolnilnih ukrepov, ki bi jih lahko preučili, ko dosežete korak 4 „Sprejmite dopolnilne ukrepe“. Ta seznam ni izčrpen. Z izbiro in izvajanjem enega ali več teh ukrepov se ne bo nujno in sistematično zagotovilo, da bo vaš prenos izpolnjeval standard v bistvu enakovrednega varstva, ki se zahteva s pravom EU. Izberite tiste dopolnilne ukrepe, s katerimi je mogoče za vaše prenose učinkovito zagotoviti to raven varstva.

70. V smislu sodbe Sodišča v zadevi „Schrems II“ se lahko za vsak dopolnilni ukrep šteje, da je učinkovit le, če in kolikor odpravlja določene pomanjkljivosti, opredeljene v vaši oceni pravnega položaja v tretji državi. Če na koncu ne morete zagotoviti v bistvu enakovredne ravni varstva, osebnih podatkov ne smete prenesti.

71. Morda morate kot upravljavec ali obdelovalec že izvajati nekatere ukrepe iz te priloge, tudi če je uvoznik vaših podatkov vključen v sklep o ustreznosti, enako kot jih morate morda izvajati, če podatke obdelujete v EGP.[66]

Tehnični ukrepi

72. V tem oddelku je opisan neizčrpen seznam primerov tehničnih ukrepov, s katerimi se lahko dopolnijo zaščitni ukrepi, ki jih vsebujejo orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov, za zagotovitev spoštovanja ravni varstva, ki se zahteva s pravom EU, v okviru prenosa osebnih podatkov v tretjo državo. Ti ukrepi so še posebno potrebni, kadar so s pravom te države uvozniku podatkov naložene obveznosti, ki so v nasprotju z zaščitnimi ukrepi, ki jih vsebujejo orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov, in lahko zlasti ogrozijo pogodbeno jamstvo ustrezne ravni varstva pred dostopom javnih organov zadevne tretje države do teh podatkov[67].

73. V tem oddelku so za večjo jasnost najprej navedeni tehnični ukrepi, ki bi bili lahko v nekaterih scenarijih/primerih uporabe učinkoviti za zagotovitev v bistvu enakovredne ravni varstva. V nadaljevanju so navedeni nekateri scenariji/primeri uporabe, v katerih ni bilo mogoče najti nobenega tehničnega ukrepa za zagotovitev te ravni varstva.

Scenariji, za katere je bilo mogoče najti *učinkovite* ukrepe

74. Cilj spodaj navedenih ukrepov je zagotoviti, da dostop javnih organov v tretjih državah do prenesenih podatkov ne posega v učinkovitost ustreznih zaščitnih ukrepov, ki jih vsebujejo orodja za prenos iz člena 46 Splošne uredbe o varstvu podatkov. Ti ukrepi se uporabljajo tudi, če je dostop javnih organov v skladu s pravom države uvoznika, kadar tak dostop presega, kar je v demokratični družbi potrebno in sorazmerno[68]. Cilj teh ukrepov je onemogočiti potencialno kršitveni dostop, tako da se organom prepreči, da bi identificirali posameznike, na katere se nanašajo osebni podatki, sklepali o informacijah o njih, jih izpostavili v drugem okolju ali prenesene podatke povezali z drugimi nabori podatkov, s katerimi morda razpolagajo in ki lahko med drugimi podatki vsebujejo spletne identifikatorje, ki jih

[66] Člen 5(2) in člen 32 Splošne uredbe o varstvu podatkov.
[67] C-311/18 (Schrems II), točka 135.
[68] Glej člena 47 in 52 Listine EU o temeljnih pravicah, člen 23(1) Splošne uredbe o varstvu podatkov in Priporočila Evropskega odbora za varstvo podatkov glede evropskih bistvenih jamstev za nadzorne ukrepe.

zagotavljajo naprave, aplikacije, orodja in protokoli, ki jih posamezniki, na katere se nanašajo osebni podatki, uporabljajo v drugih okoljih.

75. Javni organi v tretjih državah lahko poskušajo dobiti dostop do prenesenih podatkov:

a) med tranzitom, z dostopom do načinov komuniciranja, ki se uporabljajo za prenos podatkov v državo prejemnika. Ta dostop je lahko pasiven, pri čemer se vsebina sporočila, po možnosti po izbirnem postopku, preprosto skopira. Vendar je dostop lahko tudi aktiven v smislu, da javni organi posežejo v komunikacijski postopek, pri čemer vsebino ne samo preberejo, temveč tudi priredijo ali prikrijejo njene dele;

b) medtem ko so v hrambi predvidenega prejemnika podatkov, tako da sami dostopajo do zmogljivosti za obdelavo ali od prejemnika podatkov zahtevajo, da locira in pridobi podatke, ki jih zanimajo, ter jim jih izroči.

76. V tem oddelku so obravnavani scenariji, v katerih se uporabljajo ukrepi, ki so učinkoviti v obeh primerih. V določenih okoliščinah konkretnega prenosa se lahko uporabljajo in zadostujejo različni dopolnilni ukrepi, če pravo države prejemnika določa samo eno vrsto dostopa. Izvoznik podatkov mora zato s podporo uvoznika podatkov skrbno analizirati njegove obveznosti.

Na primer, ameriški uvozniki podatkov, ki spadajo pod člen 1881a naslova 50 USC (FISA 702), so neposredno zavezani, da odobrijo dostop do uvoženih osebnih podatkov, s katerimi razpolagajo, jih hranijo ali nadzorujejo, ali da jih izročijo. To lahko vključuje katere koli kriptografske ključe, potrebne za zagotovitev razumljivosti podatkov.

77. V scenarijih so opisane konkretne okoliščine in sprejeti ukrepi. Katera koli sprememba scenarijev lahko povzroči različne sklepne ugotovitve.

78. Upravljavci morajo morda uporabljati nekatere ali vse tukaj opisane ukrepe ne glede na raven varstva, ki jo zagotavlja pravo, ki se uporablja za uvoznika podatkov, ker so v konkretnih okoliščinah prenosa potrebni za uskladitev s členoma 25 in 32 Splošne uredbe o varstvu podatkov. Z drugimi besedami, izvozniki morajo morda izvajati ukrepe iz teh priporočil, tudi če so uvozniki njihovih podatkov vključeni v sklep o ustreznosti, enako kot jih morajo morda izvajati upravljavci in obdelovalci, kadar se podatki obdelujejo v EGP.

Primer uporabe 1: Hramba podatkov za namene varnostnega kopiranja in druge namene, za katere se ne zahteva dostop do nešifriranih podatkov

79. Izvoznik podatkov uporablja ponudnika storitev gostovanja v tretji državi za hrambo osebnih podatkov, na primer za namene varnostnega kopiranja.

Če:

1. se osebni podatki obdelujejo z uporabo zapletenega šifriranja pred prenosom;
2. šifrirni algoritem in njegova parametrizacija (npr. dolžina ključa, način delovanja, če je ustrezno) ustrezata najnovejšemu tehničnemu razvoju in se lahko štejeta za odporna na kriptoanalizo, ki jo opravijo javni organi v državi prejemnika, ob upoštevanju virov in tehničnih zmogljivosti (npr. računalniške zmogljivosti za napade s surovo silo), ki so jim na voljo;
3. je v moči šifriranja upoštevano določeno obdobje, v katerem je treba ohraniti zaupnost šifriranih osebnih podatkov;

4. se šifrirni algoritem izvaja brezhibno z ustreznim vzdrževanjem programske opreme, katere skladnost s specifikacijo izbranega algoritma je bila preverjena, na primer s postopkom potrjevanja;
5. se ključi zanesljivo upravljajo (ustvarijo, upravljajo, hranijo, po potrebi povežejo z identiteto predvidenega prejemnika in prekličejo) ter
6. če ključi ostanejo izključno pod nadzorom izvoznika podatkov ali drugih subjektov, ki jim je zaupana ta naloga in prihajajo iz EGP ali tretje države, z ozemlja ali iz enega ali več določenih sektorjev v tretji državi ali mednarodne organizacije, za katere je Komisija v skladu s členom 45 Splošne uredbe o varstvu podatkov ugotovila, da zagotavljajo ustrezno raven varstva podatkov,

potem EOVP meni, da izvedeno šifriranje zagotavlja učinkovit dopolnilni ukrep.

Primer uporabe 2: Prenos psevdonimiziranih podatkov

80. Izvoznik podatkov podatke, ki jih ima, najprej psevdonimizira, nato pa jih prenese v tretjo državo v analizo, na primer za raziskovalne namene.

Če:

1. izvoznik podatkov prenese osebne podatke, obdelane na tak način, da jih brez dodatnih informacij ni več mogoče pripisati določenemu posamezniku, na katerega se nanašajo osebni podatki, ali jih uporabiti za njegovo izpostavitev v večji skupini[69];
2. dodatne informacije hrani izključno izvoznik podatkov, in sicer ločeno v državi članici ali tretji državi, na ozemlju ali v enem ali več določenih sektorjih v tretji državi ali pri mednarodni organizaciji, za katere je Komisija v skladu s členom 45 Splošne uredbe o varstvu podatkov ugotovila, da zagotavljajo ustrezno raven varstva podatkov;
3. razkritje ali nedovoljeno uporabo teh dodatnih informacij preprečujejo ustrezni tehnični in organizacijski zaščitni ukrepi, če je zagotovljeno, da izvoznik podatkov ohrani izključni nadzor nad algoritmom ali odložiščem podatkov, ki omogoča deanonimizacija podatkov na podlagi dodatnih informacij, ter
4. je upravljavec s temeljito analizo zadevnih podatkov ob upoštevanju vseh informacij, s katerimi morda razpolagajo javni organi države prejemnika, ugotovil, da psevdonimiziranih osebnih podatkov niti z navzkrižnim sklicevanjem na te informacije ni mogoče pripisati določenemu ali določljivemu posamezniku,

potem EOVP meni, da opravljena psevdonimizacija zagotavlja učinkovit dopolnilni ukrep.

81. Upoštevajte, da lahko dejavniki, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto posameznika, njegova fizična lokacija ali njegova interakcija s spletno

[69] V skladu s členom 4(5) Splošne uredbe o varstvu podatkov: „‚psevdonimizacija‘ pomeni obdelavo osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku;“.

storitvijo ob določenem času[70], v številnih primerih omogočijo določitev tega posameznika, tudi če njegovo ime, naslov ali drugi neposredni identifikatorji niso navedeni.

82. To zlasti velja, kadar se podatki nanašajo na uporabo informacijskih storitev (čas dostopa, zaporedje uporabljenih funkcij, značilnosti uporabljene naprave itd.). Čisto mogoče je, da za te spletne storitve tako kot za uvoznika osebnih podatkov velja obveznost, da morajo v svoji jurisdikciji omogočiti dostop istim javnim organom, ki bodo potem verjetno razpolagali s podatki o uporabi teh informacijskih storitev s strani posameznika oziroma posameznikov, v katere so ciljno usmerjeni.

83. Glede na to, da je uporaba nekaterih informacijskih storitev javna ali da jih uporabljajo stranke z znatnimi viri, morajo biti upravljavci še posebno previdni, ker javni organi v njihovi jurisdikciji verjetno razpolagajo s podatki o uporabi informacijskih storitev s strani posameznika, v katerega so ciljno usmerjeni.

Primer uporabe 3: Šifrirani podatki, ki se prenesejo v tretje države samo zaradi tranzita

84. Izvoznik podatkov želi prenesti podatke v namembni kraj, za katerega je znano, da zagotavlja ustrezno varstvo v skladu s členom 45 Splošne uredbe o varstvu podatkov. Podatke usmeri prek tretje države.

Če:

1. izvoznik podatkov prenese osebne podatke uvozniku podatkov v jurisdikciji, ki zagotavlja ustrezno varstvo, se podatki prenesejo prek interneta in se lahko geografsko usmerijo prek tretje države, ki ne zagotavlja v bistvu enakovredne ravni varstva;
2. se uporablja šifriranje za prenos, za katerega je zagotovljeno, da so uporabljeni protokoli šifriranja v skladu z najnovejšim tehničnim razvojem in zagotavljajo učinkovito zaščito pred aktivnimi in pasivnimi napadi z viri, za katere je znano, da z njimi razpolagajo javni organi tretje države;
3. je šifriranje mogoče samo zunaj zadevne tretje države;
4. se stranke, vključene v komunikacijo, dogovorijo glede zaupanja vrednega organa za izdajanje potrdil javnega ključa ali infrastrukture javnih ključev;
5. se za zaščito pred aktivnimi in pasivnimi napadi med šifriranim prenosom uporabljajo specifični in najnovejši zaščitni ukrepi;
6. če šifriranje za prenos glede na izkušnje z ranljivostmi uporabljene infrastrukture ali programske opreme samo po sebi ne zagotavlja ustrezne varnosti in so osebni podatki z najnovejšimi šifrirnimi metodami šifrirani tudi od konca do konca na aplikacijski plasti;
7. šifrirni algoritem in njegova parametrizacija (npr. dolžina ključa, način delovanja, če je ustrezno) ustrezata najnovejšemu tehničnemu razvoju in se lahko štejeta za odporna na kriptoanalizo, ki jo opravijo javni organi v državi tranzita, ob upoštevanju virov in tehničnih zmogljivosti (npr. računalniške zmogljivosti za napade s surovo silo), ki so jim na voljo;
8. je v moči šifriranja upoštevano določeno obdobje, v katerem je treba ohraniti zaupnost šifriranih osebnih podatkov;

[70] Člen 4(1) Splošne uredbe o varstvu podatkov: „‚osebni podatki' pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: posameznik, na katerega se nanašajo osebni podatki); določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;".

9. se šifrirni algoritem izvaja brezhibno z ustreznim vzdrževanjem programske opreme, katere skladnost s specifikacijo izbranega algoritma je bila preverjena, na primer s postopkom potrjevanja;
10. je bil obstoj stranskih vrat (v strojni ali programski opremi) izključen;
11. ključe zanesljivo upravlja (ustvari, upravlja, po potrebi hrani, poveže z identiteto predvidenega prejemnika in prekliče) izvoznik ali subjekt, ki mu izvoznik zaupa, v jurisdikciji, ki zagotavlja v bistvu enakovredno raven varstva,

potem EOVP meni, da šifriranje za prenos, po potrebi v povezavi s šifriranjem vsebine od konca do koca, zagotavlja učinkovit dopolnilni ukrep.

Primer uporabe 4: Varovani prejemnik

85. Izvoznik podatkov prenese osebne podatke uvozniku podatkov v tretji državi, ki ga posebej varuje pravo te države, na primer za namene skupne zagotovitve zdravljenja za bolnika ali pravnih storitev stranki.

Če:

1. je v skladu s pravom tretje države rezidenčni uvoznik podatkov izvzet iz potencialno kršitvenega dostopa do podatkov, ki jih hrani za določen namen, na primer na podlagi obveznosti varovanja poslovne skrivnosti, ki velja za uvoznika podatkov;
2. ta izjema zajema vse informacije, s katerimi razpolaga uvoznik podatkov in ki se lahko uporabijo za izogibanje varstvu zaupnih informacij (kriptografski ključi, gesla, druge poverilnice itd.);
3. uvoznik podatkov ne uporablja storitev obdelovalca na način, ki javnim organom omogoča dostop do podatkov, ki jih hrani obdelovalec, tudi uvoznik podatkov ne posreduje podatkov drugemu subjektu, ki ni varovan, na podlagi orodij za prenos iz člena 46 Splošne uredbe o varstvu podatkov;
4. se osebni podatki pred prenosom šifrirajo z najnovejšo metodo, ki zagotavlja, da dešifriranje brez poznavanja dešifrirnega ključa (šifriranje od konca do konca) ne bo mogoče v celotnem obdobju, v katerem morajo biti podatki zaščiteni;
5. dešifrirni ključ hrani izključno uvoznik zaščitenih podatkov in je pred nepooblaščeno uporabo ali razkritjem ustrezno zavarovan z najnovejšimi tehničnimi in organizacijskimi ukrepi ter
6. je izvoznik podatkov zanesljivo ugotovil, da šifrirni ključ, ki ga namerava uporabiti, ustreza dešifrirnemu ključu, ki ga hrani prejemnik,

potem EOVP meni, da izvedeno šifriranje za prenos zagotavlja učinkovit dopolnilni ukrep.

Primer uporabe 5: Deljena ali večstranska obdelava

86. Izvoznik podatkov želi, da osebne podatke obdelujeta skupno dva ali več neodvisnih obdelovalcev v različnih jurisdikcijah, ne da bi jim razkrili njihovo vsebino. Podatke pred prenosom razdeli tako, da noben del, ki ga prejme posamezni obdelovalec, ne zadostuje za celotno ali delno obnovitev osebnih podatkov. Izvoznik podatkov prejme rezultat obdelave od vsakega obdelovalca posebej in prejete dele združi, da dobi končni rezultat, ki so lahko osebni ali zbirni podatki.

Če:

1. izvoznik podatkov obdeluje osebne podatke tako, da jih razdeli na dva ali več delov, od katerih nobenega brez dodatnih informacij ni mogoče več razložiti ali pripisati določenemu posamezniku, na katerega se nanašajo osebni podatki;

2. se vsak del prenese k ločenemu obdelovalcu v drugi jurisdikciji;
3. obdelovalci neobvezno obdelujejo podatke skupno, na primer s takim varnim večstranskim izračunavanjem, pri katerem se nobena informacija ne razkrije nikomur od njih, ki je z njimi razpolagal že pred izračunavanjem;
4. je algoritem, ki se uporablja za skupno izračunavanje, zavarovan pred dejavnimi nasprotniki;
5. ni dokazov o sodelovanju med javnimi organi v zadevnih jurisdikcijah posameznih obdelovalcev, ki bi jim omogočalo dostop do vseh naborov osebnih podatkov, ki jih hranijo obdelovalci, ter obnovitev in uporabo vsebine nešifriranih osebnih podatkov v primerih, ko se s tako uporabo ne bi spoštovalo bistvo temeljnih pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki. Prav tako javni organi katere koli države ne bi smeli imeti dovoljenja za dostop do osebnih podatkov, ki jih hranijo obdelovalci v vseh zadevnih jurisdikcijah;
6. je upravljavec s temeljito analizo zadevnih podatkov ob upoštevanju vseh informacij, s katerimi morda razpolagajo javni organi držav prejemnikov, ugotovil, da delov osebnih podatkov, ki jih prenese k obdelovalcem, niti z navzkrižnim sklicevanjem na te informacije ni mogoče pripisati določenemu ali določljivemu posamezniku,

potem EOVP meni, da deljeno obdelovanje zagotavlja učinkovit dopolnilni ukrep.

Scenariji, v katerih *učinkovitih* ukrepov ni bilo mogoče najti

87. Ukrepi iz spodaj opisanih scenarijev ne bi bili učinkoviti pri zagotavljanju v bistvu enakovredne ravni varstva za podatke, prenesene v tretjo državo, zato jih ni mogoče šteti za dopolnilne ukrepe.

Primer uporabe 6: Prenos k ponudnikom storitev v oblaku ali drugim obdelovalcem, pri katerem se zahteva dostop do nešifriranih podatkov

88. Izvoznik podatkov za obdelavo osebnih podatkov v skladu z njegovimi navodili uporablja ponudnika storitev v oblaku ali drugega obdelovalca v tretji državi.

Če:

1. upravljavec prenese podatke k ponudniku storitev v oblaku ali drugemu obdelovalcu;
2. ponudnik storitev v oblaku ali drug obdelovalec potrebuje dostop do nešifriranih podatkov, da bi lahko opravil dodeljeno nalogo, ter
3. pooblastila javnih organov v državi prejemnika za dostop do prenesenih podatkov presegajo, kar je v demokratični družbi potrebno in sorazmerno,[71]

potem si EOVP glede na trenutno najnovejšo tehnologijo ne more predstavljati učinkovitega tehničnega ukrepa, s katerim bi se preprečila kršitev pravic posameznikov, na katere se nanašajo osebni podatki, s tem dostopom. EOVP ne izključuje možnosti, da bo nadaljnji tehnološki razvoj morda zagotovil ukrepe, ki bodo dosegali predvidene poslovne namene brez potrebe po dostopu do nešifriranih podatkov.

[71] Glej člena 47 in 52 Listine EU o temeljnih pravicah, člen 23(1) Splošne uredbe o varstvu podatkov in Priporočila Evropskega odbora za varstvo podatkov glede evropskih bistvenih jamstev za nadzorne ukrepe.

89. V določenih scenarijih, kjer so nešifrirani osebni podatki tehnično potrebni za izvajanje storitve obdelovalca, tudi šifriranje za prenos in šifriranje shranjenih podatkov skupaj ne pomenita dopolnilnega ukrepa, ki bi zagotavljal v bistvu enakovredno raven varstva, če uvoznik podatkov razpolaga s kriptografskimi ključi.

Primer uporabe 7: Oddaljeni dostop do podatkov za poslovne namene

90. Izvoznik podatkov da osebne podatke na voljo subjektom v tretji državi, da bi jih uporabili za skupne poslovne namene. Značilno skupino lahko sestavljajo upravljavec ali obdelovalec s sedežem na ozemlju države članice, ki prenese osebne podatke k upravljavcu ali obdelovalcu v tretji državi, ki je njegova povezana družba ali subjekt iz skupine podjetij, ki se ukvarjajo s skupno gospodarsko dejavnostjo. Uvoznik podatkov lahko na primer prejete podatke uporablja za izvajanje osebnih storitev za izvoznika podatkov, za kar potrebuje podatke o človeških virih, ali komuniciranje s strankami izvoznika podatkov, ki živijo v Evropski uniji, po telefonu ali e-pošti.

Če:

1. izvoznik podatkov prenese osebne podatke k uvozniku podatkov v tretji državi, tako da jih da na voljo v skupnem informacijskem sistemu na način, ki uvozniku omogoča neposreden dostop do podatkov po lastni izbiri, ali tako da jih z uporabo komunikacijske storitve prenese neposredno, posamično ali v skupini;
2. uvoznik uporablja nešifrirane podatke za svoje namene;
3. pooblastila javnih organov v državi prejemnika za dostop do prenesenih podatkov presegajo, kar je v demokratični družbi potrebno in sorazmerno,

potem si EOVP ne more predstavljati učinkovitega tehničnega ukrepa, s katerim bi se preprečila kršitev pravic posameznikov, na katere se nanašajo osebni podatki, s tem dostopom.

91. V določenih scenarijih, kjer so nešifrirani osebni podatki tehnično potrebni za izvajanje storitve obdelovalca, tudi šifriranje za prenos in šifriranje shranjenih podatkov skupaj ne pomenita dopolnilnega ukrepa, ki bi zagotavljal v bistvu enakovredno raven varstva, če uvoznik podatkov razpolaga s kriptografskimi ključi.

Dodatni pogodbeni ukrepi

92. Ti ukrepi so običajno sestavljeni iz eno-, dvo- ali večstranskih[72] pogodbenih obveznosti.[73] Če se uporablja orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov, ta v večini primerov že vsebuje več (v glavnem pogodbenih) obveznosti izvoznika in uvoznika podatkov, ki naj bi se uporabljale kot zaščitni ukrepi za osebne podatke.[74]

[72] Na primer v zavezujočih poslovnih pravilih, ki bi morala v vsakem primeru urejati nekatere spodaj navedene ukrepe.

[73] Te so zasebne in se ne štejejo za mednarodne sporazume na podlagi mednarodnega javnega prava. V skladu s tem običajno ne morejo zavezovati javnega organa tretje države, ker ni pogodbena stranka, kadar se sklenejo z zasebnimi organi v tretjih državah, kot je poudarilo Sodišče v sodbi C-311/18 (Schrems II), točka 125.

[74] Glej sodbo v zadevi C-311/18 (Schrems II), točka 137, v kateri je sodišče zato priznalo, da standardno pogodbeno določilo vsebuje *„učinkovite mehanizme, ki v praksi omogočajo zagotovitev ravni varstva, ki se zahteva s pravom Unije, in to, da se prenosi osebnih podatkov, ki temeljijo na takih določilih, v primeru kršitve teh določil ali v primeru, da jih ni mogoče spoštovati, začasno ustavijo ali prepovejo“*; glej tudi točko 148.

93. V nekaterih primerih ti ukrepi lahko dopolnjujejo in okrepijo zaščitne ukrepe, ki jih lahko zagotavljata orodje za prenos in zadevna zakonodaja tretje države, če ti ob upoštevanju okoliščin prenosa ne izpolnjujejo vseh pogojev, potrebnih za zagotovitev ravni varstva, ki je v bistvu enakovredna ravni, ki se zagotavlja v EU. Glede na naravo pogodbenih ukrepov, ki običajno ne morejo zavezovati organov zadevne tretje države, če ti niso pogodbena stranka[75], bi bilo treba te ukrepe združiti z drugimi tehničnimi in organizacijskimi ukrepi za zagotovitev zahtevane ravni varstva podatkov. Z izbiro in izvajanjem enega ali več teh ukrepov se ne bo nujno in sistematično zagotovilo, da bo vaš prenos izpolnjeval standard v bistvu enakovrednega varstva, ki se zahteva s pravom EU.

94. Glede na pogodbene ukrepe, ki so že vključeni v orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov, na katero se opira, so lahko koristni tudi dodatni pogodbeni ukrepi, da se lahko izvozniki podatkov s sedežem v EGP seznanijo z novim razvojem, ki vpliva na varstvo podatkov, prenesenih v tretje države.

95. Kot je bilo navedeno, s pogodbenimi ukrepi ne bo mogoče izključiti uporabe zakonodaje tretje države, ki ne izpolnjuje standarda EOVP glede evropskih bistvenih jamstev, kadar morajo uvozniki v skladu z zakonodajo izpolniti ukaze za razkritje podatkov, ki jih prejmejo od javnih organov.[76]

96. V nadaljevanju je navedenih nekaj primerov teh možnih pogodbenih ukrepov, ki so razvrščeni v skladu z njihovo naravo.

Določitev pogodbene obveznosti za uporabo posebnih tehničnih ukrepov

97. ***Glede na konkretne okoliščine prenosov je v pogodbi morda treba določiti, da je treba za predvidene prenose uvesti posebne tehnične ukrepe (glej zgoraj predlagane tehnične ukrepe).***

98. ***Pogoji za učinkovitost:***

- To določilo bi bilo lahko učinkovito v primerih, ko izvoznik opredeli potrebo po tehničnih ukrepih. Nato bi bilo treba to zagotoviti v pravni obliki, s čimer se zagotovi, da se tudi uvoznik zaveže, da bo po potrebi uvedel potrebne tehnične ukrepe.

Obveznosti glede preglednosti:

99. ***Izvoznik bi lahko k pogodbi dodal priloge z informacijami, ki bi jih uvoznik po svojih najboljših močeh zagotovil o dostopu javnih organov do podatkov, vključno na področju obveščevalnih podatkov, če je zakonodaja v namembni državi v skladu z evropskimi bistvenimi jamstvi EOVP. To bi lahko izvozniku podatkov pomagalo izpolniti obveznost glede dokumentiranja svoje ocene ravni varstva v tretji državi.***

100. Od uvoznika bi se na primer lahko zahtevalo, naj:

(1) navede zakone in druge predpise v namembni državi, ki se uporabljajo za uvoznika ali njegove (pod)obdelovalce, v skladu s katerimi bi javni organi imeli dostop do osebnih podatkov, ki so predmet prenosa, zlasti na področju obveščevalne dejavnosti, kazenskega pregona ter upravnega in regulativnega nadzora, ki se uporabljajo za prenesene podatke;

[75] C-311/18 (Schrems II), točka 125.
[76] Sodba Sodišča v zadevi C-311/18 (Schrems II), točka 132.

(2) če ni zakonodaje, ki bi urejala dostop javnih organov do podatkov, na podlagi svojih izkušenj ali poročil iz različnih virov (npr. od partnerjev, iz javno dostopnih virov, nacionalne sodne prakse in sklepov nadzornih organov) zagotovi informacije in statistične podatke o dostopu javnih organov do osebnih podatkov v podobnih primerih prenosa zadevnih podatkov (tj. na specifičnem regulativnem področju; v zvezi z vrsto subjektov, med katere spada uvoznik podatkov ...);
(3) navede, kateri ukrepi so bili sprejeti za preprečitev dostopa do prenesenih podatkov (če sploh);
(4) zagotovi dovolj podrobne informacije o vseh zahtevah javnih organov za dostop do osebnih podatkov, ki jih je uvoznik prejel v določenem časovnem obdobju,[77] zlasti na področjih iz točke (1) zgoraj, ki vsebujejo informacije o prejetih zahtevah, zahtevanih podatkih, organu, ki je predložil zahtevo, in pravni podlagi za razkritje ter obsegu, v katerem je razkril zahtevane podatke;[78]
(5) navede, ali in v kakšnem obsegu mu je zakonsko prepovedano zagotoviti informacije iz točk (1) do (5) zgoraj.

101. Te informacije bi se lahko zagotovile na podlagi strukturiranih vprašalnikov, ki bi jih uvoznik izpolnil in podpisal, ter dopolnile z uvoznikovo pogodbeno obveznostjo, da mora v določenem roku sporočiti vsako morebitno spremembo teh informacij, kar je v skladu z veljavno prakso za postopek potrebne skrbnosti.

102. ***Pogoji za učinkovitost:***

- Uvoznik mora biti sposoben te informacije, potem ko jih uspe pridobiti po svojih najboljših močeh, zagotoviti izvozniku po svoji najboljši vednosti.[79]
- S to obveznostjo uvoznika se zagotovi, da se izvoznik seznani s tveganji, povezanimi s prenosom podatkov v tretjo državo, in ostaja seznanjen z njimi. Tako bo izvoznik lahko odstopil od sklenitve pogodbe ali, če se informacije po njeni sklenitvi spremenijo, izpolnil svojo obveznost, da začasno ustavi prenos podatkov in/ali odstopi od pogodbe, če pravo tretje države, zaščitni ukrepi, ki jih vsebuje uporabljeno orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov, in kakršni koli dodatni zaščitni ukrepi, ki jih je morda sprejel, ne morejo več zagotavljati ravni varstva, ki je v bistvu enakovredna ravni v EU. Vendar ta obveznost ne upravičuje uvoznikovega razkritja osebnih podatkov, prav tako pa se zaradi nje ne pričakuje, da ne bo nadaljnjih zahtev za dostop.

***

103. ***Izvoznik bi lahko dodal tudi določila, s katerimi uvoznik potrjuje, da (1) ni namensko ustvaril stranskih vrat ali podobnih programov, ki bi jih bilo mogoče uporabiti za dostop do sistema in/ali osebnih podatkov; da (2) ni namensko ustvaril ali spremenil svojih poslovnih procesov na način, ki omogoča dostop do osebnih podatkov ali sistemov, ter da (3) mu v skladu z nacionalnim pravom ali vladno***

[77] Dolžina obdobja naj bo odvisna od tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, katerih podatki so predmet zadevnega prenosa – npr. zadnje leto pred sklenitvijo dokumenta o izvozu podatkov z izvoznikom podatkov.
[78] Izpolnitev te obveznosti sama po sebi ne pomeni zagotovitve ustrezne ravni varstva. Hkrati pa je treba zaradi vsakega neustreznega razkritja, ki se je dejansko zgodilo, izvesti dopolnilne ukrepe.
[79] Glej točko 32.5 zgoraj.

***politiko ni treba ustvariti ali vzdrževati stranskih vrat ali omogočiti dostopa do osebnih podatkov ali sistemov ter imeti ali izročiti šifrirnega ključa.*[80]**

104. ***Pogoji za učinkovitost:***

- Zaradi obstaja zakonodaje ali vladnih politik, ki uvoznikom preprečujejo razkritje teh informacij, je lahko to določilo neučinkovito. Uvoznik tako ne bo mogel skleniti pogodbe ali pa bo moral izvoznika obvestiti, da ne more več izpolnjevati pogodbenih obveznosti.[81]
- Pogodba mora vključevati kazni in/ali možnost izvoznika, da v kratkem času odstopi od pogodbe, če uvoznik ne razkrije obstoja stranskih vrat ali podobnih programov, prirejenih poslovnih procesov ali katere koli zahteve za izvedbo kar koli od navedenega ali če izvoznika ne obvesti takoj, ko je seznanjen z njihovim obstojem.

***

105. ***Izvoznik bi lahko okrepil svojo pristojnost za izvedbo revizij*[82] *ali pregledov zmogljivosti za obdelavo podatkov uvoznika, na kraju samem in/ali na daljavo, da bi preveril, ali so bili podatki razkriti javnim organom in pod kakšnimi pogoji (dostop, ki ne presega, kar je v demokratični družbi potrebno in sorazmerno), na primer z določitvijo kratkega časa in mehanizmov, ki zagotavljajo hitro posredovanje inšpekcijskih organov in povečajo avtonomijo izvoznika pri njihovi izbiri.***

106. ***Pogoji za učinkovitost:***

- Za popolno učinkovitost bi bilo treba v obseg revizije pravno in tehnično zajeti vse obdelave uvoznikovih obdelovalcev ali podobdelovalcev osebnih podatkov, prenesenih v tretjo državo.
- Dnevniki dostopov in druge podobne sledi bi morali biti zaščiteni pred nedovoljenimi posegi, tako da revizorji lahko najdejo dokaze za razkritje. Dnevniki dostopov in druge podobne sledi bi morali tudi razlikovati med dostopi zaradi rednega poslovnega delovanja in dostopi zaradi ukazov ali zahtev za dostop.

***

107. ***Če je bilo najprej ocenjeno in se je štelo, da pravo in praksa tretje države uvoznika za podatke, ki jih prenese izvoznik, zagotavljata v bistvu enakovredno raven varstva, kot se jim zagotavlja v EU, bi lahko izvoznik še vedno okrepil obveznost uvoznika podatkov, da ga mora nemudoma obvestiti, če ne more več izpolnjevati pogodbenih obveznosti in zato ne more zagotavljati skladnosti z zahtevanim standardom „v bistvu enakovredne ravni varstva podatkov“.*[83]**

[80] To določilo je pomembno za zagotovitev ustrezne ravni varstva prenesenih osebnih podatkov in bi se po navadi moralo zahtevati.
[81] Glej točko 32.5 zgoraj.
[82] Glej na primer določilo 5(f) standardnih pogodbenih določil med upravljavci in obdelovalci, Sklep 2010/87/EU; revizije bi se lahko zagotavljale tudi v okviru kodeksa ravnanja ali prek potrjevanja.
[83] Določilo 5(a) in (d)(i) standardnih pogodbenih določil, Sklep 2010/87/EU.

108. Ta nesposobnost izpolnjevanja obveznosti lahko izhaja iz sprememb zakonodaje ali prakse tretje države.[84] Določila bi lahko vsebovala specifične in stroge roke ter postopke za hitro začasno ustavitev prenosa podatkov in/ali odstop od pogodbe ter uvoznikovo vračilo ali izbris prejetih podatkov. Izvoznik bi si moral s spremljanjem prejetih zahtev, njihovega obsega in učinkovitosti ukrepov, sprejetih za njihovo zavračanje, zagotoviti dovolj dokazov, da bi izpolnil svojo dolžnost, da začasno ustavi ali preneha prenos podatkov in/ali odstopi od pogodbe.

109. ***Pogoji za učinkovitost:***

- Obvestilo je treba izdati, preden se odobri dostop do podatkov. Sicer so bile lahko do takrat, ko izvoznik prejme obvestilo, že kršene pravice posameznika, če zahteva temelji na pravu zadevne tretje države, ki presega, kar je dovoljeno v skladu z ravnjo varstva podatkov, ki se zagotavlja v skladu s pravom EU. Z obvestilom se še vedno lahko preprečijo prihodnje kršitve in izvozniku omogoči, da izpolni svojo dolžnost, da začasno ustavi prenos osebnih podatkov v tretjo državo in/ali odstopi od pogodbe.
- Uvoznik podatkov mora spremljati ves razvoj na pravnem ali političnem področju, ki bi lahko povzročil, da ne bi več mogel izpolnjevati svojih obveznosti, ter izvoznika podatkov nemudoma obvestiti o vsaki taki spremembi in razvoju, po možnosti pred njihovo izvedbo, da bi lahko izvoznik podatkov od uvoznika pridobil nazaj podatke.
- Določila bi morala zagotoviti hiter mehanizem, s katerim izvoznik podatkov uvoznika podatkov pooblasti, da takoj zavaruje ali mu vrne podatke, ali če to ni izvedljivo, da jih izbriše ali šifrira brez nepotrebnega čakanja na izvoznikova navodila, če je dosežen določen prag, glede katerega se izvoznik in uvoznik podatkov skupno dogovorita. Uvoznik bi moral ta mehanizem izvajati od začetka prenosa podatkov in ga redno preskušati za zagotovitev, da ga je mogoče hitro uporabiti.
- Druga določila bi lahko izvozniku omogočila spremljanje uvoznikovega izpolnjevanja teh obveznosti z revizijami, pregledi in drugimi ukrepi preverjanja ter njihovo uveljavljanje s kaznimi za uvoznika in/ali izvoznikovo sposobnostjo, da začasno ustavi prenos in/ali takoj odstopi od pogodbe.

***

110. ***Če to dopušča nacionalno pravo v tretji državi, bi se lahko s pogodbo okrepile obveznosti uvoznika glede preglednosti, in sicer z zagotovitvijo metode, s katero se uvoznik zaveže, da bo redno (vsaj vsakih 24 ur) objavljal kriptografsko podpisano sporočilo, v katerem bo izvoznika obvestil, da do določenega datuma in časa ni prejel nobenega ukaza za razkritje osebnih podatkov ali česa podobnega (angl. Warrant Canary). Če izvoznik ne bo prejel naslednjega obvestila, bo to zanj dokaz, da je uvoznik morda prejel ukaz.***

111. ***Pogoji za učinkovitost:***

- Predpisi tretje države morajo uvozniku podatkov dovoljevati, da izvozniku izda to obliko pasivnega obvestila.

[84] Glej sodbo v zadevi C-311/18 (Schrems II), točko 139, v kateri Sodišče zagovarja, da *„čeprav klavzula 5(d)(i) prejemniku prenosa osebnih podatkov v primeru zakonodaje, ki mu to preprečuje, kot je prepoved po kazenski zakonodaji zaradi ohranjanja zaupnosti kazenske preiskave, omogoča, da upravljavca, ki ima sedež v Uniji, ne obvesti o pravno zavezujočih zahtevah organa kazenskega pregona za posredovanje osebnih podatkov, pa mora na podlagi klavzule 5(a) iz Priloge k Sklepu SPK upravljavca vseeno obvestiti, da ne more upoštevati standardnih določil o varstvu podatkov“*.

- Izvoznik podatkov mora samodejno spremljati obvestila po navedeni metodi.
- Uvoznik podatkov mora zagotoviti, da je njegov zasebni ključ za podpisovanje navedenih obvestil varno shranjen in da ga s predpisi tretje države ni mogoče prisiliti, da po navedeni metodi izdaja lažna obvestila. V ta namen bi bilo lahko koristno, da se zahteva več podpisov različnih oseb in/ali da tako obvestilo izdaja oseba zunaj jurisdikcije tretje države.

Obveznosti glede sprejemanja posebnih ukrepov

112. ***Uvoznik bi se lahko zavezal, da bo v skladu s pravom namembne države ocenil zakonitost vsakega ukaza za razkritje podatkov, zlasti, ali je v okviru pooblastil javnega organa, ki ga je izdal, ter da bo ukazu ugovarjal, če bo po skrbni oceni ugotovil, da v skladu s pravom namembne države obstajajo razlogi za to. V primeru ugovora bi moral uvoznik podatkov poiskati začasne ukrepe za odložitev učinkov ukaza, dokler sodišče ne odloči o njegovi utemeljenosti. Uvoznik bi imel obveznost, da zahtevanih osebnih podatkov ne razkrije, dokler se to ne zahteva v skladu z veljavnimi postopkovnimi predpisi. Uvoznik podatkov bi se tudi zavezal, da bo pri odzivu na ukaz zagotovil minimalno dopustno količino informacij v skladu z razumno razlago ukaza.***

113. ***Pogoji za učinkovitost:***

- Pravni red tretje države mora zagotavljati učinkovite pravne poti za ugovor zoper ukaze za razkritje podatkov.
- To določilo bo vedno zagotovilo zelo omejeno dodatno varstvo, ker je lahko ukaz za razkritje podatkov zakonit v skladu s pravnim redom tretje države, vendar ta pravni red morda ne izpolnjuje standardov EU. Ta pogodbeni ukrep bo treba nujno dopolniti z drugimi dopolnilnimi ukrepi.
- Ugovor zoper ukaze mora imeti v skladu s pravom tretje države odložilni učinek. V nasprotnem primeru bi javni organi še vedno imeli dostop do posameznikovih podatkov, vsak nadaljnji ukrep v korist posameznika pa bi imel omejen učinek, ki bi mu omogočil, da zahteva povračilo škode zaradi negativnih posledic razkritja podatkov.
- Uvoznik bo moral biti sposoben izvozniku dokumentirati in dokazati ukrepe, ki jih je po najboljših močeh sprejel za izpolnitev te obveznosti.

***

114. ***V enakem primeru, kot je opisan zgoraj, bi se uvoznik lahko zavezal, da bo javni organ, ki je izdal ukaz, obvestil o nezdružljivosti ukaza z zaščitnimi ukrepi, ki jih vsebuje orodje za prenos iz člena 46 Splošne uredbe o varstvu podatkov[85], in posledičnem navzkrižju svojih obveznosti. Uvoznik bi hkrati in v najkrajšem možnem času obvestil izvoznika in/ali pristojni nadzorni organ iz EGP, če je to mogoče v skladu s pravnim redom tretje države.***

[85] Na primer, standardna pogodbena določila določajo, da so se podatki obdelovali, vključno z njihovim prenosom, in se bodo še naprej obdelovali v skladu z *„veljavnim pravom o varstvu podatkov“.* To pravo je opredeljeno kot *„zakonodaja, ki varuje temeljne pravice in svoboščine posameznikov ter zlasti njihovo pravico do zasebnosti glede obdelave osebnih podatkov, ki jo uporablja upravljavec podatkov v državi članici, kjer je sedež izvoznika podatkov“.* Sodišče potrjuje, da so določbe Splošne uredbe o varstvu podatkov v povezavi z Listino EU o temeljnih pravicah del te zakonodaje, glej sodbo Sodišča v zadevi C-311/18 (Schrems II), točka 138.

115. ***Pogoji za učinkovitost:***

- Te informacije o varstvu, ki ga zagotavlja pravo EU, in navzkrižju obveznosti bi morale imeti nekaj pravnega učinka v pravnem redu tretje države, kot sta sodna ali upravna presoja ukaza ali zahteve za dostop, zahteva za sodni nalog in/ali začasna odložitev ukaza, da bi se za podatke zagotovilo dodatno varstvo.
- Pravni sistem države uvozniku ne sme preprečevati, da bi izvoznika ali vsaj pristojni nadzorni organ iz EGP obvestil o prejetem ukazu ali zahtevi za dostop.
- Uvoznik bo moral biti sposoben izvozniku dokumentirati in dokazati ukrepe, ki jih je po najboljših močeh sprejel za izpolnitev te obveznosti.

Omogočanje posameznikom, na katere se nanašajo osebni podatki, da uveljavljajo svoje pravice

116. ***Pogodba bi lahko določala, da je dostop do osebnih podatkov, prenesenih kot navadno besedilo pri običajnem poslovanju (vključno v podpornih primerih), mogoč samo z izrecno ali implicitno privolitvijo izvoznika in/ali posameznika, na katerega se nanašajo osebni podatki.***

117. ***Pogoji za učinkovitost:***

- To določilo bi bilo lahko učinkovito v primerih, ko uvozniki prejmejo zahteve javnih organov za prostovoljno sodelovanje, v nasprotju na primer z dostopom javnih organov do podatkov, ki se zgodi brez vednosti uvoznika podatkov ali proti njegovi volji.
- V nekaterih primerih posameznik, na katerega se nanašajo osebni podatki, morda ne more ugovarjati dostopu ali dati privolitve za dostop, ki izpolnjuje vse pogoje, določene v skladu s pravom EU (prostovoljna, izrecna, informirana in nedvoumna) (npr. zaposleni)[86].
- Zaradi nacionalnih predpisov ali politik, ki od uvoznika zahtevajo, naj ne razkrije ukaza za dostop, je lahko to določilo neučinkovito, če ga ni mogoče podpreti s tehničnimi metodami, ki zahtevajo posredovanje izvoznika ali posameznika, na katerega se nanašajo osebni podatki, da se omogoči dostop do podatkov v navadnem besedilu. Taki tehnični ukrepi za omejitev dostopa se lahko predvidijo zlasti, če se dostop omogoči samo v posebnih podpornih ali storitvenih primerih, vendar se sami podatki hranijo v EGP.

***

118. ***Pogodba bi lahko uvoznika in/ali izvoznika zavezovala, da mora posameznika, na katerega se nanašajo osebni podatki, takoj obvestiti o zahtevi ali ukazu, ki ga prejme od javnih organov tretje države, ali o uvoznikovi nesposobnosti za izpolnitev pogodbenih obveznosti, da lahko posameznik, na katerega se nanašajo osebni podatki, pridobi informacije in učinkovito varstvo (npr. z vložitvijo pritožbe pri pristojnem nadzornem in/ali sodnem organu ter na sodiščih tretje države dokaže svoje procesno upravičenje).***

119. ***Pogoji za učinkovitost:***

- S tem obvestilom bi bilo mogoče posameznika, na katerega se nanašajo osebni podatki, opozoriti na morebitne dostope javnih organov v tretjih državah do njegovih podatkov. Posameznik, na katerega se nanašajo osebni podatki, bi tako lahko pri izvoznikih pridobil

[86] Člen 4(11) Splošne uredbe o varstvu podatkov.

dodatne informacije in vložil pritožbo pri pristojnem nadzornem organu. To določilo bi lahko rešilo tudi nekatere težave, s katerimi se lahko posameznik sreča pri dokazovanju svojega procesnega upravičenja (*locus standi*) pri sodiščih tretje države do ugovora zoper dostop javnih organov do njegovih podatkov.

- Nacionalni predpisi in politike lahko preprečujejo to obvestilo posameznika, na katerega se nanašajo osebni podatki. Izvoznik in uvoznik bi se lahko kljub temu zavezala, da bosta posameznika, na katerega se nanašajo osebni podatki, obvestila takoj, ko so odpravljene omejitve za razkritje podatkov, in si po najboljših močeh prizadevala za opustitev prepovedi razkritja. Izvoznik ali pristojni nadzorni organ bi lahko posameznika, na katerega se nanašajo osebni podatki, obvestila vsaj o začasni ustavitvi ali prenehanju prenosa njegovih osebnih podatkov, ker uvoznik zaradi prejema zahteve za dostop ne more izpolniti pogodbenih obveznosti.

***

120. ***Pogodba bi lahko izvoznika in uvoznika zavezovala, da morata posamezniku, na katerega se nanašajo osebni podatki, pomagati pri uresničevanju njegovih pravic v jurisdikciji tretje države z ad hoc mehanizmi pravnih sredstev in pravnim svetovanjem.***

121. ***Pogoji za učinkovitost:***

- Nacionalni predpisi in politike lahko določajo pogoje, ki lahko ogrozijo učinkovitost predvidenih ad hoc mehanizmov pravnih sredstev.
- Posamezniku, na katerega se nanašajo osebni podatki, bi se lahko pomagalo s pravnim svetovanjem, zlasti glede na to, kako zapleteno in drago je lahko zanj, da razume pravni sistem tretje države in sproži pravne postopke iz tujine, morebiti v tujem jeziku. Vendar se bo s tem določilom vedno zagotovilo le omejeno dodatno varstvo, saj pomoč in pravno svetovanje posameznikom, na katere se nanašajo osebni podatki, sama po sebi ne moreta odpraviti nezmožnosti pravnega reda tretje države, da zagotovi raven varstva, ki bi bila v bistvu enakovredna ravni, ki se zagotavlja v EU. Ta pogodbeni ukrep bo treba nujno dopolniti z drugimi dopolnilnimi ukrepi.

Ta dopolnilni ukrep bi bil učinkovit samo, če pravo tretje države zagotavlja pravna sredstva pred svojimi nacionalnimi sodišči ali če obstaja ad hoc mehanizem pravnih sredstev. Vendar to nikakor ne bi bil učinkovit dopolnilni ukrep proti ukrepom nadzora, če ne obstaja mehanizem pravnih sredstev.

Organizacijski ukrepi

122. Dodatni organizacijski ukrepi so lahko notranje politike, organizacijske metode ter standardi, ki bi jih lahko upravljavci in obdelovalci uporabljali zase in jih uvedli za uvoznike podatkov v tretjih državah. Z njimi se lahko prispeva k zagotavljanju doslednega izvajanja varstva osebnih podatkov v celotnem ciklu obdelave. Z organizacijskimi ukrepi se lahko tudi izboljša seznanjenost izvoznikov s tveganjem in poskusi za pridobitev dostopa do podatkov v tretjih državah ter njihova sposobnost, da se odzovejo nanje. Z izbiro in izvajanjem enega ali več teh ukrepov se ne bo nujno in sistematično zagotovilo, da bo vaš prenos izpolnjeval standard v bistvu enakovrednega varstva, ki se zahteva s pravom EU. Glede ne posebne okoliščine prenosa in opravljeno oceno zakonodaje tretje države je treba z organizacijskimi ukrepi dopolniti pogodbene in/ali tehnične ukrepe, da bi se zagotovila raven varstva osebnih podatkov, ki bi bila v bistvu enakovredna ravni, ki se zagotavlja v EU.

123. Oceno najprimernejših ukrepov je treba opraviti za vsak primer posebej, ob upoštevanju, da morajo upravljavci in obdelovalci spoštovati načelo odgovornosti. V nadaljevanju EOVP navaja nekaj primerov organizacijskih ukrepov, ki jih lahko izvajajo izvozniki, vendar seznam ni izčrpen in so lahko ustrezni tudi drugi ukrepi.

Notranje politike za urejanje prenosov, zlasti v skupinah podjetij

124. ***Sprejetje ustreznih notranjih politik z jasno dodelitvijo odgovornosti za prenose podatkov, načinov poročanja in standardnih operativnih postopkov za primere prikritih ali uradnih zahtev javnih organov za dostop do podatkov. Te politike lahko zlasti pri prenosih med skupinami podjetij med drugim vključujejo tudi imenovanje posebne skupine, ki bi morala imeti sedež v EGP, sestavljene iz strokovnjakov za informacijsko tehnologijo, varstvo podatkov in zakonodajo o varstvu zasebnosti, da bi obravnavala zahteve, ki vključujejo osebne podatke, prenesene iz EU, o prejemu takih zahtev obveščala višje pravno in korporativno vodstvo ter izvoznika podatkov, opredelila postopkovne korake za ugovor zoper nesorazmerne ali nezakonite zahteve ter posameznikom, na katere se nanašajo osebni podatki, zagotavljala pregledne informacije.***

125. Razvoj posebnih postopkov usposabljanja za osebje, odgovorno za upravljanje zahtev javnih organov za dostop do osebnih podatkov, ki bi jih bilo treba redno posodabljati, da bi se tako upoštevala zakonodajni razvoj in razvoj sodne prakse v tretji državi in EGP. Postopki usposabljanja bi morali vključevati zahteve prava EU v zvezi z dostopom javnih organov do osebnih podatkov, zlasti iz člena 52(1) Listine o temeljnih pravicah. Osebje bi bilo treba ozaveščati zlasti z oceno praktičnih primerov zahtev javnih organov za dostop do podatkov in uporabo standarda iz člena 52(1) Listine o temeljnih pravicah za te praktične primere. Pri takem usposabljanju bi bilo treba upoštevati posebne okoliščine uvoznika podatkov, na primer zakonodajo in druge predpise tretje države, ki veljajo za uvoznika podatkov, ter ga po možnosti razviti v sodelovanju z izvoznikom podatkov.

126. ***Pogoji za učinkovitost:***

- Te politike se lahko predvidijo samo za tiste primere, ko je zahteva javnih organov v tretji državi združljiva s pravom EU.[87] Če zahteva ni združljiva, te politike ne bi zadostovale za zagotovitev ustrezne ravni varstva osebnih podatkov, in je zato treba, kot je bilo navedeno zgoraj, prenose ustaviti ali uvesti ustrezne dopolnilne ukrepe za preprečitev dostopa.

Ukrepi preglednosti in odgovornosti

127. ***Dokumentirajte in evidentirajte zahteve za dostop, prejete od javnih organov, in zagotovljeni odziv, skupaj s pravno utemeljitvijo in vključenimi akterji (npr. ali je bil izvoznik obveščen in njegov odgovor, ocena skupine, odgovorne za obravnavanje teh zahtev, itd.). To evidenco bi bilo treba dati na voljo izvozniku podatkov, ki bi jo nato moral po potrebi predložiti zadevnim posameznikom, na katere se nanašajo osebni podatki.***

128. ***Pogoji za učinkovitost:***

- Nacionalna zakonodaja v tretji državi lahko preprečuje razkritje zahtev ali bistvenih informacij iz njih, zato ta praksa ni učinkovita. Uvoznik podatkov bi moral izvoznika obvestiti, da takih

[87] Glej sodbo v zadevah C-362/14 (Schrems I), točka 94, in C-311/18 (Schrems II), točke 168, 174, 175 in 176.

dokumentov in evidenc ne more zagotoviti in mu torej omogočiti, da začasno ustavi prenose, če bi se zaradi take nesposobnosti znižala raven varstva.

***

129. ***Redno objavljanje poročil ali povzetkov o preglednosti v zvezi z vladnimi zahtevami za dostop do podatkov in vrsti zagotovljenega odgovora, če je objavljanje v skladu z lokalnim pravom.***

130. ***Pogoji za učinkovitost:***

- Zagotovljene informacije bi morale biti relevantne, jasne in čim bolj podrobne. Nacionalna zakonodaja v tretji državi lahko preprečuje razkritje podrobnih informacij. V teh primerih bi si moral uvoznik podatkov po svojih najboljših močeh prizadevati za objavo statističnih informacij ali podobnih zbirnih informacij.

Organizacijske metode in ukrepi najmanjšega obsega podatkov

131. ***Koristni ukrepi v okviru prenosa so lahko tudi že obstoječe organizacijske zahteve v skladu z načelom odgovornosti, kot je sprejetje politik strogega in razdrobljenega dostopa do podatkov in zaupnosti ter dobrih praks, ki temeljijo na dosledni uporabi načela potrebe po seznanitvi ter se spremljajo z rednimi revizijami in uveljavljajo z disciplinskimi ukrepi. Pri tem bi bilo treba upoštevati najmanjši obseg podatkov, da bi se omejila izpostavljenost osebnih podatkov nepooblaščenemu dostopu. Na primer, morda v nekaterih primerih nekaterih podatkov ne bo treba prenesti (npr. pri oddaljenem dostopu do podatkov v EGP, kot je v podpornih primerih, kadar se omogoči omejen dostop namesto neomejenega ali kadar se za izvajanje storitve zahteva samo prenos omejenega nabora podatkov in ne celotne podatkovne zbirke).***

132. ***Pogoji za učinkovitost:***

- Da bi se spremljala in uveljavljala skladnost z ukrepi najmanjšega obsega podatkov tudi v okviru prenosa, bi bilo treba uvesti redne revizije in stroge disciplinske ukrepe.
- Izvoznik podatkov mora pred prenosom opraviti oceno osebnih podatkov, s katerimi razpolaga, da bi opredelil nabore podatkov, ki niso potrebni za namene prenosa in se zato ne bodo delili z uvoznikom podatkov.
- Ukrepe najmanjšega obsega podatkov bi morali spremljati tehnični ukrepi, da se prepreči nepooblaščen dostop do podatkov. Na primer, z izvajanjem mehanizmov varnega večstranskega izračunavanja in širjenjem šifriranih naborov podatkov med različnimi zaupanja vrednimi subjekti se lahko z zasnovo prepreči razkritje določljivih podatkov zaradi enostranskega dostopa.

***

133. ***Oblikovanje dobrih praks za ustrezno in pravočasno vključitev in zagotovitev dostopa uradni osebi za varstvo podatkov, če obstaja, ter pravni in notranji revizijski službi do informacij o zadevah, povezanih z mednarodnimi prenosi osebnih podatkov.***

134. ***Pogoji za učinkovitost:***

- Uradni osebi za varstvo podatkov, če obstaja, ter pravni in notranji revizijski ekipi se morajo pred prenosom zagotoviti vse zadevne informacije ter se je treba z njimi posvetovati glede potrebe po prenosu in morebitnih dodatnih zaščitnih ukrepih.
- Zadevne informacije bi morale na primer vključevati oceno potrebe po prenosu določenih osebnih podatkov, pregled veljavne zakonodaje tretje države ter zaščitne ukrepe, za katere se je uvoznik zavezal, da jih bo izvajal.

Sprejetje standardov in dobrih praks

135. ***Sprejetje strogih politik zagotavljanja varnosti in zasebnosti podatkov na podlagi potrjevanja EU, kodeksov ravnanja ali mednarodnih standardov (npr. standardi ISO) in dobrih praks (npr. ENISA), ob ustreznem upoštevanju najnovejšega tehnološkega razvoja, v skladu s tveganjem za kategorije obdelanih podatkov in verjetnostjo poskusov javnih organov za dostop do njih.***

Drugo

136. ***Sprejetje in redni pregledi notranjih politik za oceno primernosti izvedenih dopolnilnih ukrepov ter po potrebi opredelitev in izvajanje dodatnih ali alternativnih rešitev za zagotovitev ohranitve enakovredne ravni varstva prenesenih osebnih podatkov, kot se jim zagotavlja v EU.***

***

137. ***Zaveze uvoznika podatkov, da ne bo sodeloval pri nadaljnjih prenosih osebnih podatkov v isti ali drugih tretjih državah ali da bo začasno ustavil nadaljnje prenose, če se v tretji državi ne bo mogla zagotoviti enakovredna raven varstva osebnih podatkov, kot se zagotavlja v EU.***[88]

[88] C-311/18 (Schrems II), točki 135 in 137.

PRILOGA 3: MOŽNI VIRI INFORMACIJ ZA OCENO TRETJE DRŽAVE

138. Uvoznik vaših podatkov bi vam moral biti sposoben zagotoviti ustrezne vire in informacije o tretji državi, v kateri ima sedež, ter pravu, ki se uporablja zanjo. Sklicujete se lahko tudi na druge vire informacij, kot so navedeni na spodnjem neizčrpnem seznamu:

- sodna praksa Sodišča Evropske unije in Evropskega sodišča za človekove pravice (ESČP)[89], kot je navedena v priporočilih iz evropskih bistvenih jamstev;[90]
- sklepi o ustreznosti v namembni državi, če prenos temelji na drugačni pravni podlagi;[91]
- resolucije in poročila medvladnih organizacij, kot so Svet Evrope[92], drugih regionalnih organov[93] ter organov in agencij Združenih narodov (npr. Svet za človekove pravice[94], Odbor za človekove pravice[95]);
- nacionalna sodna praksa ali sklepi neodvisnih sodnih ali upravnih organov, pristojnih za zasebnost in varstvo podatkov tretjih držav;
- poročila akademskih institucij in organizacij civilne družbe (npr. nevladnih organizacij in panožnih združenj).

[89] Glej informativni pregled sodne prakse ESČP o množičnem nadzoru: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf.
[90] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions.
[91] C-311/18 (Schrems II), točka 141; glej sklepe o ustreznosti na spletnem naslovu https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_sl.
[92] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions.
[93] Glej na primer poročila Medameriške komisije za človekove pravice za posamezne države, https://www.oas.org/en/iachr/reports/country.asp.
[94] Glej https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx.
[95] Glej: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5.