Smjernice

Smjernice 07/2022 o certificiranju kao alatu za prijenose

Verzija 2.0

Doneseno 14. veljače 2023.

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

PREGLED VERZIJA

Verzija 1.0	14. lipnja 2022.	Donošenje Smjernica za javno savjetovanje
Verzija 2.0	14. veljače 2023.	Donošenje Smjernica nakon javnog savjetovanja

SAŽETAK

Člankom 46. Opće uredbe o zaštiti podataka (OUZP) zahtijeva se da izvoznici podataka uspostave odgovarajuće zaštitne mjere za prijenose osobnih podataka trećim zemljama ili međunarodnim organizacijama. U tu se svrhu OUZP-om diversificiraju odgovarajuće zaštitne mjere koje izvoznici podataka mogu primjenjivati u skladu s člankom 46. kao okvir za prijenose trećim zemljama uvođenjem, među ostalim, certificiranja kao novog mehanizma prijenosa (članak 42. stavak 2. i članak 46. stavak 2. točka (f) OUZP-a).

Ovim se smjernicama savjetuje o primjeni članka 46. stavka 2. točke (f) OUZP-a o prijenosima osobnih podataka trećim zemljama ili međunarodnim organizacijama na temelju certificiranja. Ovaj se dokument sastoji od četiri odjeljka i Priloga.

U prvom dijelu dokumenta („OPĆE ODREDBE") pojašnjava se da se smjernicama dopunjuju postojeće opće Smjernice 1/2018 o certificiranju i da se njima rješavaju posebni zahtjevi iz poglavlja V. OUZP-a koji se primjenjuju kada se certificiranje upotrebljava kao alat za prijenos. U skladu s člankom 44. OUZP-a svaki prijenos osobnih podataka trećim zemljama ili međunarodnim organizacijama mora ispunjavati uvjete iz drugih odredbi OUZP-a te poštovati njegovo poglavlje V. Stoga se ponajprije mora osigurati usklađenost s općim odredbama OUZP-a, a zatim i poštovanje odredbi poglavlja V. OUZP-a. Opisani su dionici koji su uključeni i njihove osnovne uloge u tom kontekstu, s posebnim naglaskom na ulozi uvoznika podataka, kojem će se dodijeliti certificiranje, te ulozi izvoznika podataka, koji će ga upotrebljavati kao alat za oblikovanje prijenosa podataka (s obzirom na to da odgovornost za obradu podataka ostaje na izvozniku podataka). U tom kontekstu certificiranje može uključivati i mjere kojima se dopunjuju alati za prijenos kako bi se osigurala usklađenost s razinom zaštite osobnih podataka u EU-u. Prvi dio smjernica sadržava i informacije o postupku dobivanja certifikata koji će se upotrebljavati kao alat za prijenose.

U drugom dijelu smjernica („PROVEDBA SMJERNICA O ZAHTJEVIMA ZA AKREDITACIJU") podsjeća se na to da se zahtjevi za akreditaciju certifikacijskih tijela nalaze u okviru norme ISO 17065 i proizlaze iz tumačenja Smjernica 4/2018 o akreditaciji certifikacijskih tijela u skladu s člankom 43. OUZP-a i njegovim Prilogom u kontekstu poglavlja V. Međutim, u kontekstu prijenosa, u ovim se smjernicama dodatno objašnjavaju neki od zahtjeva za akreditaciju koji se primjenjuju na certifikacijska tijela.

U trećem dijelu smjernica („POSEBNI KRITERIJI CERTIFICIRANJA") navode se smjernice o kriterijima certificiranja koji su već navedeni u Smjernicama 1/2018 te se utvrđuju dodatni posebni kriteriji koje bi trebalo uključiti u mehanizam certificiranja koji će se upotrebljavati kao alat za prijenose u treće zemlje. Ti kriteriji obuhvaćaju procjenu zakonodavstva trećih zemalja, opće obveze izvoznika i uvoznika, pravila o daljnjim prijenosima, pravnu zaštitu i provedbu, postupke i mjere u slučaju situacija u kojima se nacionalnim zakonodavstvom i praksama sprečava usklađenost s obvezama preuzetima u okviru certificiranja i zahtjeve tijela trećih zemalja za pristup podacima.

U četvrtom dijelu smjernica („OBVEZUJUĆE I PROVEDIVE OBVEZE KOJE TREBA UVESTI") navode se elementi koje bi trebalo obuhvatiti obvezujućim i provedivim obvezama koje bi voditelji ili izvršitelji obrade na koje se OUZP ne primjenjuje trebali preuzeti u svrhu pružanja odgovarajućih zaštitnih mjera za podatke koji se prenose trećim zemljama. Te obveze, koje se mogu utvrditi u različitim instrumentima, među ostalim i ugovorima, posebno uključuju jamstvo da uvoznik nema razloga vjerovati da ga zakoni i prakse u trećoj zemlji koji se primjenjuju na predmetnu obradu, uključujući sve zahtjeve za otkrivanje osobnih podataka ili mjere kojima se tijelima javne vlasti odobrava pristup, sprečavaju da ispuni svoje obveze u okviru certificiranja.

PRILOG ovim smjernicama sadržava primjere dopunskih mjera u skladu s mjerama navedenima u Preporukama 01/2020 iz Priloga II. (Preporuke 01/2020 o mjerama kojima se dopunjuju alati za prijenos podataka kako bi se osigurala usklađenost s razinom zaštite osobnih podataka u EU-u) u kontekstu upotrebe certificiranja kao alata za prijenose. Primjeri su izrađeni kako bi se skrenula pozornost na kritične situacije.

SADRŽAJ

Europski odbor za zaštitu podataka,

uzimajući u obzir članak 70. stavak 1. točku (e) Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (dalje u tekstu „OUZP"),

uzimajući u obzir Sporazum o EGP-u, a posebno njegov Prilog XI. i Protokol 37., kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.[1],

uzimajući u obzir članke 12. i 22. svojeg Poslovnika,

DONIO JE SLJEDEĆE SMJERNICE

1. OPĆE ODREDBE

1.1. Svrha i područje primjene

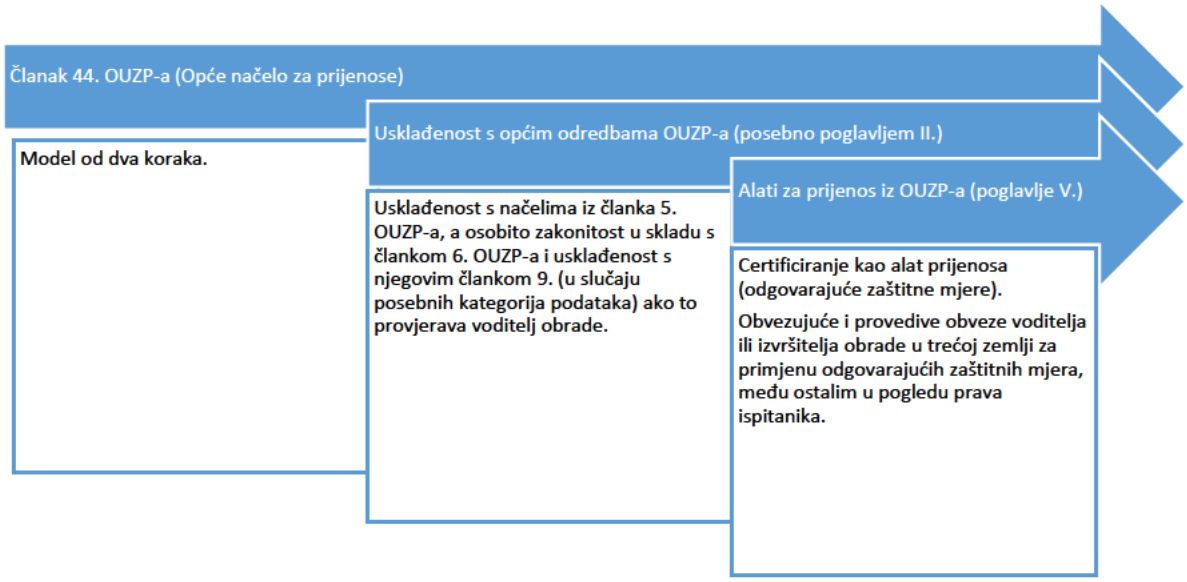
1. Ovim se dokumentom savjetuje o primjeni članka 46. stavka 2. točke (f) OUZP-a o prijenosima osobnih podataka trećim zemljama ili međunarodnim organizacijama na temelju certificiranja. Europski odbor za zaštitu podataka (EDPB) već je objavio opće smjernice o certificiranju[2] i akreditaciji[3] na temelju OUZP-a. Stoga se u ovim novim smjernicama odražavaju samo posebni aspekti certificiranja kao alata za prijenose. Njima se utvrđuje primjena članka 46. stavka 2. točke (f) i članka 42. stavka 2. OUZP-a pružanjem praktičnih smjernica u tom pogledu i uvođenjem novih elemenata u već objavljene smjernice.

2. EDPB će ocijeniti funkcioniranje tih smjernica na temelju iskustva stečenog njihovom praktičnom primjenom i dati dodatne smjernice za pojašnjenje primjene elemenata navedenih u nastavku, uključujući ulogu sporazuma o certificiranju u pogledu obvezujućih i provedivih obveza iz članka 46. stavka 2. točke (f) OUZP-a.

1.2. Opća pravila koja se primjenjuju na međunarodne prijenose

3. U skladu s člankom 44. OUZP-a svaki prijenos osobnih podataka trećim zemljama[4] ili međunarodnim organizacijama mora ispunjavati uvjete iz drugih odredbi OUZP-a te poštovati njegovo poglavlje V. Prema tome, svaki prijenos mora biti u skladu s načelima zaštite podataka iz članka 5. OUZP-a, zakonit u skladu s člankom 6. OUZP-a te biti u skladu s člankom 9. OUZP-a u slučaju posebnih kategorija podataka. Stoga se mora primijeniti test u dva koraka. Prvo se mora osigurati usklađenost s općim odredbama OUZP-a, a zatim i poštovanje odredbi poglavlja V. OUZP-a.

[1] Upućivanja na „države članice" u ovom dokumentu treba tumačiti kao upućivanja na „države članice EGP-a".
[2] Smjernice 1/2018 o certificiranju i utvrđivanju kriterija certificiranja u skladu s člancima 42. i 43. Uredbe (EU) 2016/679.
[3] Smjernice 4/2018 o akreditaciji certifikacijskih tijela u skladu s člankom 43. Opće uredbe o zaštiti podataka (2016/679).
[4] Smjernice 05/2021 o međudjelovanju primjene članka 3. i odredbi o međunarodnim prijenosima prema Poglavlju V. OUZP-a, str. 4.



4. Člankom 46. OUZP-a određeno je da „ako nije donesena odluka na temelju članka 45. stavka 3., voditelj obrade ili izvršitelj obrade trećoj zemlji ili međunarodnoj organizaciji osobne podatke mogu prenijeti samo ako je voditelj obrade ili izvršitelj obrade predvidio odgovarajuće zaštitne mjere i pod uvjetom da su ispitanicima na raspolaganju provediva prava i učinkovita sudska zaštita". U skladu s člankom 46. stavkom 2. točkom (f) OUZP-a takve odgovarajuće zaštitne mjere mogu se predvidjeti odobrenim mehanizmom certificiranja uz obvezujuće i provedive obveze voditelja ili izvršitelja obrade u trećoj zemlji za primjenu odgovarajućih zaštitnih mjera, među ostalim u pogledu prava ispitanika.

5. Kao rezultat toga, izvoznik podataka može se odlučiti osloniti na certifikat koji je dobio uvoznik podataka kao element za dokazivanje usklađenosti s vlastitim obvezama, npr. u skladu s člankom 24. stavkom 3. ili člankom 28. stavkom 5. OUZP-a. Uvoznik podataka može odlučiti podnijeti zahtjev za certificiranje kako bi dokazao da su na snazi odgovarajuće zaštitne mjere.

6. Izvoznik i uvoznik podataka mogu imati različite uloge (na primjer kao voditelj ili izvršitelj obrade)[5], ovisno o obradi u okviru poglavlja V., što dovodi do različitih odgovornosti:

7. Osim upotrebe certifikata ili drugih alata ili mehanizama za prijenos iz članaka 45. i 46., člankom 49. OUZP-a propisano je da se u ograničenom broju posebnih situacija međunarodni prijenosi podataka mogu obavljati ako se ne poštuje nijedan drugi mehanizam iz poglavlja V.[6] Međutim, kako je objašnjeno u prethodnim smjernicama EDPB-a, odstupanja predviđena člankom 49. OUZP-a moraju se usko tumačiti i uglavnom se odnose na aktivnosti obrade koje su povremene i ne ponavljaju se[7].

[5] Vidjeti u nastavku: PROVEDBA SMJERNICA O KRITERIJIMA CERTIFICIRANJA
[6] Za dodatne opće informacije o članku 49. i njegovu međudjelovanju s člankom 46. vidjeti Smjernice 2/2018 o odstupanjima iz članka 49. Uredbe (EU) 2016/679.
[7] Smjernice 2/2018 o odstupanjima iz članka 49. Uredbe (EU) 2016/679, str. 5.

1.3 Tko su uključeni dionici i koja je njihova uloga u certificiranju kao alatu za prijenose?

8. **Europski odbor za zaštitu podataka (EDPB)** ovlašten je za odobravanje kriterija certificiranja na razini EGP-a (Europskog pečata za zaštitu podataka) i za davanje mišljenja o nacrtima odluka nadzornih tijela o kriterijima certificiranja i zahtjevima za akreditaciju certifikacijskih tijela kako bi se osigurala dosljednost. Odbor je nadležan i za razvrstavanje svih mehanizama certificiranja te pečata i oznaka za zaštitu podataka u registar i njihovo objavljivanje[8].

9. **Nadzorna tijela** odobravaju kriterije certificiranja kada mehanizam certificiranja nije Europski pečat za zaštitu podataka[9]. Nadzorna tijela usto mogu akreditirati certifikacijsko tijelo, osmisliti kriterije certificiranja i izdavati certifikate ako je to utvrđeno nacionalnim pravom njihove države članice[10].

10. **Nacionalno akreditacijsko tijelo** može akreditirati certifikacijska tijela treće strane primjenom norme ISO 17065 i dodatnih zahtjeva za akreditaciju nadzornih tijela, koji bi trebali biti u skladu s odjeljkom 2. ovih smjernica. U nekim državama članicama akreditaciju može ponuditi i nadležno nadzorno tijelo, a može je provoditi i nacionalno akreditacijsko tijelo ili oba tijela.

11. **Nositelj programa** organizacija je koja je postavila kriterije certificiranja i zahtjeve metodologije prema kojima se ocjenjuje sukladnost. Organizacija koja provodi procjene mogla bi biti ista organizacija koja je razvila program i koja je njegov nositelj, ali mogu postojati slučajevi u kojima je jedna organizacija nositelj programa, a druga (ili više njih) provodi procjene kao certifikacijsko tijelo.

12. Ovisno o nacionalnom pravu, umjesto nadzornih tijela certifikate može izdavati **certifikacijsko tijelo** akreditirano u skladu s navedenim zahtjevima[11]. Certifikacijsko tijelo može osmisliti kriterije certificiranja i stoga postati nositelj programa (vidjeti točku 11.). Mora imati poslovni nastan u EGP-u, posebno kako bi se omogućilo učinkovito izvršavanje korektivnih ovlasti iz članka 58. stavka 2. točke (f) OUZP-a. Certifikacijsko tijelo može podugovoriti aktivnosti s lokalnim stručnjacima ili ustanovama izvan EGP-a koji će u njegovo ime obavljati revizijske aktivnosti[12]. Međutim, ne smije podugovoriti odluku o dodjeli ili neodobravanju certifikata.

13. **Uvoznik podataka** je subjekt (voditelj ili izvršitelj obrade) u trećoj zemlji koji prima podatke od izvoznika podataka.

14. **Izvoznik podataka** je subjekt (voditelj ili izvršitelj obrade) koji prenosi podatke od EGP-a do uvoznika podataka. Izvoznik podataka mora osigurati usklađenost s poglavljem V.

1.4. Koje je područje primjene certificiranja i predmet certificiranja kao alata za prijenos?

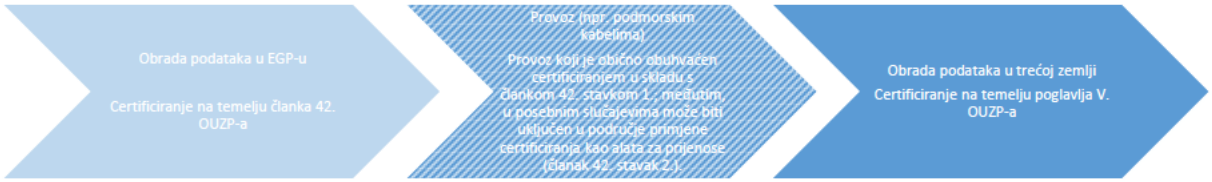
15. Cilj mehanizma certificiranja kao alata za prijenos u skladu s člankom 42. stavkom 2. mora biti osiguravanje odgovarajućih zaštitnih mjera za obradu osobnih podataka u skladu s uvjetima iz članka 46.

---

[8] Članak 42. stavak 8. OUZP-a.
[9] Smjernice 1/2018 o certificiranju i utvrđivanju kriterija certificiranja u skladu s člancima 42. i 43. Uredbe (EU) 2016/679, točka 2.2.
[10] Članak 42. stavak 5. i članak 43. stavak 1. OUZP-a.
[11] Članak 42. stavak 5. OUZP-a.
[12] Certifikacijska tijela moraju ocijeniti svoje lokalne stručnjake u skladu s normom ISO 17065 i dodatnim zahtjevima za akreditaciju koje je utvrdilo nadzorno tijelo (članak 43. stavak 1. točka (b) OUZP-a).

stavka 2. točke (f). Certificiranjem se dokazuje postojanje odgovarajućih zaštitnih mjera koje osiguravaju voditelji ili izvršitelji obrade izvan EGP-a ili voditelji ili izvršitelji obrade koji čine međunarodnu organizaciju koja prima podatke od voditelja ili izvršitelja obrade iz EGP-a kako bi se suzbili posebni rizici prijenosa osobnih podataka.

16. Općenito, prijenos osobnih podataka iz države članice u treću zemlju sam po sebi predstavlja obradu osobnih podataka u smislu članka 4. stavka 2. OUZP-a koja se provodi u državi članici[13] i stoga se može certificirati u skladu s člankom 42. stavkom 1. OUZP-a. Međutim, ovisno o kontekstu, u nekim bi se situacijama u područje primjene certificiranja kao alata za prijenose mogao uključiti provoz. Stoga bi predmet certificiranja, koji se podudara s ciljem evaluacije tijekom certificiranja[14], općenito trebao biti obrada podataka koje je uvoznik podataka u trećoj zemlji primio od EGP-a te provoz, ako je pod kontrolom uvoznika.



17. Predmet certificiranja može biti jedan postupak obrade ili skup postupaka. Ti postupci mogu obuhvaćati postupke upravljanja u smislu organizacijskih mjera, što znači da su sastavni dijelovi postupka obrade[15].

18. Stoga bi subjekt koji podnosi zahtjev bio uvoznik podataka u trećoj zemlji u pogledu njegova predmeta certificiranja.

1.5. Koja bi trebala biti uloga izvoznika u upotrebi certificiranja kao alata za prijenose?

19. Prijenos koji obavlja izvoznik podataka kao takav općenito je izravno obuhvaćen OUZP-om. To znači da izvoznik mora ispuniti svoje obveze na temelju OUZP-a, a posebno mora osigurati siguran prijenos podataka u skladu s člankom 32. i poglavljem V. kako bi se osiguralo da razina zaštite pojedinaca zajamčena tom uredbom nije ugrožena (članak 44. OUZP-a)[16]. To se, naravno, može certificirati u skladu s člankom 42. stavkom 1.

20. Nadalje, izvoznik podataka koji želi upotrijebiti certificiranje kao odgovarajuću zaštitnu mjeru u skladu s člankom 46. stavkom 2. točkom (f) OUZP-a posebno je obvezan provjeriti je li certifikat na koji se

---

[13] Presuda Suda Europske unije u predmetu C-311/18 – Data Protection Commissioner protiv Facebook Ireland Ltd i Maximilliana Schremsa, br. 83.
[14] Smjernice 1/2018 o certificiranju i utvrđivanju kriterija certificiranja u skladu s člancima 42. i 43. Uredbe (EU) 2016/679, str. 17.
[15] Smjernice 1/2018 o certificiranju i utvrđivanju kriterija certificiranja u skladu s člancima 42. i 43. Uredbe (EU) 2016/679, str. 16. (npr. mehanizam za rješavanje pritužbi).
[16] U tom je pogledu važno napomenuti da se člankom 44. OUZP-a jasno predviđa da prijenos može izvršiti ne samo voditelj obrade nego i izvršitelj obrade. Stoga će postojati situacija prijenosa u kojoj izvršitelj šalje podatke drugom izvršitelju ili čak voditelju obrade u trećoj zemlji prema uputama voditelja obrade (članak 28. stavak 3. točka (a) OUZP-a). U tim slučajevima izvršitelj obrade djeluje kao izvoznik podataka u ime voditelja obrade i mora osigurati usklađenost s odredbama poglavlja V. za predmetni prijenos u skladu s uputama voditelja obrade, što uključuje upotrebu odgovarajućeg alata za prijenos. S obzirom na to da je prijenos aktivnost obrade koja se provodi u ime voditelja obrade, voditelj obrade odgovoran je i može podlijegati odgovornosti u skladu s poglavljem V. te mora osigurati da će izvršitelj obrade pružiti dostatna jamstva u skladu s člankom 28.

namjerava osloniti učinkovit s obzirom na značajke namjeravane obrade. U tu svrhu izvoznik podataka mora pregledati izdani certifikat kako bi provjerio je li valjan, utvrdio da nije istekao, ustanovio obuhvaća li taj certifikat određeni prijenos koji se mora provesti i je li prijenos osobnih podataka u okviru certificiranja te provjerio je li riječ o daljnjim prijenosima i je li za njih priložena odgovarajuća dokumentacija. Osim toga, izvoznik mora provjeriti je li certifikacijsko tijelo koje izdaje certifikat akreditiralo nacionalno akreditacijsko tijelo ili nadležno nadzorno tijelo. Nadalje, izvoznik podataka trebao bi se pozvati na upotrebu certificiranja kao alata za prijenos u ugovoru o obradi podataka u skladu s člankom 28. OUZP-a u slučaju prijenosa od voditelja do izvršitelja obrade ili ugovora o razmjeni podataka s uvoznikom podataka u slučaju prijenosa od jednog voditelja obrade do drugog.

21. S obzirom na to da je izvoznik odgovoran za primjenu svih odredbi poglavlja V., mora procijeniti i je li certificiranje na koje se namjerava osloniti kao alat za prijenose učinkovito s obzirom na pravo i prakse u trećoj zemlji koji su na snazi i koji su relevantni za predmetni prijenos. Za potrebe te procjene i kao važan element kojim dokazuje usklađenost sa svojom odgovornošću, izvoznik podataka može se osloniti na provjeru uvoznikove dokumentirane procjene zakona i praksi treće zemlje koju provodi certifikacijsko tijelo.

22. Ako se procjenom uvoznika otkrije da će on i/ili izvoznik podataka možda morati osigurati dopunske mjere predviđene certificiranjem kako bi se osigurala u načelu istovjetna razina zaštite kako je predviđeno u EGP-u, izvoznik podataka mora provjeriti dopunske mjere koje je predvidio uvoznik podataka koji posjeduje certifikat i ustanoviti može li zadovoljiti tehničke i (ako postoje) dopunske mjere koje je zatražio uvoznik podataka.

23. Ako te odredbe nisu ispunjene, izvoznik podataka morat će od uvoznika zahtijevati da uvede prilagođene dopunske mjere ili da ih sam uspostavi.

1.6. Koji je postupak certificiranja kao alata za prijenose?

24. Certificiranje je dobrovoljno, no kada se traži, mora se odobriti transparentnim postupkom koji se temelji na obveznim pravilima. U okviru OUZP-a znatno se povjerenje polaže u privatne mehanizme certificiranja kao „reguliranu samoregulaciju”. Stoga se tim mehanizmima mora osigurati da certifikati materijalno ispunjavaju zahtjeve za odgovarajuće zaštitne mjere kako su definirani u članku 46. OUZP-a.

25. Stoga se certificiranje mora temeljiti na evaluaciji kriterija certificiranja u skladu s obvezujućom revizijskom metodologijom. Te će kriterije odobriti nacionalna nadzorna tijela ili Europski odbor za zaštitu podataka kako je opisano u članku 42. stavku 5. OUZP-a. Kriteriji certificiranja uključuju zahtjeve za procjenu obrade koju provodi uvoznik podataka, uključujući daljnje prijenose, i relevantnog pravnog okvira treće zemlje kako bi se izbjeglo da pravila i prakse treće zemlje sprečavaju uvoznika da ispuni svoje obveze u okviru certificiranja.

26. Tijekom postupka certificiranja cilj evaluacije na temelju kriterija certificiranja provjerava certifikacijsko tijelo koje je akreditiralo nacionalno akreditacijsko tijelo ili nadležno nadzorno tijelo[17].

[17] Smjernice 4/2018 o akreditaciji certifikacijskih tijela u skladu s člankom 43. Opće uredbe o zaštiti podataka (2016/679), str. 9.

27. U skladu s člankom 43. stavkom 1. OUZP-a certifikacijska tijela koja imaju odgovarajuću razinu stručnosti u području zaštite podataka izdaju i obnavljaju certifikate nakon što o tome obavijeste nadzorno tijelo kako bi mu se omogućilo da prema potrebi izvršava svoje ovlasti u skladu s člankom 58. stavkom 2. točkom (h) OUZP-a.

28. U skladu s člankom 43. stavkom 5. OUZP-a certifikacijska tijela nadležnim nadzornim tijelima dostavljaju razloge za izdavanje ili povlačenje zatraženog certifikata. To ne znači da je certifikacijskom tijelu za izdavanje certifikata potrebno odobrenje nadzornog tijela. Certifikacijsko tijelo pratit će usklađenost svojih klijenata s kriterijima certificiranja.

29. Nadzorno tijelo ima korektivnu ovlast da povuče certifikat ili da naredi certifikacijskom tijelu da povuče certifikat izdan u skladu s člancima 42. i 43. OUZP-a odnosno da ne izda certifikat ako zahtjevi za certificiranje više nisu ispunjeni.

30. Europski pečat za zaštitu podataka za međunarodne prijenose podataka može poslužiti kao alat za pokrivanje prijenosa u treće zemlje uz obvezujuće i provedive obveze[18].

31. Međutim, certifikati koji će se upotrebljavati kao alat za prijenose u državama EGP-a mogu se izdavati i u skladu s nacionalnim programima certificiranja. Kao takvi, vrijede samo za prijenose u treće zemlje od izvoznika u državi članici EGP-a u kojoj je program certificiranja odobren jer ne postoji uzajamno priznavanje različitih certifikata država EGP-a. Međutim, nadzorna tijela u različitim državama EGP-a mogu odobriti isti certifikacijski mehanizam za prijenose[19].

2. PROVEDBA SMJERNICA O KRITERIJIMA AKREDITACIJE

32. Zahtjevi za akreditaciju certifikacijskih tijela u pogledu certificiranja kao alata za prijenose nalaze se u okviru normi ISO 17065 i tumačenja Smjernica 4/201820 u kontekstu poglavlja V., kako je objašnjeno u nastavku.

33. Prema mišljenju EDPB-a, dodatnim zahtjevima za akreditaciju izrađenima na temelju Smjernica 4/2018 i norme ISO 17065 donesenima u skladu s člankom 64. stavkom 1. točkom (c) OUZP-a već su obuhvaćeni posebni zahtjevi potrebni za akreditaciju certifikacijskog tijela u pogledu certificiranja kao alata za prijenose. Međutim, u scenariju prijenosa neki zahtjevi iziskuju određena poboljšanja u smislu objašnjenja i tumačenja.

34. S obzirom na zahtjeve u pogledu resursa (vidjeti zahtjev 6. iz Priloga 1. Smjernicama 4/2018), certifikacijsko tijelo osigurava da ima resurse koji su mu potrebni da, u skladu s kriterijima certificiranja, provjeri je li uvoznik propisno i ispravno proveo potrebnu procjenu pravne situacije i prakse treće zemlje / trećih zemalja u kojima ima poslovni nastan ili u kojima posluje[21]. Ta bi se procjena trebala provesti u pogledu aktivnosti obrade koje treba certificirati kao dio cilja evaluacije u pogledu odgovarajućih

[18] Vidjeti članak 42. stavak 5. OUZP-a te stavak 35. Smjernica EDPB-a 1/2018 o certificiranju i utvrđivanju kriterija certificiranja u skladu s člancima 42. i 43. OUZP-a.
[19] Ako nadzorno tijelo predvodi donošenje kriterija certificiranja X u okviru svoje nacionalne inicijative i, nakon toga, vodi računa o kriterijima programa i primjenjivih posebnih nacionalnih propisa, druge zemlje koje žele donijeti iste kriterije certificiranja mogu ih donijeti bez pokretanja mišljenja EDPB-a u skladu s člankom 64. OUZP-a i osloniti se na mišljenje dano prvom nadzornom tijelu, u skladu s člankom 64. stavkom 3. OUZP-a (vidjeti dokument Upućivanje na Smjernice – Dopuna (Prilog Smjernicama 1/2018 o certificiranju i utvrđivanju kriterija certificiranja u skladu s člancima 42. i 43. OUZP-a), stavak 66.).
20 Smjernice 4/2018 o akreditaciji certifikacijskih tijela u skladu s člankom 43. OUZP-a i njegovim Prilogom.
[21] Vidjeti prethodno navedenu točku 12.

zaštitnih mjera iz članka 46. OUZP-a te, prema potrebi, uključivati dopunske mjere koje je utvrdio i proveo uvoznik. To uključuje i znatno poznavanje relevantnih lokalnih zakona i praksi te odgovarajuće jezične vještine u odnosu na treću zemlju / treće zemlje.

35. Kad je riječ o zahtjevima u pogledu postupka (vidjeti zahtjev 7. iz Priloga 1. Smjernicama 4/2018), certifikacijsko tijelo osigurava da se postupak certificiranja može poduprijeti mogućim revizijama na licu mjesta, da se provodi u pogledu obrade koja će se odviti u trećoj zemlji / trećim zemljama te da procjena obuhvaća i praktičnu provedbu postojećih zakona i politika u trećoj zemlji / trećim zemljama.

36. Kad je riječ o zahtjevima u pogledu promjena koje utječu na certificiranje (vidjeti zahtjev 7.10. iz Priloga 1. Smjernicama 4/2018), certifikacijsko tijelo prati promjene u zakonodavstvu treće zemlje i/ili njezinoj sudskoj praksi koje mogu utjecati na obradu obuhvaćenu područjem primjene cilja evaluacije.

3. POSEBNI KRITERIJI CERTIFICIRANJA

37. U kontekstu razmatranja posebnih kriterija certificiranja ove se smjernice temelje na Smjernicama 1/2018 o certificiranju i utvrđivanju kriterija certificiranja u skladu s člancima 42. i 43. OUZP-a (verzija 3.0), odgovarajućim Prilogom 2. o pregledu i procjeni kriterija certificiranja u skladu s člankom 42. stavkom 5. i Dopuni Smjernicama za ocjenjivanje kriterija certificiranja.

38. Prema mišljenju EDPB-a, kriteriji certificiranja izrađeni na temelju Priloga 2. Smjernicama 1/2018 i Dopuni Smjernicama za ocjenu kriterija certificiranja već obuhvaćaju većinu kriterija certificiranja koje je potrebno uzeti u obzir pri izradi programa certificiranja koji će se upotrebljavati kao alat za prijenose. Međutim, možda će biti potrebno dodatno precizirati neke od navedenih postojećih kriterija kako bi ih se prilagodilo posebnom scenariju prijenosa (vidjeti odjeljak 3.1.). Osim toga, možda će biti potrebno utvrditi dodatne kriterije za potrebe primjene odgovarajućih zaštitnih mjera, među ostalim u pogledu prava ispitanika (vidjeti odjeljak 3.2.).

3.1. PROVEDBA SMJERNICA O KRITERIJIMA CERTIFICIRANJA

39. U pogledu područja primjene mehanizma certificiranja i cilja evaluacije (vidjeti odjeljak 2. točku a. Priloga 2.) trebalo bi ga jasno opisati u relevantnoj dokumentaciji, među ostalim u pogledu prijenosa osobnih podataka trećoj zemlji ili u pogledu toga namjerava li se njome obuhvatiti i njihov provoz.

40. U pogledu područja primjene mehanizma certificiranja i cilja evaluacije (vidjeti odjeljak 2. točku b. Priloga 2.), u relevantnoj dokumentaciji trebalo bi konkretno opisati za koju se vrstu subjekta (npr. voditelja i/ili izvršitelja obrade) primjenjuje mehanizam certificiranja.

41. U pogledu područja primjene mehanizma certificiranja i cilja evaluacije (vidjeti odjeljak 2.f. Priloga 2.), kriterijima bi trebalo zahtijevati da se predmet evaluacije konkretno definira kako bi se izbjegli nesporazumi. To bi trebalo uključivati barem sljedeće:

42. proizvodne radnje, među ostalim u slučaju da su predviđeni daljnji prijenosi

    a) cilj

    b) vrstu subjekta (npr. voditelja i/ili izvršitelja obrade)

    c) vrstu prenesenih podataka, uzimajući pritom u obzir jesu li uključene posebne kategorije osobnih podataka kako su definirane u članku 9. OUZP-a

    d) kategorije ispitanika

e) države u kojima se obrađuju podaci.

43. Kad je riječ o transparentnosti i pravima ispitanika (vidjeti odjeljak 8. Priloga 2.), kriteriji certificiranja trebali bi:

a) zahtijevati da se ispitanicima pruže informacije o aktivnostima obrade, među ostalim, prema potrebi, o prijenosu osobnih podataka trećoj zemlji ili međunarodnoj organizaciji (vidjeti članke 12., 13. i 14. OUZP-a)

b) zahtijevati da se ispitanicima zajamče prava na pristup, ispravak, brisanje, ograničavanje, obavješćivanje o ispravku ili brisanju ili ograničavanju, prigovor na obradu, pravo da se na njih ne primjenjuju odluke koje se temelje isključivo na automatiziranoj obradi, uključujući izradu profila, u načelu prava istovjetna onima iz članaka od 15. do 19. te 21. i 22. OUZP-a

c) zahtijevati da uvoznik podataka koji posjeduje certifikat uspostavi odgovarajući postupak rješavanja pritužbi kako bi se osigurala učinkovita provedba prava ispitanika

d) zahtijevati procjenu jesu li i u kojoj mjeri ta prava provediva za ispitanike u predmetnoj trećoj zemlji, kao i sve dodatne odgovarajuće mjere koje bi mogle biti potrebne za njihovu provedbu, npr. zahtjev da uvoznik pristane surađivati s nadzornim tijelom nadležnim za izvoznike u svim postupcima čiji je cilj osigurati usklađenost s tim pravima, kao i biti podvrgnut njegovoj nadležnosti, a posebno da pristane odgovoriti na upite, podvrgnuti se revizijama i poštovati mjere koje je donijelo prethodno navedeno nadzorno tijelo, uključujući korektivne i kompenzacijske mjere.

44. Kad je riječ o tehničkim i organizacijskim mjerama kojima se jamči zaštita (odjeljak 10. točka q. Priloga 2.), kriterijima certificiranja trebalo bi od uvoznika zahtijevati da obavijesti izvoznika i, ako uvoznik djeluje kao voditelj obrade, da obavijesti nadzorno tijelo u EGP-u nadležno za izvoznike podataka o povredama osobnih podataka te da o njima obavijesti ispitanike ako je vjerojatno da će povreda rezultirati visokim rizikom za njihova prava i slobode, u skladu sa zahtjevima iz članka 34. OUZP-a.

3.2. DODATNI POSEBNI KRITERIJI CERTIFICIRANJA

45. S obzirom na zaštitne mjere utvrđene za druge instrumente prijenosa u skladu s člankom 46. OUZP-a (kao što su obvezujuća korporativna pravila ili kodeksi ponašanja), u svrhu osiguravanja dosljedne razine zaštite te uzimajući u obzir presudu Suda Europske unije u predmetu Schrems II, EDPB smatra da bi mehanizam certificiranja koji će se upotrebljavati kao alat za prijenose u treće zemlje trebao uključivati i kriterije navedene u nastavku.

1. Procjena zakonodavstva trećih zemalja

a) Zahtijeva li se kriterijima od uvoznika da procijeni pravila i prakse treće zemlje u kojoj posluje i utvrdi sprečavaju li ga da ispuni svoje obveze u okviru certificiranja?
b) Zahtijeva li se kriterijima od uvoznika da dokumentira procjenu pravila i praksi treće zemlje u kojoj posluje i da dokumentaciju stavi na raspolaganje certifikacijskom tijelu i, na zahtjev, nadzornom tijelu u EGP-u nadležnom za izvoznika podataka, kao i izvozniku podataka?
c) Zahtijeva li se kriterijima od uvoznika da utvrdi i provede organizacijske i tehničke mjere kako bi osigurao odgovarajuće zaštitne mjere u skladu s člankom 46. OUZP-a uzimajući u obzir „Preporuke 01/2020 o mjerama kojima se dopunjuju alati za prijenos podataka kako bi se osigurala usklađenost s razinom zaštite osobnih podataka u EU-u”?
d) Zahtijeva li se kriterijima od uvoznika da dokumentira organizacijske i tehničke mjere koje su učinkovito provedene u svrhu osiguravanja odgovarajućih zaštitnih mjera u skladu s

člankom 46. OUZP-a i da dokumentaciju stavi na raspolaganje certifikacijskom tijelu i na zahtjev nadležnim tijelima za zaštitu podataka i izvozniku podataka?

e) Zahtijeva li se kriterijima od uvoznika da utvrdi i provede organizacijske i tehničke mjere u svrhu osiguravanja prenesenih osobnih podataka, uzimajući u obzir „Preporuke 01/2020 o mjerama kojima se dopunjuju alati za prijenos podataka kako bi se osigurala usklađenost s razinom zaštite osobnih podataka u EU-u" ako je provoz obuhvaćen certificiranjem kao alatom za prijenose?

f) Zahtijeva li se kriterijima od uvoznika da certifikacijskom tijelu i izvozniku zajamči da nema razloga vjerovati da bi ga zakonodavstvo i prakse koji se na njega primjenjuju mogli spriječiti da ispuni svoje obveze u okviru certificiranja?

2. Opće obveze izvoznika i uvoznika

a) Zahtijeva li se kriterijima da se u ugovornim sporazumima (npr. u postojećem ugovoru o javnim uslugama) između izvoznika i uvoznika utvrdi opis konkretnog prijenosa na koji se certificiranje odnosi te da su predmetne osobe čiji se podaci obrađuju svjesni prava treće strane korisnika?

b) U slučaju da se kriterijima zahtijeva poseban sadržaj tih ugovornih sporazuma ili instrumenata te ako je naveden predložak, zahtijeva li se kriterijima da i oni budu predmet evaluacije?

3. Pravila o daljnjim prijenosima

a) Zahtijeva li se kriterijima da daljnji prijenosi podliježu posebnim zaštitnim mjerama u skladu sa zahtjevima iz poglavlja V. OUZP-a kako bi se osiguralo da razina zaštite zajamčena u EGP-u neće biti ugrožena i zahtijeva li se kriterijima da odgovarajuća dokumentacija na zahtjev bude dostupna certifikacijskom tijelu i nadzornom tijelu u EGP-u nadležnom za izvoznike podataka i izvozniku podataka?

4. Pravna zaštita i provedba

a) Je li kriterijima predviđeno da ispitanici pred sudom EGP-a u mjestu uobičajenog boravišta ispitanika mogu ostvariti svoja prava treće strane korisnika u odnosu na uvoznika podataka ili međunarodnu organizaciju, uključujući naknadu štete koju je ispitanik pretrpio u slučaju da uvoznik ne ispoštuje predmetni program certificiranja?

b) Omogućuje li se kriterijima odgovarajuća procjena odgovornosti uvoznika EGP-u za štetu koju je ispitanik pretrpio u slučaju neusklađenosti s predmetnim programom certificiranja?

c) Zahtijeva li se kriterijima da ispitanici protiv uvoznika mogu podnijeti pritužbu nadzornom tijelu u EGP-u, posebno u državi EGP-a u kojoj imaju uobičajeno boravište ili mjesto rada ili u državi nadležnoj za izvoznike podataka?

d) Zahtijeva li se kriterijima da uvoznik surađuje s nadzornim tijelom u EGP-u nadležnim za izvoznike podataka i prihvati da oni provedu reviziju i inspekciju nad njime te da uzme u obzir njihove savjete i poštuje njihove odluke?

5. Postupci i mjere u slučaju situacija u kojima se nacionalnim zakonodavstvom i praksama sprečava usklađenost s obvezama preuzetima u okviru certificiranja

a) Zahtijeva li se kriterijima obveza uvoznika podataka u trećoj zemlji ili međunarodnoj organizaciji da, ako ima razloga vjerovati da bi ga promjene u zakonodavstvu i praksi koje se na njega primjenjuju mogle spriječiti u ispunjavanju obveze u okviru certificiranja, o tome

odmah obavijesti certifikacijsko tijelo i izvoznika podataka kako bi izvoznik podataka mogao procijeniti treba li odmah prekinuti prijenose?

b) Zahtijeva li se kriterijima opis koraka koje treba poduzeti (uključujući obavješćivanje izvoznika u EGP-u i poduzimanje odgovarajućih dodatnih mjera) ako uvoznik podataka sazna za zakonodavstvo ili prakse treće zemlje kojima se sprečava ispunjavanje obveza u okviru certificiranja, kao i opis mjera koje treba poduzeti u slučaju zahtjeva za informacije od nadležnih tijela treće zemlje (uključujući obvezu preispitivanja i, prema potrebi, osporavanja zakonitosti zahtjeva i smanjenja otkrivenih informacija na najmanju moguću mjeru)?

6. Obrada zahtjeva tijela trećih zemalja za pristup podacima

a) Zahtijeva li se kriterijima da uvoznik podataka odmah obavijesti izvoznika podataka u slučaju da tijela treće zemlje podnesu zahtjev za pristup i da u tom slučaju poduzme odgovarajuće dodatne mjere?

b) Zahtijeva li se kriterijima da se prijenosi koji su rezultat nerazmjernih zahtjeva za pristup javnih tijela trećih zemalja, osobito zahtjeva kojima se traže masovni i neselektivni prijenosi osobnih podataka, ne bi smjeli odvijati?

7. Dodatne zaštitne mjere koje se odnose na izvoznika

46. Zahtijeva li se kriterijima da uvoznik podataka, ako je to predviđeno, osigura, a isto se obvezujućim zahtjevima traži i od izvoznika podataka, da su dopunske mjere koje je utvrdio usklađene s odgovarajućim dopunskim mjerama izvoznika podataka, uzimajući u obzir Preporuke EDPB-a 01/2020 i slučajeve upotrebe u svrhu osiguravanja učinkovite provedbe uvoznikovih dopunskih mjera?

4. OBVEZUJUĆE I PROVEDIVE OBVEZE KOJE TREBA UVESTI

47. Člankom 42. stavkom 2. OUZP-a zahtijeva se da voditelji obrade i izvršitelji obrade na koje se ta uredba ne primjenjuje i koji se pridržavaju mehanizma certificiranja namijenjenoga za prijenose preuzmu dodatne obvezujuće i provedive obveze, putem ugovornih ili drugih pravno obvezujućih instrumenata[22], da primjenjuju odgovarajuće zaštitne mjere predviđene mehanizmom certificiranja, među ostalim i u pogledu prava ispitanika.

48. Kao što je navedeno u OUZP-u, takve se obveze mogu preuzeti na temelju ugovora, što se čini najjednostavnijim rješenjem. Mogli bi se upotrebljavati i drugi instrumenti, pod uvjetom da voditelji obrade / izvršitelji obrade koji se pridržavaju mehanizma certificiranja mogu dokazati da su ta druga sredstva obvezujuća i provediva.

49. U svakom slučaju, obvezujuća priroda i provedivost moraju se osiguravati na temelju prava Unije, a obveze bi trebale biti obvezujuće i provedive i za ispitanike kao treće strane korisnike.

50. Jednostavna opcija bila bi uključivanje obvezujućih i provedivih obveza u ugovor između izvoznika podataka i uvoznika podataka. U praksi bi stranke mogle upotrijebiti postojeći ugovor (npr. sporazum o uslugama između izvoznika i uvoznika podataka, ugovor o obradi podataka u skladu s člankom 28. OUZP-a između voditelja obrade i izvršitelja obrade ili sporazum o razmjeni podataka između zasebnih

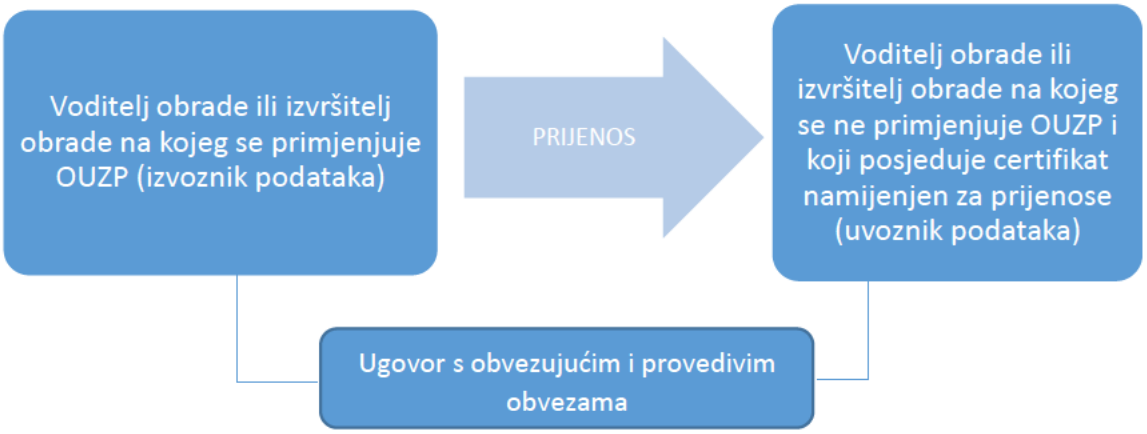
[22] Taj pravno obvezujući instrument nije još jedan alat iz poglavlja V. (kao što su, na primjer, standardne ugovorne klauzule) jer obvezujuće i provedive obveze iz članka 46. stavka 2. točke (f) moraju biti osmišljene kako bi se osiguralo da uvoznik poštuje kriterije certificiranja.

voditelja obrade) u koji bi mogle biti uključene obvezujuće i provedive obveze. Te bi se obveze trebale jasno razlikovati od svih drugih klauzula. Druga mogućnost mogla bi biti oslanjanje na zaseban ugovor, tako da se mehanizmu certificiranja namijenjenom za prijenos doda predložak ugovora koji bi zatim trebali potpisati voditelji obrade / izvršitelji obrade u trećoj zemlji i svi predmetni izvoznici podataka.

51. Trebala bi postojati fleksibilnost u odabiru najprikladnije opcije, ovisno o konkretnoj situaciji.

52. Kad se mehanizam certificiranja primjenjuje na prijenose i daljnje prijenose od izvršitelja obrade podizvršiteljima obrade, upućivanje na mehanizam certificiranja i instrument kojim se predviđaju obvezujuće i provedive obveze trebalo bi navesti i u sporazumu o izvršitelju obrade koji su potpisali izvršitelj obrade i njegov voditelj obrade.

Primjer obvezujućih i provedivih obveza uključenih u ugovor između izvoznika podataka i uvoznika podataka:



53. Općenito, ugovorom ili drugim pravno obvezujućim instrumentom mora se utvrditi da se voditelj obrade / izvršitelj obrade koji ima certifikat i koji djeluje kao uvoznik obvezuje pri obradi relevantnih podataka primljenih od EGP-a poštovati pravila navedena u certifikatu namijenjenom za prijenose te jamči da nema razloga vjerovati da ga zakoni i prakse u trećoj zemlji koji se primjenjuju na predmetnu obradu, uključujući sve zahtjeve za otkrivanje osobnih podataka ili mjere kojima se odobrava pristup javnih tijela, sprečavaju da ispuni svoje obveze u okviru certificiranja te da će obavijestiti izvoznika o svim predmetnim promjenama u zakonodavstvu ili praksi.

54. Ugovorom ili drugim instrumentom moraju se odrediti i mehanizmi koji omogućuju izvršavanje takvih obveza u slučaju da voditelj obrade / izvršitelj obrade ne poštuje pravila u okviru certificiranja, posebno u pogledu prava ispitanika čiji će se podaci prenijeti u okviru certificiranja.

55. Konkretnije, ugovor ili drugi instrument trebali bi obuhvaćati:

- postojanje prava ispitanika čiji se podaci prenose na temelju certificiranja da kao treće strane korisnici osiguraju izvršenje obveza koje je u okviru certificiranja preuzeo certificirani uvoznik podataka
- pitanje odgovornosti u slučaju da uvoznik podataka koji posjeduje certifikat izdan izvan EGP-a ne poštuje pravila u okviru certificiranja ako uvoznik podataka koji posjeduje certifikat izdan izvan EGP-a ne poštuje pravila u okviru certificiranja, ispitanici imaju mogućnost podnijeti tužbu protiv tog subjekta nadzornom tijelu u EGP-u i sudu u EGP-u nadležnom za uobičajeno boravište ispitanika, pozivajući se na pravo treće strane korisnika, uključujući pravo na naknadu uvoznik podataka koji posjeduje certifikat mora prihvatiti odluku ispitanika u tom pogledu; ispitanicima mora biti omogućeno i da, u slučaju da nepoštovanje pravila uvoznika dovede u pitanje

odgovornost izvoznika podataka, podnesu tužbu protiv izvoznika podataka nadležnom tijelu ili sudu nadležnom za poslovni nastan izvoznika podataka ili uobičajeno boravište ispitanika[23] uvoznik i izvoznik podataka trebali bi prihvatiti i da ispitanika može zastupati neprofitno tijelo, organizacija ili udruženje pod uvjetima utvrđenima u članku 80. stavku 1. OUZP-a

- postojanje prava izvoznika da postavlja pravila uvozniku podataka koji posjeduje certifikat u okviru certificiranja kao treća strana korisnik
- postojanje obveze uvoznika podataka koji posjeduje certifikat da izvoznika podataka i nadzorno tijelo izvoznika podataka obavijesti o svim mjerama koje je poduzelo certifikacijsko tijelo kao odgovor na utvrđeno nepoštovanje pravila istog uvoznika podataka.

[23] Ta odgovornost ne bi trebala dovoditi u pitanje mehanizme koje u okviru certificiranja primjenjuje certifikacijsko tijelo, koje može certificiranim voditeljima obrade / izvršiteljima obrade u okviru certificiranja narediti primjenu korektivnih mjera.

PRILOG

A. PRIMJERI DOPUNSKIH MJERA KOJE UVOZNIK MORA PROVESTI AKO JE PROVOZ UKLJUČEN U PODRUČJE PRIMJENE CERTIFIKATA

Prvi slučaj upotrebe: pohrana podataka u sigurnosne i druge svrhe za koje nije potreban jasan pristup podacima

Potrebno je utvrditi kriterije koji se odnose na standarde šifriranja i sigurnost ključa za dešifriranje, osobito kriterije koji se odnose na pravnu situaciju u trećoj zemlji. Ako uvoznik može biti prisiljen predati ključeve za dešifriranje, dodatna se mjera ne može smatrati djelotvornom[24].

Drugi slučaj upotrebe: prijenos pseudonimiziranih podataka

U slučaju pseudonimiziranih podataka utvrđuju se kriteriji u pogledu sigurnosti dodatnih informacija potrebnih za pripisivanje prenesenih podataka osobi čiji je identitet utvrđen ili se može utvrditi, a posebno:

– kriteriji u pogledu pravne situacije u trećoj zemlji; ako uvoznik može biti prisiljen pristupiti dodatnim podacima ili ih upotrijebiti kako bi pripisao podatke osobi čiji je identitet utvrđen ili se može utvrditi, mjera se ne može smatrati djelotvornom[25]

– kriteriji povezani s definicijom dodatnih informacija dostupnih tijelima trećih zemalja koje bi mogle biti dovoljne za pripisivanje podataka osobi čiji je identitet utvrđen ili se može utvrditi.

Treći slučaj upotrebe: šifriranje podataka kako bi ih se pri provozu između izvoznika i uvoznika zaštitilo od pristupa javnih tijela treće zemlje uvoznika

U slučaju šifriranih podataka uključuju se svi kriteriji za sigurnost provoza. Ako uvoznik može biti prisiljen predati kriptografske ključeve za dešifriranje ili autentifikaciju ili izmijeniti komponentu koja se upotrebljava za provoz na način kojim se ugrožavaju njegova sigurnosna svojstva, dodatna se mjera ne može smatrati djelotvornom[26].

Četvrti slučaj upotrebe: zaštićeni primatelj

U slučaju zaštićenih primatelja moraju se utvrditi kriteriji za granice povjerljivosti. Obrada podataka mora ostati u granicama povjerljivosti. To se odnosi i na obradu koju obavljaju (pod)izvršitelji obrade i na daljnje prijenose, za čije primatelje isto tako mora postojati granica povjerljivosti[27].

[24] Prilog 2., Preporuke 01/2020 o mjerama kojima se dopunjuju alati za prijenos podataka kako bi se osigurala usklađenost s razinom zaštite osobnih podataka u EU-u, verzija 2.0, prvi slučaj upotrebe: Pohrana podataka u sigurnosne i druge svrhe za koje nije potreban jasan pristup podacima, str. 85.; https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

[25] Vidjeti prethodne točke od 86. do 89.

[26] Vidjeti prethodnu točku 90.

[27] Vidjeti prethodnu točku 91.

B. PRIMJERI DOPUNSKIH MJERA KOJE MORA OSIGURATI IZVOZNIK U SLUČAJU DA PROVOZ NIJE OBUHVAĆEN CERTIFIKATOM

Drugi slučaj upotrebe: prijenos pseudonimiziranih podataka

Navode se kriteriji koji se odnose na dodatne informacije dostupne tijelima treće zemlje koje bi mogle biti dovoljne za pripisivanje podataka osobi čiji je identitet utvrđen ili se može utvrditi.

Treći slučaj upotrebe: šifriranje podataka kako bi ih se pri provozu između izvoznika i uvoznika zaštitilo od pristupa javnih tijela treće zemlje uvoznika

Navode se kriteriji koji se odnose na pouzdanost tijela koja izdaju certifikate javnih ključeva ili korištene infrastrukture, sigurnost kriptografskih ključeva koji se upotrebljavaju za autentifikaciju ili dešifriranje te pouzdanost upravljanja ključevima i upotrebu pravilno održavanog softvera bez poznatih ranjivosti.

Ako uvoznik može biti prisiljen otkriti kriptografske ključeve prikladne za dešifriranje ili autentifikaciju ili izmijeniti komponentu koja se upotrebljava za provoz na način kojim se ugrožavaju njegova sigurnosna svojstva, mjera se ne može smatrati djelotvornom[28].

Četvrti slučaj upotrebe: zaštićeni primatelj

U slučaju zaštićenih primatelja moraju se utvrditi kriteriji za granice povjerljivosti. Obrada podataka mora ostati u granicama povjerljivosti. To se odnosi i na obradu koju obavljaju (pod)izvršitelji obrade i na daljnje prijenose, za čije primatelje isto tako mora postojati granica povjerljivosti[29].

[28] Vidjeti prethodnu točku 90. Preporuka.
[29] Vidjeti prethodnu točku 91. Preporuka.