Dokumenti EDPB-a

Dokument Europskog odbora za zaštitu podataka o postupku za odobravanje kriterija certificiranja koji provodi Europski odbor za zaštitu podataka i iz kojeg proizlazi zajednička certifikacija: Europski pečat za zaštitu podataka

Doneseno 28. siječnja 2020.

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

Sadržaj

Europski odbor za zaštitu podataka,

uzimajući u obzir članak 42. stavak 5., članak 64. stavak 2. i članak 70. stavak 1. točku (o) 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 „Opća uredba o zaštiti podataka”),

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 3. i 22. svojeg Poslovnika od 25. svibnja 2018.,

DONIO JE SLJEDEĆI DOKUMENT:

1. ODOBRENJE Europskog odbora za zaštitu podataka za kriterije certificiranja na razini EU-a (Pečat EU-a za zaštitu podataka): PREISPITIVANJE, PODNOŠENJE, PRIHVATLJIVOST i DONOŠENJE

1.1. Podnošenje

Autori programa (koji mogu biti organizacije ili privatna poduzeća koji nisu zaduženi za izdavanje certifikata) ili certifikacijska tijela trebaju formalno podnijeti svoje kriterije certificiranja na razini EU-a (redoslijedom podnošenja zahtjeva):

1) nadležnom nadzornom tijelu na čijem se području nadležnosti nalazi sjedište autorâ programa[2];
2) nadležnom nadzornom tijelu na čijem se području nadležnosti nalazi sjedište certifikacijskog tijela koje upravlja mehanizmom certificiranja[3], uzimajući u obzir državu članicu u kojoj će se najvjerojatnije izdati najviše certifikata.

Nadalje, i nadzorna tijela mogu na vlastitu inicijativu izraditi nacrt kriterija certificiranja za mehanizam certificiranja na razini EU-a[4].

Nadzorna tijela mogu kriterije za mehanizam certificiranja na razini EU-a iz članka 42. stavka 5. podnijeti na odobrenje Europskom odboru za zaštitu podataka u skladu s člankom 63. i člankom 70. stavkom 1. točkom (o)[5]. Nadzorno tijelo provest će preispitivanje kako bi osiguralo da nacrt kriterija certificiranja ispunjava zahtjeve za kriterije certificiranja na razini EU-a koji se temelje na Općoj uredbi

[1] Upućivanja na „EU” u ovom dokumentu treba tumačiti kao upućivanja na „EGP”.
[2] Autor programa može biti i certifikacijsko tijelo.
[3] Akreditiranje certifikacijskog tijela (koje provodi nacionalno akreditacijsko tijelo ili nadležno nadzorno tijelo) uključuje i procjenu mehanizma certificiranja. Konkretno, to uključuje provjeru toga jesu li predložene metodologije procjene prikladne s obzirom na odobrene kriterije certificiranja. Akreditiranje će se odvijati tamo gdje se nalazi sjedište certifikacijskog tijela, u skladu s točkom 44. Smjernica 1/2018 Europskog odbora za zaštitu podataka.
[4] To nadzorno tijelo djelovat će kao autor programa.
[5] Nadzorno tijelo ne može podnijeti kriterije certificiranja radi dobivanja mišljenja ako već nije podnijelo svoje zahtjeve za akreditaciju radi dobivanja odobrenja.

o zaštiti podataka, uzimajući u obzir smjernice o certificiranju Europskog odbora za zaštitu podataka[6]. Preispitivanje nadležnog nadzornog tijela poduprijet će se potpunim ispunjavanjem predloška za procjenu kriterija certificiranja koji je donio Europski odbor za zaštitu podataka (mora se ispuniti i odjeljak za nacionalnu razinu i odjeljak za razinu EU-a). Taj se dokument može podnijeti Europskom odboru za zaštitu podataka samo ako nadležno nadzorno tijelo smatra da bi Odbor mogao odobriti kriterije (vidjeti korak 3.a)[7].

1.2. Početna prihvatljivost kriterija certificiranja

Ako nadležno nadzorno tijelo utvrdi da nacrt kriterija nije prihvatljiv, ono će autora programa o tome obavijestiti pisanim putem uz navođenje temelja za svoju odluku (vidjeti korak 3.b).

Ako nadležno nadzorno tijelo utvrdi da je nacrt kriterija prihvatljiv, ono će autoru programa pisanim putem potvrditi da će prijeći u sljedeću fazu postupka i ocijeniti nacrt kriterija. Time će se pokrenuti sljedeći postupak neformalne suradnje u pogledu ocjenjivanja kriterija za odobrenje.

1.3. Suradnja (faza neformalne suradnje na razini nadzornih tijela)

Faza neformalne suradnje ključan je element u omogućivanju učinkovitog postupka odobravanja koji provodi Odbor. Faza neformalne suradnje omogućit će prethodno utvrđenom nadležnom nadzornom tijelu da vodi procjenu kriterija i, prema potrebi, pruža povratne informacije autoru programa. Nadležno nadzorno tijelo pravodobno će izvješćivati autora programa o novostima o svim fazama.

Nadležno nadzorno tijelo obavijestit će sva nadzorna tijela, a ona će podnijeti zahtjev kojim se na dobrovoljnoj osnovi traže najviše dva korevizora koji će pomoći sa sadržajnom procjenom kriterija (vidjeti korak 4.). Zahtjev kojim se traže korevizori upućuje se elektroničkom poštom tajništvu Europskog odbora za zaštitu podataka. Komunikacija putem elektroničke pošte mora uključivati predložak za procjenu koji je donio Europski odbor za zaštitu podataka i koji ispunjava nadležno nadzorno tijelo.

Faza neformalne suradnje (vidjeti korake od 4. do 6.) može započeti tek nakon što sljedeći dokumenti budu dostupni na engleskom jeziku i mogu se razmijeniti s drugim nadzornim tijelima:

- predložak za procjenu koji je donio Europski odbor za zaštitu podataka i koji je nadležno nadzorno tijelo u potpunosti ispunilo; on mora sadržavati informacije o tome kako su sva mjerodavna nacionalna zakonodavstva uzeta u obzir i o planiranom početku primjene u državama članicama i
- primjerak kriterija za certificiranje i svih relevantnih priloga.

Kriteriji certificiranja koji se odnose na zakonodavstvo određene države članice mogu se podnijeti na nacionalnom jeziku te države, ako su dostupni.

Uloga korevizora bit će pomaganje nadležnom nadzornom tijelu u ocjenjivanju nacrta kriterija. Korevizori bi trebali osigurati uključivanje stručnjaka u skladu s predmetom certificiranja. Nakon što korevizori budu potvrđeni, oni bi trebali podnijeti svoje primjedbe o kriterijima u roku od trideset dana od trenutka kada dobiju dokumente. Nadležno nadzorno tijelo zatim će pri provedbi svoje ocjene razmotriti te primjedbe. Preispitivanje će uglavnom biti usmjereno na tehničku prihvatljivost kriterija certificiranja (vidjeti korak 5.).

[6] Smjernice 1/2018 o certificiranju i utvrđivanju kriterija certificiranja u skladu s člancima 42. i 43. Uredbe

[7] Vidjeti odjeljak 4.2. (točke 35. – 45.) Smjernica o kriterijima certificiranja Europskog odbora za zaštitu podataka.

Nakon završetka preispitivanja koje provode korevizori nadležno nadzorno tijelo proslijedit će nacrt kriterija svim nadzornim tijelima. Tajništvo Europskog odbora za zaštitu podataka može pomagati u komunikaciji među nadzornim tijelima (vidjeti korak 6.). Sva predmetna nadzorna tijela imat će 30 dana za odgovor, a sva značajna pitanja podnosit će se na raspravu relevantnoj podskupini Europskog odbora za zaštitu podataka. Preispitivanje će se sastojati od osiguravanja da je nacionalno zakonodavstvo obuhvaćeno na odgovarajući način te će uključivati i analizu usklađenosti kriterija koji obuhvaćaju nacionalno zakonodavstvo. Ako nadzorna tijela ne odgovore, kriteriji će prijeći u sljedeću fazu postupka.

Nadležno nadzorno tijelo može, prema potrebi, odlučiti ponoviti korake 5. i 6.

Nakon svakog koraka u fazi neformalne suradnje, nadležno nadzorno tijelo može autoru programa dati mogućnost da ažurira kriterije certificiranja uzimajući u obzir primjedbe nadzornih tijela.

Nakon koraka 6. i pod pretpostavkom pozitivnog ishoda, nadležno nadzorno tijelo zatražit će sastanak podskupine radi rasprave o kriterijima koji se preispituju (vidjeti korak 7.) Nadležno nadzorno tijelo ažurirat će predložak za procjenu koji je donio Europski odbor za zaštitu podataka unošenjem ključnih točaka s tog sastanka. Nadležno nadzorno tijelo može početi provoditi sve mjere koje su iznesene na sastanku, a autor programa može revidirati kriterije.

Na kraju faze neformalne suradnje nadležno nadzorno tijelo može (u savjetovanju s autorom programa) odlučiti o tome hoće li kriterije certificiranja podnijeti na formalno odobrenje Europskom odboru za zaštitu podataka. Nadležno nadzorno tijelo donijet će konačnu odluku o tome bi li nacrt kriterija trebalo podnijeti Odboru radi odobrenja, u skladu s člankom 63. Opće uredbe o zaštiti podataka. Ako nadležno nadzorno tijelo odluči da kriterije certificiranja neće podnijeti Europskom odboru za zaštitu podataka, time taj postupak završava (vidjeti korak 8.b). Kasnijim ponovnim podnošenjem kriterija certificiranja doći će do pokretanja novog postupka preispitivanja.

Autor programa trebao bi sudjelovati u postupku preispitivanja u neformalnoj fazi. Nadležno nadzorno tijelo trebalo bi autora programa obavijestiti o primjedbama iznesenima tijekom faze suradnje, a autoru programa trebala bi se dati mogućnost da traži pojašnjenja i da odgovori na primjedbe[8].

1.4. Formalno podnošenje i odobrenje (faza u Europskom odboru za zaštitu podataka)

Odobravanje Pečata EU-a za zaštitu podataka odvija se u okviru postupka mišljenja iz članka 64. stavka 2.

Od nadležnog nadzornog tijela traži se da vodi računa o rasporedu rada stručne podskupine za usklađenost, e-upravu i zdravlje (CEH) prije podnošenja kriterija putem Informacijskog sustava unutarnjeg tržišta (IMI).

Formalno podnošenje mora se provesti putem platforme IMI-ja (korak 8.a). Za formalno podnošenje moraju se ispuniti sljedeći kriteriji prihvatljivosti kako bi Europski odbor za zaštitu podataka prihvatio podnesak:

- svi relevantni dokumenti moraju se podnijeti na engleskom,

[8] Nadležno nadzorno tijelo mora osigurati da autor programa bude obaviješten o toj mogućnosti i da mu se pruži prilika da je iskoristi.

- nadležno nadzorno tijelo mora ispuniti i podnijeti predložak za procjenu koji je donio Europski odbor za zaštitu podataka (predložak se mora ažurirati u skladu s rezultatima početne faze preispitivanja) i
- moraju se podnijeti primjerak kriterija certificiranja i svi prilozi.

Tajništvo će provjeriti jesu li podneseni svi dokumenti i jesu li oni potpuni. Tajništvo može od nadležnog nadzornog tijela zatražiti da u određenom roku dostavi dodatne informacije koje su potrebne za potpunost dokumentacije. Kao opće pravilo i ne dovodeći u pitanje ostale prijevode ako su oni potrebni ili se zahtijevaju zakonom, podnositelj zahtjeva trebao bi dostaviti sve relevantne dokumente na jeziku nadležnog nadzornog tijela i na engleskom. Ako je to potrebno, primjerice, u slučaju dokumenata koji ne potječu od nadzornog tijela ili ih ono nije sastavilo, tajništvo će dokumente koje je podnijelo nadležno nadzorno tijelo dati prevesti na engleski bez nepotrebne odgode. U tim slučajevima, kad nadležno tijelo pristane na prijevod, a predsjednik Odbora i nadležno nadzorno tijelo odluče da je spis potpun, tajništvo će, u ime predsjednika, proslijediti spis članovima Odbora.

Mišljenje Odbora donosi se u roku od osam tjedana nakon što predsjednik i nadležno nadzorno tijelo (prema potrebi) utvrde da je spis potpun. Taj se rok može produljiti za dodatnih šest tjedana, uzimajući u obzir složenost predmeta, na temelju odluke predsjednika koju donosi na vlastitu inicijativu ili na temelju zahtjeva najmanje jedne trećine članova Odbora.

Nacrte mišljenja, prije podnošenja na glasovanje Odboru, priprema i sastavlja tajništvo i, na temelju odluke predsjednika, zajedno s izvjestiteljem i članovima stručnih podskupina. Radi izrade mišljenja, a ovisno o području primjene mehanizma certificiranja, može se zatražiti stručno znanje drugih podskupina Europskog odbora za zaštitu podataka.

Na temelju odluke predsjednika, putem elektroničke pošte ili na sastanku CEH-a može se osnovati tim za izradu nacrta mišljenja, ovisno o vremenu podnošenja. Poziv na dobrovoljno uključivanje u rad skupine za izradu nacrta upućuje tajništvo zajedno s koordinatorima stručne skupine za CEH. Kako bi se izbjegli sukobi interesa, nadležno nadzorno tijelo ne bi smjelo sudjelovati u radu užeg tima za izradu nacrta mišljenja. Međutim, ako ima ikakvih pitanja, uži tim za izradu nacrta mišljenja uvijek ih može uputiti nadležnom nadzornom tijelu.

Tajništvo i tim za izradu nacrta mišljenja (prema potrebi) preispituju podnesene kriterije za certificiranje i popratne dokumente (uključujući predložak za procjenu) i sastavljaju nacrt mišljenja. Pritom se uvijek u obzir uzima sadržaj prethodnih mišljenja o istoj temi kako bi se osigurala dosljednost. Pri izradi nacrta mišljenja kao interni radni dokument može se koristiti predložak za procjenu koji je donio Europski odbor za zaštitu podataka i koji je podnijelo nadležno nadzorno tijelo. To preispitivanje mora se provesti unutar roka za izradu mišljenja.

1.5. Mišljenje na temelju članka 64. stavka 2.

Na temelju članka 64. stavka 2. i članka 70. stavka 1. točke (o), Europski odbor za zaštitu podataka daje mišljenje i odobrenje koje se odnosi na pitanja navedena u članku 42. stavku 5. Opće uredbe o zaštiti podataka (vidjeti korak 9.)[9].

[9] Člankom 64. stavkom 2. Opće uredbe o zaštiti podataka omogućuje se nadzornim tijelima da zatraže mišljenje o predmetu opće primjene ili s učincima u više od jedne države članice. Budući da Pečat EU-a za zaštitu podataka ima učinke u cijelom EU-u, mišljenje odbora obuhvaćeno je područjem primjene članka 64. stavka 2., a ne članka 64. stavka 1.

Na donošenje mišljenja primjenjuju se pravila iz članka 10. Poslovnika Europskog odbora za zaštitu podataka[10]. Nadzorno tijelo koje odluči zatražiti mišljenje na temelju članka 64. stavka 2. morat će za taj zahtjev navesti pisano obrazloženje, u skladu s člankom 10. stavkom 3. Poslovnika. U kontekstu zahtjeva kojim se od Europskog odbora za zaštitu podataka traži da odobri Europski pečat za zaštitu podataka za kriterije certificiranja, nadležno nadzorno tijelo mora tražiti mišljenje na temelju članka 64. stavka 2. o predmetu s učincima u više od jedne države članice.

Postupak dobivanja odobrenja Europskog odbora za zaštitu podataka završava odobrenjem ili odbijanjem zahtjeva za pečat EU-a za zaštitu podataka za podnesene kriterije. Na temelju članka 64. stavka 2. ne postoji potreba za daljnjim praćenjem mišljenja Odbora.

Mišljenje Europskog odbora za zaštitu podataka na temelju članka 64. stavka 2. primjenjivo je u svim državama članicama[11].

1.6. Daljnji koraci nakon mišljenja Europskog odbora za zaštitu podataka

Nakon što Europski odbor za zaštitu podataka donese mišljenje o kriterijima za pečat EU-a za zaštitu podataka moraju se dovršiti sljedeći koraci:

- tajništvo objavljuje mišljenje koje sadržava odobrenje ili odbijanje pečata EU-a za zaštitu podataka,

Ako Europski odbor za zaštitu podataka pozitivnim mišljenjem odobri zahtjev za pečat EU-a za zaštitu podataka:

- nadležno nadzorno tijelo obavijestit će autora programa o ishodu postupka dobivanja odobrenja Europskog odbora za zaštitu podataka u pogledu zahtjeva za odobrenje pečata EU-a za zaštitu podataka,
- vodeće/koordinirajuće nadležno nadzorno tijelo dužno je osigurati da su tajništvu dostavljeni dokumenti potrebni za objavljivanje u javnom registru Europskog odbora za zaštitu podataka.

Ako Europski odbor za zaštitu podataka negativnim mišljenjem odbije zahtjev za pečat EU-a za zaštitu podataka:

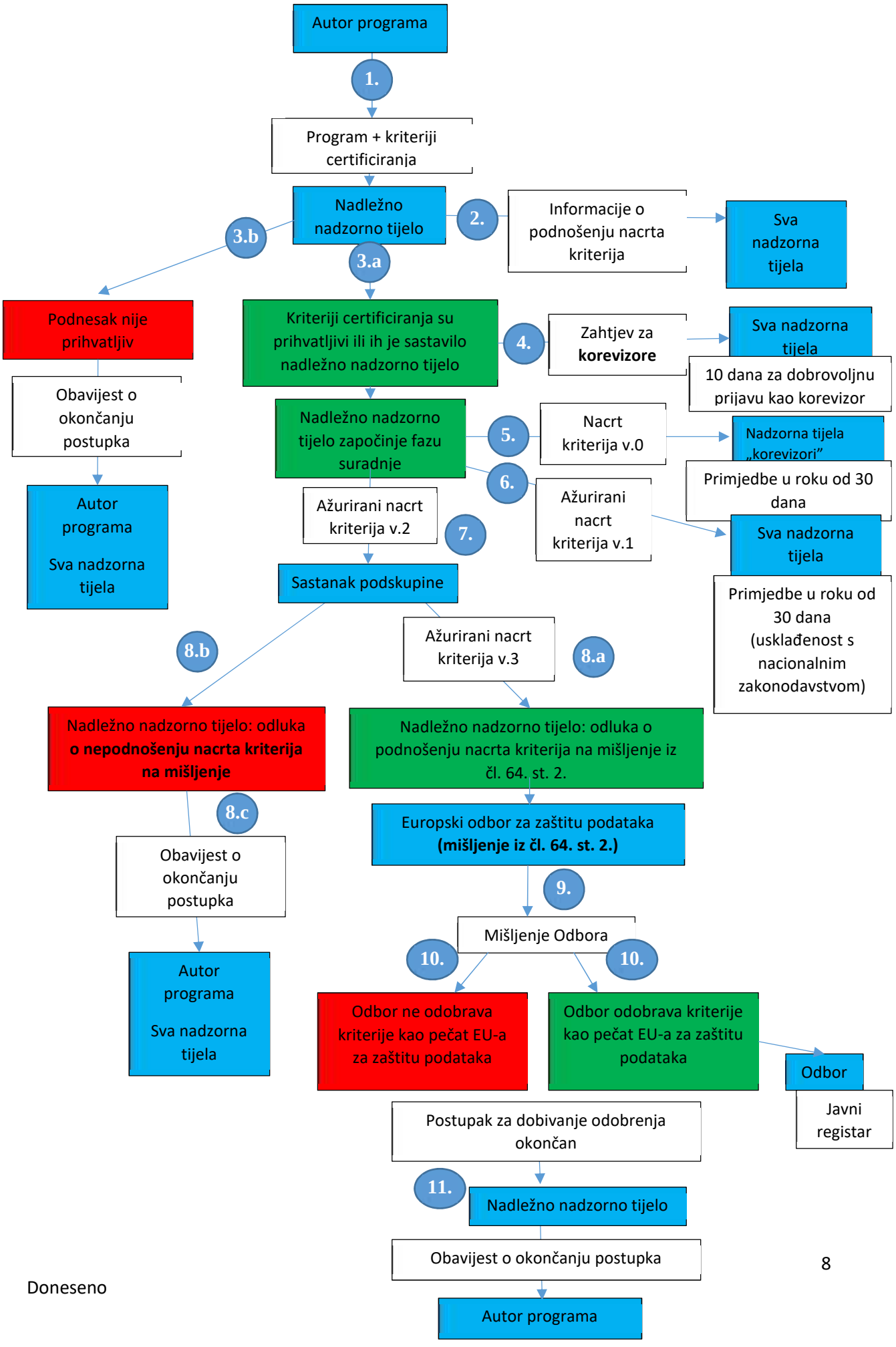
- nadležno nadzorno tijelo obavješćuje autora programa da, prema mišljenju Europskog odbora za zaštitu podataka, mehanizam certificiranja ne ispunjava zahtjeve za dobivanje odobrenja Odbora,
- nadležno nadzorno tijelo može odlučiti ponovno podnijeti kriterije certificiranja radi podnošenja zahtjeva za pečat EU-a za zaštitu podataka. Nadležno nadzorno tijelo može odlučiti započeti novu fazu neformalne suradnje ili podnijeti kriterije izravno u fazi mišljenja na temelju članka 64. stavka 2.

Smjernice o ovlastima Europske komisije na temelju članka 43. stavaka 8. i 9. bit će pravodobno dodane, zajedno sa svim daljnjim zahtjevima za kriterije za međunarodni prijenos.

[10] Treba napomenuti i to da su moguća samo mišljenja kojima se zahtjev „odobrava" ili „odbija" jer bi moglo biti zavaravajuće kad bi se „odobrio" pečat u pogledu kojeg još uvijek postoje neriješena pitanja.

[11] Ako se nadzorno tijelo ne pridržava donesenog mišljenja i ne prihvati odobrenje za pečat EU-a za zaštitu podataka, bilo koje drugo nadzorno tijelo može iznijeti to pitanje pred Odbor kako bi dobilo obvezujuću odluku na temelju članka 65. stavka 1. točke (c)[11].

Tijek rada – Odobrenje kriterija certificiranja za pečat EU-a za zaštitu podataka koje daje Europski odbor za zaštitu podataka



Doneseno