Mišljenje Odbora (članak 64.)

Mišljenje 28/2022 o kriterijima certificiranja Europrivacy u vezi s njihovim odobrenjem kao Europskog pečata za zaštitu podataka koje daje Odbor u skladu s člankom 42. stavkom 5. (Opća uredba o zaštiti podataka)

Doneseno 10. listopada 2022.

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

Europski odbor za zaštitu podataka

uzimajući u obzir članak 63., članak 64. stavak 2. i članak 42. Uredbe 2016/679/EU 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 (u daljnjem tekstu: Opća uredba),

uzimajući u obzir Sporazum o Europskom gospodarskom prostoru (u daljnjem 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 (u daljnjem tekstu: EDPB ili Odbor) i Europska komisija potiču, posebno na razini Unije, uspostavu mehanizama certificiranja zaštite podataka (u daljnjem tekstu: mehanizmi certifikacije) te pečata i oznaka za zaštitu podataka u svrhu dokazivanja usklađenosti postupaka obrade koje provode voditelji obrade i izvršitelji obrade s Općom uredbom, uzimajući u obzir posebne potrebe mikropoduzeća te malih i srednjih poduzeća.[2] Usto, uspostavljanje mehanizama certificiranja može povećati transparentnost i omogućiti ispitanicima da procijene razinu zaštite podataka za relevantne proizvode i usluge.[3]

(2) Kriteriji certificiranja sastavni su dio mehanizma certificiranja. Stoga se Općom uredbom zahtijeva da kriterije nacionalnog mehanizma certificiranja odobri nadležno nadzorno tijelo (članak 42. stavak 5. i članak 43. stavak 2. točka (b) Opće uredbe) ili, u slučaju Europskog pečata za zaštitu podataka, da ih odobri EDPB (članak 42. stavak 5. i članak 70. stavak 1. točka (o) Opće uredbe).

(3) Ako nadzorno tijelo namjerava predložiti odobrenje europskog pečata za zaštitu podataka koje daje EDPB u skladu s člankom 42. stavkom 5. Opće uredbe, nadzorno tijelo 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 Opće uredbe o zaštiti podataka putem mehanizma konzistentnosti iz članaka 63., 64. i 65. Opće uredbe. U tom okviru, u skladu s člankom 64. stavkom 2. Opće uredbe, EDPB odobrava kriterije certificiranja.

(4) Cilj je ovog mišljenja osigurati dosljednu primjenu Opće uredbe, uključujući primjenu koju provode nadzorna tijela, voditelji obrade i izvršitelji obrade s obzirom na ključne elemente koje mehanizmi certificiranja moraju razviti. Konkretno, procjena EDPB-a provodi se na temelju „Smjernica 1/2018 o certificiranju i utvrđivanju kriterija certificiranja u skladu s člancima 42. i 43. Uredbe" (u daljnjem tekstu: Smjernice) i njihova Dodatka u kojemu se navode „Smjernice za ocjenu kriterija certificiranja" (u daljnjem tekstu: Dodatak), za koje je razdoblje javnog savjetovanja isteklo 26. svibnja 2021.

(5) U skladu s tim, EDPB potvrđuje da bi se svaki mehanizam certificiranja trebao rješavati pojedinačno i da se njime ne dovodi u pitanje procjena bilo kojeg drugog mehanizma certificiranja.

(6) Mehanizmi certificiranja trebali bi omogućiti voditeljima obrade i izvršiteljima obrade da dokažu usklađenost s Općom uredbom. Stoga bi kriteriji trebali na odgovarajući način odražavati zahtjeve i

[1] Upućivanja na „države članice" u ovom mišljenju treba tumačiti kao upućivanja na „države članice EGP-a".
[2] Članak 42. stavak 1. Opće uredbe.
[3] Uvodna izjava 100. Opće uredbe.

načela u pogledu zaštite osobnih podataka koji su utvrđeni u Općoj uredbi i pridonijeti njezinoj dosljednoj primjeni.

(7) Istodobno, vlasnik programa trebao bi osigurati usklađivanje i sukladnost mehanizma certificiranja sa svim uključenim ili poboljšanim ISO normama i praksama certificiranja.

(8) Kao rezultat toga, certifikacijama bi se trebala dodati vrijednost voditeljima obrade i izvršiteljima obrade tako što bi se pomoglo u provedbi standardiziranih i određenih organizacijskih i tehničkih mjera kojima se dokazano olakšava i poboljšava usklađenost postupaka obrade s Općom uredbom, uzimajući u obzir zahtjeve specifične za sektor.

(9) EDPB pozdravlja napore koje su vlasnici programa uložili u razradu mehanizama certificiranja, koji su praktični i potencijalno isplativi alati za osiguravanje veće dosljednosti s Općom uredbom te za poticanje prava na privatnost i zaštitu podataka ispitanika povećanjem transparentnosti.

(10) EDPB podsjeća da su certifikacije dobrovoljni alati za odgovornost i da poštovanje mehanizma certificiranja ne umanjuje odgovornost voditelja obrade ili izvršitelja obrade za usklađenost s Općom uredbom niti sprječava nadzorna tijela u izvršavanju njihovih zadaća i ovlasti u skladu s Općom uredbom i relevantnim nacionalnim zakonima.

(11) U ovom se mišljenju EDPB bavi pitanjima kao što su područje primjene kriterija, primjenjivost i relevantnost kriterija u svim državama članicama.

(12) Ovo je mišljenje usmjereno na kriterije certificiranja. U slučaju da EDPB zahtijeva informacije visoke razine o metodama evaluacije kako bi mogao temeljito procijeniti mogućnost revizije kriterija u kontekstu svojeg mišljenja, potonje ne obuhvaća nikakvo odobrenje takvih metoda evaluacije.

(13) Mišljenje EDPB-a donosi se na temelju članka 64. stavka 2. Opće uredbe 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 odluče da je dokumentacija cjelovita. Odlukom predsjednika taj se rok može produljiti za dodatnih šest tjedana, uzimajući u obzir složenost predmeta. Ako se u mišljenju EDPB-a zaključi da se predmetni kriteriji ne mogu odobriti, nadzorno tijelo može ponovno podnijeti kriterije na odobrenje kada se otklone razlozi za zabrinutost izraženi u početnom mišljenju EDPB-a.

DONIO JE SLJEDEĆE MIŠLJENJE:

SAŽETAK ČINJENICA

1. U skladu s člankom 42. stavkom 5. Opće uredbe i Smjernicama, kriterije Europrivacy v.60 (u daljnjem tekstu: nacrt kriterija certificiranja, kriteriji certificiranja ili kriteriji) sastavio je Europski centar za certifikaciju i privatnost (u daljnjem tekstu: vlasnik programa).

2. Nadzorno tijelo Luksemburga (u daljnjem tekstu: luksemburško nadzorno tijelo) 28. rujna 2022. podnijelo je EDPB-u na odobrenje kriterije certificiranja Europrivacy u skladu s člankom 64. stavkom 2. Opće uredbe. Odluka da je dokumentacija cjelovita donesena je 28. rujna 2022.

3. Mehanizam certificiranja Europrivacy nije certifikacija u skladu s člankom 46. stavkom 2. točkom (f) Opće uredbe namijenjena za međunarodne prijenose osobnih podataka, stoga ne pruža odgovarajuće zaštitne mjere u okviru prijenosa osobnih podataka trećim zemljama ili međunarodnim organizacijama pod uvjetima iz članka 46. stavka 2. točke (f). Naime, svaki prijenos osobnih podataka trećoj zemlji ili međunarodnoj organizaciji provodi se samo ako se poštuju odredbe poglavlja V. Opće uredbe.

2 PROCJENA

4. EDPB je proveo procjenu kriterija certificiranja radi njihova odobrenja na temelju članka 42. stavka 5. Opće uredbe u skladu sa strukturom predviđenom u Prilogu 2. Smjernicama (u daljnjem tekstu: Prilog) i Dodatku Smjernicama.

5. EDPB napominje da provedbene smjernice i predloženi načini provjere mehanizma certificiranja koje pruža vlasnik programa nisu uvijek dosljedni u cijelom katalogu kriterija. Primjerice, u odjeljku T.2.3.2. zahtijeva se da pravila, politike, postupci ili mehanizmi budu uspostavljeni radi otkrivanja i prijavljivanja neovlaštenog ulaska (npr. sustav za otkrivanje neovlaštenog ulaska kojim se prati mrežni promet zbog sumnjivih aktivnosti i upozorenja kada je takva aktivnost otkrivena), dok se predloženi načini provjere odnose na inspekciju i penetracijska testiranja (koja se zahtijevaju u odjeljku T.2.3.1.). Iako takve nedosljednosti nisu obuhvaćene njegovom procjenom, EDPB ističe da one mogu biti prepreka akreditaciji certifikacijskog tijela, osim ako ih vlasnik programa ne ispravi.

2.1 Područje primjene mehanizma certificiranja i predmet evaluacije (ToE)

6. Mehanizam certificiranja Europrivacy opći je program jer je usmjeren na širok raspon različitih postupaka obrade koje provode voditelji obrade i izvršitelji obrade iz različitih sektora djelatnosti. Glavni kriteriji tog mehanizma certificiranja sastoje se od „temeljnih kriterija" i „provjera i kontrola tehničkih i organizacijskih mjera" u pogledu tehnoloških i organizacijskih mjera uspostavljenih kako bi se osigurali obrađeni osobni podatci. Skup kriterija „provjere i kontrole tehničkih i organizacijskih mjera" primjenjuje se samo ako se u okviru predmeta evaluacije obrađuju posebne kategorije podataka, podatci povezani s kaznenim djelima ili osobni podatci djeteta.

7. Uz to, kriteriji uključuju i „dopunske kontekstualne provjere i kontrole" čiji je cilj osigurati da obrada podataka koja je uključena u predmet evaluacije bude u skladu sa zahtjevima specifičnima za određeno područje i zahtjevima specifičnima za određenu tehnologiju. U informativnoj matrici koju je dostavio vlasnik sustava opisuje se na koje se kategorije postupaka obrade podataka primjenjuje svaki skup kriterija za „dopunske kontekstualne provjere i kontrole".

8. EDPB pozdravlja opće programe koji uključuju posebne kriterije kako bi ih se učinilo prilagodljivima i primjenjivima na određene postupke obrade ili sektor djelatnosti. Međutim, EDPB želi pojasniti i da u kontekstu općeg programa potpunost kriterija koji se odnose na određene postupke obrade nije potrebna te stoga ona nije ocijenjena u kontekstu ovog mišljenja. Uz to, EDPB podsjeća da pri objavljivanju dokumenata povezanih s određenim aktivnostima obrade vlasnik programa i akreditirana certifikacijska tijela uzimaju u obzir takve dokumente.

9. Kriteriji koji se primjenjuju na specifikaciju predmeta evaluacije definirani su u zahtjevima iz odjeljka A.2.1.1. Posebna pravila koja se primjenjuju na postupak koja podnositelj zahtjeva i certifikacijsko tijelo trebaju slijediti kako bi definirali predmet evaluacije utvrđena su u programu Europrivacy (10.2. – Aktivnosti prije certifikacije).

10. Odbor u dokumentaciji povezanoj s područjem primjene mehanizma certificiranja, koju je dostavilo luksemburško nadzorno tijelo, napominje da se program Europrivacy primjenjuje na voditelje obrade i izvršitelje obrade s poslovnim nastanom u Europskoj uniji (EU) ili u Europskom gospodarskom prostoru (EGP). Primjenjivost kriterija definirana je ovisno o ulozi i odgovornostima podnositelja zahtjeva

11. Odbor napominje da voditelj obrade podataka može na postupak certificiranja Europrivacy podnijeti predmet evaluacije koji podliježe zajedničkom vođenju obrade (kriteriji A.2.7.1.). Ako predmet evaluacije podliježe zajedničkom vođenju obrade, Odbor želi naglasiti da će akreditirano certifikacijsko tijelo morati pažljivo provesti postupak podnošenja zahtjeva kako bi se osiguralo da predmet evaluacije bude smislen i da podnositelj zahtjeva bude u potpunosti odgovoran za usklađenost predmeta evaluacije sa svim obvezama iz Opće uredbe koje se nastoje dokazati mehanizmom certificiranja. Posljedično, dogovor koji su sklopili podnositelj zahtjeva i drugi zajednički voditelji obrade uključeni u predmet evaluacije u pogledu njihovih pojedinačnih odgovornosti za poštovanje obveza iz Opće uredbe[4] mogao bi, ovisno o kontekstu aktivnosti obrade predmeta evaluacije, spriječiti podnositelja zahtjeva da ispuni kriterije certificiranja.

12. Odbor napominje da je obrada podataka genetskih podataka isključena iz područja primjene mehanizma certificiranja Europrivacy. Stoga procjena kriterija koju provodi Odbor ne obuhvaća prikladnost kriterija za predmet evaluacije koji bi uključivali takvu obradu podataka.

2.2 Postupci obrade

13. Kriteriji se odnose na relevantne sastavnice postupaka obrade (podatci, sustavi i obrada) u pogledu općeg područja primjene mehanizma certificiranja. Konkretno, kriteriji omogućuju utvrđivanje posebnih kategorija podataka kako su definirane u članku 9. Opće uredbe (odjeljak G.2. kriterija – posebna obrada podataka).

2.3 Zakonitost obrade podataka

14. Kriteriji zahtijevaju provjeru zakonitosti obrade podataka za svaki pojedinačni postupak obrade u predmetu evaluacije i zahtijevaju provjeru zahtjeva pravne osnove kako je definirana u članku 6. Opće uredbe (odjeljak G.1. kriterija – Zakonitost obrade podataka).

2.4 Načela obrade podataka

15. Kriteriji se na odgovarajući način odnose na načela zaštite podataka u skladu s člankom 5. Opće uredbe. Posebno se kriterijima od podnositelja zahtjeva zahtijeva da dokaže da su osobni podatci primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju (smanjenje količine podataka).

2.5 Opće obveze voditelja obrade i izvršitelja obrade

16. Kriteriji odražavaju obveze voditelja obrade u skladu s člankom 24. Opće uredbe (G.4. – Odgovornost voditelja obrade podataka) i zahtijevaju evaluaciju ugovornih sporazuma između izvršitelja obrade i voditelja obrade u skladu s člankom 28. Opće uredbe (odjeljak G.5. kriterija – Izvršitelji obrade podataka ili podizvršitelji obrade podataka).

17. Prema kriterijima, svi podnositelji zahtjeva moraju imenovati službenika za zaštitu podataka, čak i ako podnositelj zahtjeva nije obvezan imenovati službenika za zaštitu podataka u skladu s člankom 37.

[4] *Utvrđivanje njihovih odgovornosti mora se osobito odnositi na ostvarivanje prava ispitanika i dužnosti pružanja informacija. Uz to, podjela odgovornosti treba obuhvatiti i druge obveze voditelja obrade, poput obveza koje se odnose na opća načela zaštite podataka, pravnu osnovu, sigurnosne mjere, obvezu obavješćivanja o povredi podataka, procjene utjecaja na zaštitu podataka, angažiranje izvršitelja obrade, prijenose u treće zemlje i kontakte s ispitanicima i nadzornim tijelima* (Smjernice 07/2020 o konceptima voditelja obrade i izvršitelja obrade u Općoj uredbi)

Opće uredbe. Kriterijima se provjerava ispunjava li službenik za zaštitu podataka zahtjeve iz članaka od 37. do 39. (odjeljak G.9. kriterija – Službenik za zaštitu podataka).

18. Kriterijima se provjerava sadržaj evidencije o aktivnostima obrade u skladu s člankom 30. Opće uredbe (odjeljak G.5.3. kriterija – Evidencija aktivnosti obrade).

2.6 Prava ispitanikâ

19. Kriteriji se na odgovarajući način bave pravom ispitanika na informacije u skladu s poglavljem III. Opće uredbe i zahtijevaju uspostavu odgovarajućih mjera. Kriterijima se zahtijeva i uspostava mjera kojima se predviđa mogućnost intervencije u postupak obrade kako bi se zajamčila prava ispitanikâ i omogućili ispravci, brisanje ili ograničenja (odjeljak G.3. kriterija – Prava ispitanikâ).

2.7 Rizici za prava i slobodu

20. Prema kriterijima potrebno je procijeniti rizik za prava i slobode pojedinaca povezan s obradom podataka uključenom u predmet evaluacije u skladu s člankom 35. Opće uredbe (odjeljak G.8. kriterija – Procjena učinka zaštite podataka).

2.8 Tehničke i organizacijske mjere kojima se jamči zaštita

21. Kriteriji zahtijevaju primjenu tehničkih i organizacijskih mjera kojima se osigurava povjerljivost, cjelovitost i dostupnost postupaka obrade. Kriterijima se također zahtijeva primjena tehničkih mjera za provedbu tehničke i integrirane zaštite podataka u skladu s člancima 25. i 32. Opće uredbe (odjeljak G.6. kriterija – Sigurnost obrade i tehnička zaštita podataka, odjeljak T.1./T.2. kriterija – Osnovni sigurnosni zahtjevi / prošireni sigurnosni zahtjevi).

22. Kriterijima se zahtijeva primjena mjere kako bi se osiguralo da se obveze obavješćivanja o povredi osobnih podataka izvršavaju pravodobno i u skladu s člancima 33. i 34. Opće uredbe (odjeljak G.7. kriterija – Upravljanje povredama podataka).

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

23. Kriterijima se zahtijeva utvrđivanje svih prijenosa osobnih podataka trećim zemljama i međunarodnim organizacijama uključenima u predmet evaluacije te obrazloženje odabira mehanizma za prijenos podataka kojim se osiguravaju odgovarajuće zaštitne mjere u skladu s poglavljem V. Opće uredbe (odjeljak G.10. kriterija – Prijenosi osobnih podataka trećim zemljama ili međunarodnim organizacijama).

3. DODATNI KRITERIJI ZA EUROPSKI PEČAT ZA ZAŠTITU PODATAKA

24. U skladu sa Smjernicama, procjena uključuje pitanje „mogu li se u kriterijima uzeti u obzir zakoni ili scenariji država članica o zaštiti podataka”. U odjeljku G.1.1.3. kriterija od podnositelja zahtjeva traži se da takvu procjenu dostavi u izvješću o ocjeni usklađenosti s nacionalnim obvezama (NOCAR). Odbor napominje da takvo izvješće uključuje procjenu nacionalnih obveza koje se primjenjuju na predmet evaluacije te da se u njemu dokumentiraju mjere koje je podnositelj zahtjeva poduzeo kako bi ispunio primjenjiva pravila i, po mogućnosti, korektivne mjere koje su u tijeku. Podnositelj zahtjeva ne smije upotrebljavati popis ključnih dopunskih nacionalnih zahtjeva koji je za svaku zemlju dostavio vlasnik programa kao iscrpan popis nacionalnih obveza relevantnih za predmet evaluacije. Okvirni popis

minimalnih dodatnih provjera i kontrola koje je dostavio vlasnik programa ne predstavlja kriterije certificiranja u okviru ovog mišljenja.

ZAKLJUČCI/PREPORUKE

25. Zaključno, EDPB smatra da su kriteriji certificiranja Europrivacy sukladni s Općom uredbom te ih odobrava u skladu sa zadaćom Odbora utvrđenom u članku 70. stavku 1. točki (o) Opće uredbe, što dovodi do zajedničkog certificiranja (Europski pečat za zaštitu podataka).

26. EDPB će registrirati mehanizam certificiranja Europrivacy u javnom registru mehanizama certificiranja te pečata i oznaka za zaštitu podataka u skladu s člankom 42. stavkom 8.

ZAVRŠNE NAPOMENE

27. 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