



Mišljenje 15/2026 o kriterijima certificiranja Europrivacy u vezi s njihovim odobrenjem, koje daje Odbor, kao Europskog pečata za zaštitu podataka koji će se koristiti kao alat za prijenose u skladu s člancima 42. i 46. Opće uredbe o zaštiti podataka

Doneseno 15. travnja 2026.

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

Sadržaj

1. Sažetak činjenica	5
2. Procjena.....	5
2.1. Područje primjene mehanizma certificiranja i predmet evaluacije.....	6
2.2. Postupci obrade	7
2.3. Načela obrade podataka	7
2.4. Opće obveze voditelja obrade i izvršitelja obrade.....	8
2.5. Prava ispitanika.....	8
2.6. Tehničke i organizacijske mjere i procjena rizika za prava i slobode ispitanika.....	9
2.7. Kriteriji kojima se dokazuje postojanje odgovarajućih zaštitnih mjera pri prijenosu osobnih podataka.....	9
3. Dodatni kriteriji za Europski pečat za zaštitu podataka koji će se koristiti kao alat za prijenos.....	10
4. Zaključci/preporuke	11
5. Završne napomene	11

Europski odbor za zaštitu podataka

uzimajući u obzir članak 63., članak 64. stavak 2., članak 42. i članak 46. 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 Europskom gospodarskom prostoru (dalje u tekstu „EGP”), 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 10. i 22. svojeg Poslovnika,

1. Države članice, nadzorna tijela, Europski odbor za zaštitu podataka (dalje u tekstu „EDPB” ili „Odbor”) i Europska komisija potiču, osobito na razini Unije, uspostavu mehanizama certificiranja zaštite podataka (dalje u tekstu „mehanizmi certificiranja”) te pečata i oznaka za zaštitu podataka u svrhu dokazivanja da su postupci obrade koje provode voditelji obrade i izvršitelji obrade u skladu s OUZP-om, uzimajući u obzir posebne potrebe mikropoduzeća te malih i srednjih poduzeća². Osim toga, uspostava mehanizama certificiranja može povećati transparentnost i omogućiti ispitanicima da procijene razinu zaštite podataka za relevantne proizvode i usluge³.
2. Osim što ih poštuju voditelji obrade ili izvršitelji obrade na koje se primjenjuje OUZP, mehanizmi certificiranja zaštite podataka, pečati ili oznake odobreni na temelju članka 42. stavka 5. OUZP-a mogu se uspostaviti kako bi se dokazalo postojanje odgovarajućih zaštitnih mjera koje osiguravaju voditelji obrade i izvršitelji obrade na koje se OUZP ne primjenjuje na temelju članka 3. u okviru prijenosa osobnih podataka trećim zemljama ili međunarodnim organizacijama (dalje u tekstu „uvoznici podataka”) pod uvjetima iz članka 46. stavka 2. točke (f) OUZP-a⁴.
3. Certificiranje koje će se koristiti kao alat za prijenose novi je mehanizam prijenosa uveden člankom 46. OUZP-a kako bi se osiguralo da, ako nije donesena odluka u skladu s člankom 45. stavkom 3. OUZP-a, voditelj obrade ili izvršitelj obrade u skladu s OUZP-om (dalje u tekstu „izvoznik podataka iz EGP-a”) može prenijeti osobne podatke trećoj zemlji ili međunarodnoj organizaciji samo ako su predviđene odgovarajuće zaštitne mjere i pod uvjetom da su ispitanicima na raspolaganju provediva prava i učinkoviti pravni lijekovi. Naime, u skladu s člankom 46. stavkom 2. točkom (f) OUZP-a mehanizam certificiranja odobren na temelju članka 42. OUZP-a može pružiti te odgovarajuće zaštitne mjere ako je popraćen obvezujućim i provedivim obvezama uvoznika podataka za primjenu odgovarajućih zaštitnih mjera, među ostalim u pogledu prava ispitanika. Kriteriji certificiranja sastavni su dio mehanizma certificiranja. Stoga je OUZP-om propisano da kriterije nacionalnog mehanizma certificiranja odobrava nadležno nadzorno tijelo (članak 42. stavak 5. i članak 43. stavak 2. točka (b) OUZP-a) ili, u slučaju Europskog pečata za zaštitu podataka, EDPB (članak 42. stavak 5. i članak 70. stavak 1. točka (o) OUZP-a).
4. Nadzorno tijelo koje namjerava predložiti da EDPB odobri Europski pečat za zaštitu podataka u skladu s člankom 42. stavkom 5. OUZP-a trebalo bi navesti namjeru vlasnika programa da ponudi mehanizam certificiranja u svim državama članicama. U tom je slučaju glavna uloga EDPB-a osigurati dosljednu primjenu OUZP-a uz pomoć mehanizma

¹ Upućivanja na „države članice” u ovom Mišljenju treba tumačiti kao upućivanja na „države članice EGP-a”.

² Članak 42. stavak 1. OUZP-a.

³ Uvodna izjava 100. OUZP-a.

⁴ Vidjeti članak 42. stavak 2. OUZP-a.

konzistentnosti iz članaka 63., 64. i 65. OUZP-a. U tom kontekstu u skladu s člankom 64. stavkom 2. OUZP-a EDPB odobrava kriterije certificiranja.

5. Europski pečat za zaštitu podataka odobren u skladu s člankom 42. stavkom 5. OUZP-a, uspostavljen kako bi se dokazalo postojanje odgovarajućih zaštitnih mjera koje osiguravaju uvoznici podataka, uz obvezujuće i provedive obveze, služi kao alat koji se primjenjuje na prijenose podataka iz svih država članica EGP-a trećim zemljama ili međunarodnim organizacijama⁵.
6. Pri evaluaciji mehanizma certificiranja koji će se koristiti kao alat za prijenose EDPB provodi procjenu na temelju „Smjernica 1/2018 o certificiranju i utvrđivanju kriterija certificiranja u skladu s člancima 42. i 43. Uredbe” (dalje u tekstu „Smjernice”) i njihove Dopune, koja sadržava „Smjernice za procjenu kriterija certificiranja” (dalje u tekstu „Dopuna”), te „Smjernica 07/2022 o certificiranju kao alatu za prijenose” (dalje u tekstu „Smjernice o certificiranju kao alatu za prijenose”).
7. EDPB potvrđuje da bi se svaki mehanizam certificiranja trebao razmatrati pojedinačno i da to ne dovodi u pitanje procjenu bilo kojeg drugog mehanizma certificiranja.
8. Mehanizmi certificiranja koji će se koristiti kao alat za prijenose trebali bi uvoznicima podataka omogućiti da dokažu postojanje odgovarajućih zaštitnih mjera kako bi se osiguralo da se pri obradi osobnih podataka prenesenih izvan EGP-a ne ugrozi razina zaštite pojedinaca zajamčena OUZP-om⁶. Njegovi kriteriji stoga bi trebali na odgovarajući način obuhvaćati zahtjeve i načela zaštite osobnih podataka utvrđene u OUZP-u kako bi se osiguralo da se zaštita predviđena OUZP-om primjenjuje na osobne podatke i nakon prijenosa⁷.
9. S druge strane, vlasnik programa trebao bi osigurati usklađivanje i sukladnost mehanizma certificiranja sa svim uključenim ili primijenjenim normama ISO i praksama certificiranja.
10. Kao rezultat toga, certifikati bi uvoznicima podataka trebali dodati vrijednost tako što bi pomogli u provedbi standardiziranih i određenih organizacijskih i tehničkih mjera kako bi se dokazalo da se pri obradi osobnih podataka koje primaju izvoznici podataka iz EGP-a provode odgovarajuće zaštitne mjere. U tom kontekstu EDPB podsjeća da bi predmet certificiranja, koji se podudara s predmetom evaluacije tijekom certificiranja, općenito trebao biti obrada podataka prenesenih uvozniku podataka u trećoj zemlji te provoz, ako je pod kontrolom tog uvoznika⁸.
11. Osim toga, certifikati će stvoriti dodanu vrijednost za izvoznika podataka koji se odluči osloniti na certifikat koji je dobio uvoznik podataka kao alat za prijenos osobnih podataka u skladu s člankom 46. stavkom 2. točkom (f) OUZP-a i kao element za dokazivanje usklađenosti s obvezama, npr. u skladu s člankom 24. stavkom 3. ili člankom 28. stavkom 5. OUZP-a⁹.
12. U tom smislu EDPB podsjeća da je izvoznik podataka koji želi koristiti certificiranje kao odgovarajuću zaštitnu mjeru u skladu s člankom 46. stavkom 2. točkom (f) OUZP-a obavezan provjeriti je li certifikat na koji se 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

⁵ Smjernice EDPB-a 07/2022 o certificiranju kao alatu za prijenose, verzija 2.0., donesene 14. veljače 2023., točka 30.

⁶ Članak 44. OUZP-a.

⁷ Vidjeti Komunikaciju Europske komisije Europskom parlamentu i Vijeću, „Razmjena i zaštita osobnih podataka u globaliziranom svijetu”, COM(2017) 7 final, str. 4.

⁸ Vidjeti Smjernice EDPB-a 07/2022 o certificiranju kao alatu za prijenose, verzija 2.0., donesene 14. veljače 2023., točka 16.

⁹ Smjernice 7/2022 o certificiranju kao alatu za prijenose, točka 5.

prijenos koji se mora provesti i je li provoz osobnih podataka u okviru certificiranja te kako bi provjerio je li riječ o daljnjim prijenosima i je li za njih priložena odgovarajuća dokumentacija¹⁰.

13. Osim toga, izvoznik podataka 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 ugovoru o razmjeni podataka s uvoznikom podataka u slučaju prijenosa od jednog voditelja obrade do drugog¹¹. Mora ispuniti i posebne obveze predviđene člankom 13. stavkom 1. točkom (f) OUZP-a, posebno obvezu obavješćivanja ispitanika o odgovarajućim zaštitnim mjerama koje se primjenjuju, tj., u slučaju certificiranja na temelju članka 46. stavka 2. točke (f) OUZP-a, o certifikatu koji je uvoznik dobio u skladu s posebnim mehanizmom certificiranja te o načinu pribavljanja primjerka certifikata i zaštitnih mjera sadržanih u kriterijima certificiranja ili mjestu na kojem su stavljeni na raspolaganje.
14. EDPB pozdravlja trud koji su vlasnici programa uložili u razradu mehanizama certificiranja – praktičnih i potencijalno troškovno učinkovitih instrumenata za postizanje veće usklađenosti s OUZP-om i promicanje prava na privatnost i zaštitu podataka ispitanika povećanjem transparentnosti.
15. EDPB podsjeća da su certifikati dobrovoljni instrumenti za dokazivanje odgovornosti i da primjena mehanizma certificiranja ne sprečava nadzorna tijela da izvršavaju svoje zadaće i ovlasti u skladu s OUZP-om i relevantnim nacionalnim zakonima. To se načelo, u kontekstu certifikata koji se koriste kao alat za prijenose, posebno primjenjuje i na ispunjavanje obveza koje su uvoznici podataka preuzeli kao obvezujuće i provedive u odnosu na izvoznike podataka, u okviru ugovornih ili drugih pravno obvezujućih instrumenata, radi primjene odgovarajućih zaštitnih mjera predviđenih mehanizmom certificiranja, među ostalim s obzirom na prava ispitanika.
16. Cilj je ovog Mišljenja osigurati dosljednu primjenu OUZP-a, među ostalim među nadzornim tijelima, voditeljima obrade i izvršiteljima obrade, uzimajući u obzir osnovne elemente koje je potrebno uspostaviti u okviru mehanizama certificiranja. Konkretno, cilj je ovog Mišljenja procijeniti kriterije certificiranja koje će uvoznici podataka koristiti kao alat za prijenose. EDPB stoga u njemu razmatra pitanja kao što su područje primjene, primjenjivost i relevantnost kriterija u slučaju prijenosa iz svih država članica EGP-a i/ili od bilo kojeg izvoznika podataka obuhvaćenog područjem primjene OUZP-a.
17. Mišljenje EDPB-a odnosi se isključivo na kriterije certificiranja. EDPB može zahtijevati informacije na visokoj razini o metodama evaluacije kako bi mogao temeljito procijeniti mogućnost revizije kriterija u kontekstu svojeg mišljenja. Međutim, to ne obuhvaća nikakvo odobravanje takvih metoda evaluacije.
18. Mišljenje EDPB-a donosi se na temelju članka 64. stavka 2. OUZP-a u vezi s člankom 10. stavkom 2. Poslovnika EDPB-a u roku od osam tjedana od prvog radnog dana nakon što predsjednik i nadležno nadzorno tijelo donesu odluku o potpunosti dokumenta. Odlukom predsjednika to se razdoblje može produljiti za dodatnih šest tjedana uzimajući u obzir složenost predmeta. Ako EDPB u svojem mišljenju zaključi da ne može odobriti predmetne kriterije, nadzorno tijelo može ih ponovno podnijeti na odobrenje nakon otklanjanja problema na koje je EDPB upozorio u prvotnom mišljenju,

¹⁰ Smjernice 7/2022 o certificiranju kao alatu za prijenose, točka 20.

¹¹ Vidjeti prethodnu bilješku.

donio je sljedeće mišljenje:

1. Sažetak činjenica

19. U skladu s člankom 42. stavkom 2. i člankom 46. stavkom 2. točkom (f) OUZP-a, Smjernicama 1/2018 i Smjernicama 7/2022 o certificiranju kao alatu za prijenose Europski centar za certificiranje i privatnost (dalje u tekstu „vlasnik programa”) sastavio je 82. verziju kriterija Europrivacy (dalje u tekstu „kriteriji certificiranja”).
20. EDPB podsjeća da je 10. listopada 2022. izdavanjem Mišljenja 28/2022 već odobrio kriterije certificiranja Europrivacy (60. verzija) kao Europski pečat za zaštitu podataka u skladu s člankom 42. stavkom 5. Opće uredbe o zaštiti podataka, koji je namijenjen za dokazivanje usklađenosti s OUZP-om u skladu s člankom 42. stavkom 1. OUZP-a. Taj program nije se smatrao certificiranjem namijenjenim za prijenos podataka u skladu s člankom 46. stavkom 2. točkom (f).
21. Luksemburško nadzorno tijelo dostavilo je 29. siječnja 2026. EDPB-u ažuriranu verziju već odobrenih kriterija certificiranja Europskog pečata za zaštitu podataka Europrivacy s proširenim područjem primjene, koje posebno uključuje podnositelje zahtjeva na koje se primjenjuje članak 3. stavak 2. OUZP-a, kao i druge izmjene koje se odnose na osnovne kriterije certificiranja (82. verzija). EDPB je o toj ažuriranoj verziji (82. verzija) kriterija certificiranja Europrivacy namijenjenih za dokazivanje sukladnosti s OUZP-om u skladu s člankom 42. stavkom 5. donio Mišljenje 14/2026.
22. Istog je datuma luksemburško nadzorno tijelo EDPB-u radi odobrenja u skladu s člankom 64. stavkom 2. OUZP-a dostavilo i dodatan skup kriterija certificiranja („Proširenje programa certificiranja Europrivacy za certificiranje uvoznika podataka u skladu s člankom 46.”) koji će se koristiti kao alat za prijenose u skladu s člankom 46. stavkom 2. točkom (f) OUZP-a.
23. Odluka o potpunosti tog dokumenta donesena je 31. ožujka 2026.

2. Procjena

24. EDPB je procijenio kriterije certificiranja koje će uvoznici podataka koristiti kao alat za prijenose radi njihova odobrenja na temelju članka 42. stavka 5. u vezi s člankom 46. stavkom 2. točkom (f) OUZP-a u skladu sa strukturom predviđenom u Prilogu 2. Smjernicama 1/2018 (dalje u tekstu „Prilog”), Dopuni Smjernicama i Smjernicama o certificiranju kao alatu za prijenose¹².
25. Odbor ističe da je, u skladu s uvjetima utvrđenima u članku 42. stavku 2. i članku 46. stavku 2. točki (f) OUZP-a, trenutačni program namijenjen za korištenje kao alat za prijenos te da se izvoznici podataka u smislu poglavlja V. OUZP-a (tj. voditelji obrade ili izvršitelji obrade na koje se OUZP primjenjuje za predmetnu obradu¹³) mogu osloniti na certifikate izdane u skladu s tim programom za prijenos osobnih podataka certificiranim uvoznicima podataka na koje se ne primjenjuje OUZP na temelju članka 3.¹⁴ To znači da se prijenos osobnih podataka uvozniku podataka u trećoj zemlji može izvršiti tek nakon što se taj uvoznik certificira i nakon što preuzme obvezujuće i provedive obveze prema izvozniku podataka iz EGP-a da će pri obradi prenesenih osobnih podataka u okviru predmeta evaluacije

¹² Vidjeti posebno: odjeljke 3. i 4. Smjernica 07/2022.

¹³ Vidjeti Smjernice 05/2021 o međudjelovanju primjene članka 3. i odredbi o međunarodnim prijenosima iz poglavlja V. Opće uredbe o zaštiti podataka, verzija 2.0., donesene 14. veljače 2023., točka 9.

¹⁴ Članak 42. stavak 2. OUZP-a.

primjenjivati odgovarajuće zaštitne mjere predviđene kriterijima certificiranja, uključujući zaštitne mjere koje se odnose na prava ispitanika.

26. U kontekstu ovog Mišljenja i radi odobrenja kriterija certificiranja Europrivacy koji će se koristiti kao alat za prijenos EDPB je ocijenio preliminarne provjere i kontrole podnošenja zahtjeva i predmeta evaluacije za uvoznike podataka (ADI), osnovne kriterije za usklađenost uvoznika podataka s OUZP-om u okviru programa Europrivacy (GI), provjere i kontrole tehničkih i organizacijskih mjera (T).
27. Kad je riječ o postupku certificiranja, s obzirom na posebnost certificiranja koje će se koristiti kao alat za prijenose EDPB ističe da je potrebna visoka razina transparentnosti i pozdravlja pojašnjenja u programu certificiranja Europrivacy prema kojima „prijenosi ne mogu započeti prije izdavanja certifikata”. U tom smislu EDPB potvrđuje da se prije prijenosa osobnih podataka „procjena može provesti na osobnim podacima koji nisu obuhvaćeni OUZP-om ili na neosobnim podacima” te da se „prema potrebi, za procjenu određenih kriterija mogu koristiti lažni podaci”, a nakon početka prijenosa podataka „revizor ponovno procjenjuje te kriterije u okviru sljedeće nadzorne revizije”¹⁵.
28. EDPB podsjeća da će možda biti potrebne određene prilagodbe akreditacije certifikacijskih tijela u vezi s certificiranjem kao alatom za prijenose u skladu sa Smjernicama o certificiranju kao alatu za prijenose¹⁶. Međutim, to pitanje nije u nadležnosti EDPB-a i stoga se ne razmatra u ovom Mišljenju.
29. EDPB podsjeća i da je u skladu s člankom 42. stavkom 8. OUZP-a kriterije certificiranja potrebno objaviti, ponajprije ako se certificiranje koristi kao alat za prijenose, u skladu s člankom 13. stavkom 1. točkom (f) OUZP-a, ispitanicima čiji će se osobni podaci prenijeti na temelju certifikata izdanog uvozniku podataka.
30. Odbor napominje, kako je pojašnjeno u definicijama programa, da se upućivanja na „nadležna tijela za zaštitu podataka” u cijelom programu trebaju tumačiti kao tijela za zaštitu podataka u EGP-u¹⁷.
31. Slično tome, Odbor napominje da se upućivanja na „primjenjivo pravo” i „pravo treće zemlje” odnose na pravo koje se primjenjuje na podnositelja zahtjeva i/ili na osobne podatke koji se obrađuju u okviru predmeta evaluacije u mjeri u kojoj to pravo ne propisuje ograničenja prava na zaštitu podataka koja prelaze ono što je nužno i razmjerno u demokratskom društvu kako bi se zaštitio jedan od ciljeva navedenih u članku 23. stavku 1. OUZP-a, razmjerno je cilju koji se želi postići, ne dovodi u pitanje bit prava na zaštitu podataka i predviđa posebne mjere za zaštitu temeljnih prava i interesa ispitanika.

2.1. Područje primjene mehanizma certificiranja i predmet evaluacije

32. Proširenje programa certificiranja Europrivacy za certificiranje uvoznika podataka u skladu s člankom 46. namijenjeno je, u skladu s člankom 42. stavkom 2. i člankom 46. stavkom 2.

¹⁵ Vidjeti Proširenje programa certificiranja Europrivacy™/® za certificiranje uvoznika podataka u skladu s člankom 46. OUZP-a, EP-CS.1.DI, točka 6.1.

¹⁶ Smjernice 07/2022, odjeljak 2.

¹⁷ Vidjeti definiciju „nadležnog nadzornog tijela” iz kriterija Europrivacy: „Pojam ‚nadležno tijelo za zaštitu podataka’ odnosi se na tijela za zaštitu podataka u EGP-u. Općenito se odnosi na nacionalna tijela za zaštitu podataka nadležna za osiguravanje usklađenosti obrade osobnih podataka koju provodi predmet evaluacije. U slučaju certifikata u skladu s OUZP-om izdanog uvozniku podataka na temelju članka 46. OUZP-a nadležnim tijelom za zaštitu podataka smatra se tijelo izvoznika podataka u EGP-u, osim u slučaju podnošenja pritužbe, pri čemu je nadležno bilo koje tijelo u EGP-u.”

točkom (f) OUZP-a, uvoznici podataka koji se nalaze izvan EGP-a i na koje se OUZP ne primjenjuje na temelju članka 3. kako bi dokazali postojanje odgovarajućih zaštitnih mjera u okviru prijenosa osobnih podataka trećim zemljama ili međunarodnim organizacijama. Njegovo područje primjene stoga se razlikuje od područja primjene certificiranja Europrivacy iz članka 42. stavka 1. OUZP-a, navedenog u točki 3. ovog Mišljenja, jer sadržava posebne kriterije koje je potrebno primjenjivati i poštovati kad se certifikat Europrivacy izdaje podnositeljima zahtjeva (voditeljima obrade ili izvršiteljima obrade) koji se nalaze izvan EGP-a i koji će djelovati kao uvoznici podataka.

33. Program certificiranja Europrivacy kao alat za prijenose može se primjenjivati na pojedinačne prijenose osobnih podataka, ali i na skup prijenosa ako su oni međusobno usko povezani. Program certificiranja sadržava kriterije certificiranja za postupke obrade koji se u okviru predmeta evaluacije provode nad osobnim podacima prenesenima uvozniku podataka, uključujući njihov provoz ako je pod kontrolom istog uvoznika¹⁸.
34. EDPB prima na znanje da područje primjene ovog programa certificiranja ne obuhvaća zajedničke voditelje obrade i da, ako je „zajedničko vođenje obrade uključeno u predmet evaluacije, certifikacijsko tijelo odbija izdati certifikat”¹⁹.

2.2. Postupci obrade

35. Kriteriji certificiranja obuhvaćaju relevantne sastavnice postupaka obrade osobnih podataka koji se prenose u okviru područja primjene predmeta evaluacije. Naime, kriterijima certificiranja predviđaju se zaštitne mjere za obradu posebnih kategorija osobnih podataka (odjeljak Gl.2. kriterija o posebnoj obradi podataka). U tom smislu Odbor pozdravlja činjenicu da u skladu s kriterijima certificiranja (kriterij Gl.2.1.3. o dodatnim zaštitnim mjerama za obradu posebnih kategorija osobnih podataka) podnositelj zahtjeva mora uvesti i dodatna ograničenja i zaštitne mjere prilagođene specifičnoj prirodi podataka i odgovarajućim rizicima ako su u obradu uključene posebne kategorije osobnih podataka.

2.3. Načela obrade podataka

36. U odjeljku Gl.1. kriteriji certificiranja obuhvaćaju odgovarajuća načela zaštite podataka, u skladu s onima iz članka 5. OUZP-a, kako bi se osiguralo da je obrada u predmetu evaluacije zakonita i proporcionalna.
37. Konkretno, u okviru kriterija certificiranja Gl.1.1.2. primjereno su razrađeni načelo ograničavanja svrhe i relevantne obveze koje podnositelj zahtjeva mora ispuniti da bi se uskladio s tim načelom. EDPB napominje da se preneseni osobni podaci mogu obrađivati samo u svrhe u koje su preneseni. U okviru kriterija certificiranja Gl.1.1.3., u skladu s aktualnim standardnim ugovornim klauzulama koje je donijela Europska komisija²⁰, utvrđuju se jedina izuzeća u skladu s kojima se podaci mogu dalje obrađivati za druge svrhe osim onih za koje su prvotno prikupljeni (tj. prethodni informirani pristanak, pravna obveza, životno važni interesi ispitanika i pravni zahtjevi).
38. EDPB napominje i da je podnositelj zahtjeva dužan dostaviti pisanu procjenu kako bi se osiguralo da ga pravo i praksa treće zemlje ne sprečavaju u ispunjavanju kriterija

¹⁸ Vidjeti kriterije certificiranja Gl.11.1.5. i Gl.11.1.6.

¹⁹ Proširenje programa certificiranja Europrivacy™/® za certificiranje uvoznika podataka u skladu s člankom 46. OUZP-a, EP-CS.1.DI, točka 3.2.2., u kojoj je jasno navedeno i da je „zajedničko vođenje obrade isključeno iz područja primjene programa za podnositelje zahtjeva u skladu s člankom 46.”.

²⁰ Provedbena odluka Komisije (EU) 2021/914 od 4. lipnja 2021. o standardnim ugovornim klauzulama za prijenos osobnih podataka u treće zemlje u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća.

Europrivacy, da ne dovode u pitanje bit temeljnih prava i sloboda ispitanika i ne prelaze ono što je nužno i razmjerno u demokratskom društvu kako bi se zaštitio jedan od ciljeva iz članka 23. stavka 1. OUZP-a. Certificirani subjekt mora preispitati procjenu kad god regulatorne ili organizacijske promjene mogu otežati ispunjavanje kriterija ili utjecati na predmet evaluacije ili prava ispitanika te o tome treba obavijestiti certifikacijsko tijelo (kriterij Gl.1.1.1.).

2.4. Opće obveze voditelja obrade i izvršitelja obrade

39. U okviru kriterija certificiranja u obzir se uzimaju obveze voditelja obrade na temelju članka 24. OUZP-a (odjeljak Gl.4. kriterija) te se mora provesti evaluacija ugovornih sporazuma između izvršitelja obrade i voditelja obrade u skladu s člankom 28. OUZP-a (odjeljak Gl.5. kriterija certificiranja o izvršiteljima ili podizvršiteljima obrade podataka) kako bi se osiguralo da izvršitelji obrade koji sudjeluju u obradi podataka u okviru predmeta evaluacije osiguraju razinu zaštite podataka jednaku onoj koja je potrebna u skladu s kriterijima programa Europrivacy. EDPB stoga pozdravlja uvođenje kriterija certificiranja koji se odnose na angažiranje podizvršitelja obrade za podnositelje zahtjeva koji djeluju kao voditelji obrade ili izvršitelji obrade jer ta razlika omogućuje da se bolje uzme u obzir podjela uloga i odgovornosti među akterima u lancu obrade (odjeljak Gl.5.1.).
40. U skladu s kriterijima certificiranja svi podnositelji zahtjeva dužni su imenovati službenika za zaštitu podataka, čak i ako podnositelj zahtjeva nije obavezan imenovati službenika za zaštitu podataka u skladu s člankom 37. OUZP-a. U skladu s kriterijima certificiranja provjerava se ispunjava li službenik za zaštitu podataka iste zahtjeve kao što su oni predviđeni u člancima od 37. do 39. (odjeljak Gl.9. kriterija certificiranja o imenovanju službenika za zaštitu podataka) kako bi se osiguralo da uloga, funkcija i kvalifikacije službenika za zaštitu podataka koji nadzire usklađenost obrade podataka u okviru predmeta evaluacije ispunjavaju „potrebne zahtjeve”. U tom smislu Odbor napominje da imenovanje službenika za zaštitu podataka nije obveza voditelja obrade i izvršitelja obrade u skladu s OUZP-om, osim ako su ispunjeni uvjeti iz članka 37. stavka 1. OUZP-a.
41. U skladu s kriterijima certificiranja provjerava se sadržaj evidencije aktivnosti obrade u skladu s člankom 30. OUZP-a (odjeljak Gl.5.3. kriterija o evidenciji aktivnosti obrade). U tom kontekstu Odbor pozdravlja činjenicu da je u skladu s kriterijima certificiranja podnositelj zahtjeva dužan postupati prema zahtjevima tijela za zaštitu podataka u EGP-u koja su nadležna za izvoznike te im na zahtjev staviti na raspolaganje evidenciju aktivnosti obrade (kriterij Gl.5.3.5.).

2.5. Prava ispitanika

42. Kriteriji certificiranja obuhvaćaju prava ispitanika u skladu s poglavljem III. OUZP-a te zahtijevaju uvođenje odgovarajućih mjera kako bi se osiguralo da se obradom u okviru predmeta evaluacije poštuju prava ispitanika i omogućuje njihovo učinkovito ostvarivanje. U odjeljku Gl.3. kriterija certificiranja koji se odnose na transparentne informacije, komunikaciju i modalitete za ostvarivanje prava ispitanika predviđa se, među ostalim zaštitnim mjerama, da ispitanici imaju pravo biti obaviješteni o obradi podataka i o načinu na koji mogu ostvarivati svoja prava. EDPB posebno pozdravlja činjenicu da se u kriterijima certificiranja predviđa da podnositelj zahtjeva uspostavi postupke ili mehanizam za postupanje po zahtjevima ispitanika i da u slučaju nepostupanja po zahtjevu ispitanike obavijesti o razlozima zbog kojih nije postupio, o pravu na podnošenje pritužbe tijelu za zaštitu podataka u EGP-u i o pravu na traženje pravnog lijeka.

2.6. Tehničke i organizacijske mjere i procjena rizika za prava i slobode ispitanika

43. Prema kriterijima certificiranja moraju se primjenjivati tehničke i organizacijske mjere koje dokazuju da je razina sigurnosti primjerena riziku obrade i kojima se uvodi tehnička i integrirana zaštita podataka u skladu s člancima 25. i 32. OUZP-a (odjeljak Gl.6. kriterija certificiranja o tehničkoj i integriranoj zaštiti podataka te o sigurnosti obrade) kako bi se uspostavila odgovarajuća razina sigurnosti te tehnička i integrirana zaštita podataka koji se obrađuju u okviru predmeta evaluacije. Osim toga, kriteriji certificiranja uključuju odjeljak (tj. kriterije T o tehničkim i organizacijskim mjerama, provjerama i kontrolama) u kojem se posebno razmatraju tehničke i organizacijske mjere.
44. U skladu s kriterijima certificiranja obvezna je primjena mjera koje osiguravaju da se obveze obavješćivanja o povredi osobnih podataka izvršavaju pravodobno i u odgovarajućem opsegu u skladu s člancima 33. i 34. OUZP-a (odjeljak Gl.7. kriterija certificiranja o upravljanju povredama podataka).
45. U tom kontekstu Odbor napominje da kriteriji certificiranja uključuju podroban popis (kriterij Gl.7.1.1. „Obveza dokumentiranja povreda podataka”) informacija koje podnositelj zahtjeva mora dokumentirati ako dođe do povrede podataka (npr. kategorije osobnih podataka na koje povreda utječe ili bi mogla utjecati, približan broj ispitanika na koje povreda utječe ili bi mogla utjecati, kategorije i približan broj dotičnih evidencija osobnih podataka, vjerojatne posljedice povrede osobnih podataka). Osim toga, EDPB pozdravlja činjenicu da se u kriterijima certificiranja jasno predviđa da, ako je vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca, podnositelj zahtjeva mora imati uspostavljena pravila, postupak ili mehanizam za obavješćivanje tijela za zaštitu podataka u EGP-u nadležnog za izvoznike i ispitanike u skladu sa zahtjevima iz članaka 33. i 34. OUZP-a (kriteriji Gl.7.1.2. „Obveza voditelja obrade da obavješćuje ispitanika o povredama podataka” i Gl.7.2. „Obavješćivanje ispitanika o povredi osobnih podataka”).
46. EDPB je zadovoljan i činjenicom da se prema kriterijima certificiranja mora procijeniti rizik za prava i slobode pojedinaca u vezi s obradom podataka obuhvaćenom predmetom evaluacije, pri čemu se predviđa sudjelovanje tijela za zaštitu podataka u EGP-u nadležnog za izvoznike u skladu s člankom 35. OUZP-a (odjeljak Gl.8. kriterija certificiranja „Obveza ocjenjivanja potrebe za procjenom učinka na zaštitu podataka”).

2.7. Kriteriji kojima se dokazuje postojanje odgovarajućih zaštitnih mjera pri prijenosu osobnih podataka

47. U skladu s kriterijima certificiranja obvezno je utvrđivanje svih prijenosa osobnih podataka trećim zemljama i međunarodnim organizacijama uključenih u predmet evaluacije te obrazloženje odabira mehanizma za prijenos podataka kojim se osiguravaju odgovarajuće zaštitne mjere u skladu s onima predviđenima u poglavlju V. OUZP-a (odjeljak Gl.10. kriterija o prijenosima osobnih podataka trećim zemljama ili međunarodnim organizacijama). EDPB potvrđuje da će se ti kriteriji certificiranja primjenjivati u slučaju „daljnjih prijenosa” osobnih podataka uključenih u predmet evaluacije istoj trećoj zemlji u kojoj se nalazi podnositelj zahtjeva ili drugoj trećoj zemlji. Odbor pozdravlja činjenicu da je prema tim kriterijima certificiranja podnositelj zahtjeva izričito dužan imati jasan pregled ili evidenciju svih protoka osobnih podataka obuhvaćenih predmetom evaluacije i utvrđenih prijenosa trećim zemljama i međunarodnim organizacijama te primjenjivati odgovarajuću osnovu za prijenos osobnih podataka u skladu s onima predviđenima u poglavlju V. OUZP-a, uzimajući u obzir obvezu da se ne ugrozi razina zaštite osobnih podataka kako je predviđena u EGP-u.

48. EDPB napominje i da prema kriterijima certificiranja podnositelj zahtjeva mora provesti procjenu učinka prijenosa i, prema potrebi, primijeniti dopunske mjere kako bi se osiguralo da se ne ugrozi razina zaštite prenesenih podataka (kriterij Gl.10.1.5.).

3. Dodatni kriteriji za Europski pečat za zaštitu podataka koji će se koristiti kao alat za prijenos

49. U skladu sa Smjernicama o certificiranju kao alatu za prijenose program certificiranja trebao bi osigurati da je uvoznik podataka „procijenio pravila i praksu treće zemlje u kojoj posluje te utvrdio sprečavaju li ga oni u ispunjavanju obveza preuzetih u okviru certificiranja”. U tom smislu Odbor napominje da se kriterijem ADI.2.1.5. utvrđuju uvjeti koje podnositelji zahtjeva moraju ispuniti pri definiranju predmeta evaluacije tijekom preispitivanja njihovih zahtjeva za certifikaciju. Naime, prije razmatranja revizije za potrebe certificiranja certifikacijsko tijelo dužno je provjeriti može li podnositelj zahtjeva dokazati da „zakoni i praksa treće zemlje ne sprečavaju podnositelja zahtjeva u ispunjavanju zahtjeva za certificiranje”. Ako ne može, postupak certificiranja zaustavit će se u fazi podnošenja zahtjeva.
50. Odbor napominje i da bi u skladu s kriterijem Gl.11.1.3. podnositelj zahtjeva trebao analizirati zakone i prakse u trećoj zemlji te utvrditi mogući učinak na prava i slobode ispitanika čiji se podaci mogu uvoziti, kao i uspostaviti „pravila, postupke ili politike koji omogućuju da se njegova pisana analiza lokalnih zakona i praksi na zahtjev stavi na raspolaganje certifikacijskom tijelu i nadležnim tijelima za zaštitu podataka.
51. Osim toga, u skladu sa Smjernicama o certificiranju kao alatu za prijenose u kriterijima certificiranja predviđa se da, prema potrebi, podnositelj zahtjeva donese dodatne mjere kako bi se osiguralo da se ne ugrozi razina zaštite prenesenih osobnih podataka i da, ako to nije moguće, uvoznik podataka o tome mora obavijestiti izvoznika podataka, a prijenos osobnih podataka trebalo bi suspendirati ili zaustaviti (kriterij Gl.11.1.3.).
52. Nadalje, Odbor napominje da se, u skladu s člankom 42. stavkom 2. OUZP-a, programom Europrivacy predviđa da uvoznik i izvoznik podataka prije bilo kakvog prijenosa potpišu ugovor koji uključuje relevantne obvezujuće i provedive obveze te da je osiguran predložak takvog ugovora. U tom kontekstu EDPB prima na znanje da, u skladu sa Smjernicama o certificiranju kao alatu za prijenose, kriteriji certificiranja uključuju detaljan popis sadržaja obvezujućih i provedbenih obveza koje podnositelj zahtjeva treba preuzeti u odnosu na svakog izvoznika u EGP-u, među kojima su obveza priznavanja prava ispitanika kao treće strane korisnika da u odnosu na uvoznika podataka koji posjeduje certifikat izvršavaju pravila u okviru certificiranja, obveza suradnje s tijelima za zaštitu podataka u EGP-u nadležnima za izvoznike podataka (među ostalim prihvaćanjem njihovih revizija i inspekcija, uvažavanjem njihovih savjeta i poštovanjem njihovih odluka), obveza poštovanja svih obvezujućih odluka donesenih u okviru nadležnosti sudova država članica EGP-a u vezi s certificiranjem, obveza obrade primljenih podataka isključivo dok je certifikat valjan te obveza vraćanja i/ili brisanja primljenih podataka ako se certifikat povuče. Kriterijima certificiranja predviđa se i da podnositelj zahtjeva zajamči da nema razloga vjerovati da ga zakoni i prakse u trećoj zemlji koji se primjenjuju na obradu u okviru predmeta evaluacije, uključujući sve zahtjeve za otkrivanje osobnih podataka ili mjere kojima se javnim tijelima odobrava pristup, sprečavaju u ispunjavanju njegovih obveza u okviru certificiranja te da obavješćuje izvoznika podataka o svim relevantnim promjenama u zakonodavstvu ili praksi u tom pogledu (kriterij Gl.11.1.1. „Obvezujuće i provedive obveze za uvoznike podataka”).

4. Zaključci/preporuke

53. Zaključno, EDPB smatra da su kriteriji certificiranja Europrivacy koji će se koristiti kao alat za prijenose sukladni s OUZP-om te ih odobrava u skladu sa zadaćom Odbora utvrđenom u članku 70. stavku 1. točki (o) OUZP-a, što dovodi do zajedničkog certificiranja (Europski pečat za zaštitu podataka) koje će se koristiti kao alat za prijenose.
54. EDPB smatra da su kriteriji certificiranja sastavni dio programa certificiranja te će program certificiranja Europrivacy upisati u javni registar mehanizama certificiranja te pečata i oznaka za zaštitu podataka, a kriterije će objaviti u skladu s člankom 42. stavkom 8. OUZP-a.

5. Završne napomene

55. Ovo Mišljenje upućuje se luksemburškom nadzornom tijelu i objavit će se u skladu s člankom 64. stavkom 5. točkom (b) Opće uredbe.

Za Europski odbor za zaštitu podataka

Predsjednica

Anu Talus