Mnenje št. 28/2022 o merilih potrjevanja Europrivacy v zvezi z njihovo odobritvijo s strani odbora kot evropskega pečata za varstvo podatkov v skladu s členom 42.5 Splošne uredbe o varstvu podatkov

Sprejeto 10. oktobra 2022

Evropski odbor za varstvo podatkov je –

ob upoštevanju členov 63, 64(2) in 42 Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: Splošna uredba o varstvu podatkov),

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

ob upoštevanju členov 10 in 22 svojega poslovnika,

(1) ob upoštevanju naslednjega: države članice, nadzorni organi, Evropski odbor za varstvo podatkov in Evropska komisija zlasti na ravni Unije spodbujajo vzpostavitev mehanizmov potrjevanja za varstvo podatkov (v nadaljevanju: mehanizmi potrjevanja) ter pečatov in označb za varstvo podatkov za namene dokazovanja, da so dejanja obdelave, ki jih izvajajo upravljavci in obdelovalci, v skladu s Splošno uredbo o varstvu podatkov, ob upoštevanju posebnih potreb mikro, malih in srednjih podjetij.[2] Poleg tega se lahko z uvedbo mehanizmov potrjevanja poveča preglednost in posameznikom, na katere se nanašajo osebni podatki, omogoči, da ocenijo raven varstva podatkov zadevnih proizvodov in storitev.[3]

(2) Merila potrjevanja so sestavni del mehanizma potrjevanja. Splošna uredba o varstvu podatkov zato zahteva odobritev meril nacionalnega mehanizma potrjevanja s strani pristojnega nadzornega organa (člena 42(5) in 43(2)(b) Splošne uredbe o varstvu podatkov) ali v primeru evropskega pečata za varstvo podatkov s strani Evropskega odbora za varstvo podatkov (člena 42(5) in 70(1)(o) Splošne uredbe o varstvu podatkov).

(3) Kadar namerava nadzorni organ predlagati odobritev evropskega žiga za varstvo podatkov s strani Evropskega odbora za varstvo podatkov v skladu s členom 42(5) Splošne uredbe o varstvu podatkov, mora navesti namen lastnika sheme, da bo mehanizem potrjevanja zagotavljal v vseh državah članicah. V tem primeru je glavna vloga Evropskega odbora za varstvo podatkov zagotoviti dosledno uporabo Splošne uredbe o varstvu podatkov prek mehanizma za skladnost iz členov 63, 64 in 65 navedene uredbe. V tem okviru Evropski odbor za varstvo podatkov v skladu s členom 64(2) Splošne uredbe o varstvu podatkov odobri merila potrjevanja.

(4) Cilj tega mnenja je zagotoviti dosledno uporabo Splošne uredbe o varstvu podatkov, vključno na ravni nadzornih organov, upravljavcev in obdelovalcev, ob upoštevanju glavnih elementov, ki jih morajo razviti mehanizmi potrjevanja. Ocena Evropskega odbora za varstvo podatkov temelji zlasti na „Smernicah št. 1/2018 o certificiranju in opredelitvi meril za certificiranje v skladu s členoma 42 in 43 Uredbe“ (v nadaljevanju: smernice) in njihovem dodatku, ki vsebuje „smernice o oceni meril potrjevanja (v nadaljevanju: dodatek), za katerega se je obdobje javnega posvetovanja izteklo 26. maja 2021.

(5) V skladu s tem Evropski odbor za varstvo podatkov priznava, da bi bilo treba vsak mehanizem potrjevanja obravnavati posamično in brez poseganja v oceno drugih mehanizmov potrjevanja.

[1] Sklice na „države članice“ v tem mnenju je treba razumeti kot sklice na „države članice EGP“.
[2] Člen 42(1) Splošne uredbe o varstvu podatkov.
[3] Uvodna izjava 100 Splošne uredbe o varstvu podatkov.

(6) Mehanizmi potrjevanja bi morali omogočati upravljavcem in obdelovalcem, da dokažejo skladnost s Splošno uredbo o varstvu podatkov. Njihova merila bi zato morala ustrezno odražati zahteve in načela varstva osebnih podatkov iz Splošne uredbe o varstvu podatkov ter prispevati k njeni dosledni uporabi.

(7) Hkrati bi moral lastnik sheme zagotoviti usklajenost mehanizma potrjevanja z vsemi vključenimi ali izboljšanimi standardi ISO in praksami potrjevanja.

(8) Potrdila bi zato morala dodati vrednost upravljavcem in obdelovalcem ter jim pomagati izvajati standardizirane in določene organizacijske in tehnične ukrepe, ki ob upoštevanju sektorskih zahtev dokazano olajšujejo in povečujejo skladnost obdelave s Splošno uredbo o varstvu podatkov.

(9) Evropski odbor za varstvo podatkov pozdravlja prizadevanje lastnikov shem pri razvoju mehanizmov potrjevanja, ki so praktična in po možnosti stroškovno učinkovita orodja za zagotavljanje večje skladnosti s Splošno uredbo o varstvu podatkov ter z večanjem preglednosti krepijo pravico posameznikov, na katere se nanašajo osebni podatki, do zasebnosti in varstva podatkov.

(10) Evropski odbor za varstvo podatkov opozarja, da so potrdila prostovoljna orodja, ki zagotavljajo odgovornost, ter da upoštevanje mehanizma potrjevanja ne zmanjšuje odgovornosti upravljavcev ali obdelovalcev za skladnost s Splošno uredbo o varstvu podatkov ali ne preprečuje nadzornim organom izvajati njihove naloge in pooblastila v skladu z navedeno uredbo in zadevnim nacionalnim pravom.

(11) Evropski odbor za varstvo podatkov v tem mnenju obravnava vprašanja, kot so področje uporabe meril ter uporaba in ustreznost meril v vseh državah članicah.

(12) To mnenje je osredinjeno na merila potrjevanja. Če Evropski odbor za varstvo podatkov zahteva informacije na visoki ravni o metodah vrednotenja, da bi lahko temeljito ocenil možnost revidiranja meril v okviru tega mnenja, to ne vključuje odobritve takih metod vrednotenja.

(13) Mnenje Evropskega odbora za varstvo podatkov se sprejme v skladu s členom 64(2) Splošne uredbe o varstvu podatkov v povezavi s členom 10(2) poslovnika Evropskega odbora za varstvo podatkov v osmih tednih od prvega delovnega dne po odločitvi predsednika in pristojnega nadzornega organa, da je dokumentacija popolna. Po predsednikovi odločitvi se glede na kompleksnost vsebine to obdobje lahko podaljša za šest tednov. Če Evropski odbor za varstvo podatkov v mnenju sprejme sklep, da zadevnih meril ni mogoče odobriti, lahko nadzorni organ merila vnovič predloži v odobritev, ko so pomisleki iz prvega mnenja Evropskega odbora za varstvo podatkov odpravljeni –

SPREJEL NASLEDNJE MNENJE:

POVZETEK DEJSTEV

1. Merila sheme Europrivacy v.60 (v nadaljevanju: osnutek meril potrjevanja, merila potrjevanja ali merila) je v skladu s členom 42(5) Splošne uredbe o varstvu podatkov in smernicami pripravil Evropski center za potrjevanje in zasebnost (*European Center for Certification and Privacy*) (v nadaljevanju: lastnik sheme).

2. Nadzorni organ Luksemburga je merila potrjevanja sheme Europrivacy 28. septembra 2022 predložil Evropskemu odboru za varstvo podatkov v odobritev v skladu s členom 64(2) Splošne uredbe o varstvu podatkov. Sklep o popolnosti dokumentacije je bil sprejet 28. septembra 2022.

3. Mehanizem potrjevanja Europrivacy ni potrjevanje za mednarodne prenose osebnih podatkov iz člena 46(2)(f) Splošne uredbe o varstvu podatkov in zato ne zagotavlja ustreznih zaščitnih ukrepov v okviru prenosov osebnih podatkov v tretje države ali mednarodne organizacije v skladu s točko (f)

člena 46(2). Prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo se dejansko lahko izvede le ob upoštevanju določb poglavja V Splošne uredbe o varstvu podatkov.

2 OCENA

4. Evropski odbor za varstvo podatkov je ocenil merila potrjevanja za njihovo odobritev na podlagi člena 42(5) Splošne uredbe o varstvu podatkov v skladu s strukturo iz Priloge 2 k smernicam (v nadaljevanju: priloga) in njihovega dodatka.

5. Evropski odbor za varstvo podatkov ugotavlja, da smernice za izvajanje in predlagani načini preverjanja mehanizma potrjevanja, ki jih je zagotovil lastnik sheme, v katalogu meril niso vedno usklajeni. Na primer, v skladu z oddelkom T.2.3.2 je treba uvesti pravila, politike, postopke ali mehanizme za odkrivanje vdorov in poročanje o njih (na primer sistem za odkrivanje vdorov, ki spremlja omrežni promet za odkrivanje sumljive dejavnosti in opozarja, ko se taka dejavnost odkrije), predlagani načini preverjanja pa se nanašajo na inšpekcijski pregled in penetracijsko testiranje (ki se zahtevata v skladu z oddelkom T.2.3.1). Čeprav taka neskladja ne spadajo na področje uporabe njegove ocene, Evropski odbor za varstvo podatkov poudarja, da bi lahko bila ovira za pooblastitev organa za potrjevanje, če jih lastnik sheme ne odpravi.

2.1 Področje uporabe mehanizma potrjevanja in cilj ovrednotenja

6. Mehanizem potrjevanja Europrivacy je splošna shema, saj je ciljno usmerjena v najrazličnejša dejanja obdelave, ki jih izvajajo upravljavci ali obdelovalci z različnih področij dejavnosti. Glavna merila tega mehanizma potrjevanja sestavljajo „osnovna merila“ ter „preverjanja in kontrole tehnoloških in organizacijskih ukrepov“, ki se nanašajo na tehnološke in organizacijske ukrepe, vzpostavljene za zavarovanje obdelanih osebnih podatkov. Niz preverjanj in kontrol tehnoloških ter organizacijskih ukrepov se lahko uporablja le, če se v okviru cilja ovrednotenja obdelujejo posebne vrste podatkov, podatki v zvezi s kaznivimi dejanji ali osebni podatki otroka.

7. Poleg tega merila vključujejo tudi „dopolnilna vsebinska preverjanja in kontrole“, katerih cilj je zagotoviti, da je obdelava podatkov, vključena v cilj ovrednotenja, v skladu s področnimi in tehnološkimi zahtevami. V informativni matriki, ki jo je zagotovil lastnik sheme, je opisano, za katere vrste dejanj obdelave podatkov se uporabljajo merila posameznega niza „dopolnilnih vsebinskih preverjanj in kontrol“.

8. Evropski odbor za varstvo podatkov pozdravlja splošne sheme, ki vključujejo specifična merila ter jih je zato mogoče nadgraditi in uporabljati za specifična dejanja obdelave ali področja dejavnosti. Vendar Evropski odbor za varstvo podatkov želi tudi pojasniti, da se v okviru splošne sheme ne zahteva popolnost meril za specifična dejanja obdelave, zato v okviru tega mnenja ta ni bila ocenjena. Poleg tega Evropski odbor za varstvo podatkov opozarja, da kadar objavi dokumente v zvezi s specifičnimi dejanji obdelave, jih morajo lastnik sheme in pooblaščeni organi za potrjevanje upoštevati.

9. Merila, ki se uporabljajo za določitev cilja ovrednotenja, so opredeljena v zahtevah iz oddelka A.2.1.1. V shemi Europrivacy so navedena specifična pravila, ki se uporabljajo za obdelavo ter jih morata upoštevati vložnik in organ za potrjevanje pri opredelitvi cilja ovrednotenja (10.2 – Dejavnosti pred potrjevanjem).

10. Evropski odbor za varstvo podatkov na podlagi dokumentacije o področju uporabe mehanizma potrjevanja, ki jo je zagotovil nadzorni organ Luksemburga, ugotavlja, da se shema Europrivacy

uporablja za upravljavce in obdelovalce s sedežem v Evropski uniji (EU) ali v Evropskem gospodarskem prostoru (EGP). Uporaba meril je opredeljena glede na vlogo in odgovornosti vložnika.

11. Evropski odbor za varstvo podatkov ugotavlja, da lahko upravljavec podatkov predloži v postopek potrjevanja v okviru sheme Europrivacy cilj ovrednotenja, ki je predmet skupnega upravljanja (merila A.2.7.1). Kadar je cilj ovrednotenja predmet skupnega upravljanja, želi Evropski odbor za varstvo podatkov poudariti, da mora pooblaščeni organ za potrjevanje skrbno izvesti postopek vložitve, da zagotovi, da je cilj ovrednotenja smiseln in da je vložnik v celoti odgovoren, da ta cilj izpolnjuje vse obveznosti iz Splošne uredbe o varstvu podatkov, kar naj bi se dokazalo z mehanizmom potrjevanja. Dogovor, sklenjen med vložnikom in drugimi skupnimi upravljavci iz cilja ovrednotenja v zvezi z njihovimi zadevnimi odgovornostmi za izpolnjevanje obveznosti iz Splošne uredbe o varstvu podatkov[4], bi lahko vložniku glede na okoliščine dejavnosti na področju obdelave cilja ovrednotenja preprečil izpolnitev meril potrjevanja.

12. Evropski odbor za varstvo podatkov ugotavlja, da je obdelava genskih podatkov izključena s področja uporabe mehanizma potrjevanja Europrivacy, zato ocena meril, ki jo je opravil Evropski odbor za varstvo podatkov, ne vsebuje presoje ustreznosti meril za cilj ovrednotenja, ki bi vključeval obdelavo takih podatkov.

2.2 Postopki obdelave

13. Merila obravnavajo ustrezne elemente dejanj obdelave (podatke, sisteme in obdelavo) glede na splošno področje uporabe mehanizma potrjevanja. Merila zlasti omogočajo opredelitev posebnih vrst podatkov, kot so opredeljeni v členu 9 Splošne uredbe o varstvu podatkov (oddelek G.2 meril – Obdelava posebnih podatkov).

2.3 Zakonitost obdelave

14. Merila zahtevajo preverjanje zakonitosti obdelave podatkov za vsako posamezno dejanje obdelave v okviru cilja ovrednotenja in preverjanje zahtev pravne podlage iz člena 6 Splošne uredbe o varstvu podatkov (oddelek G.1 meril – Zakonitost obdelave podatkov).

2.4 Načela obdelave podatkov

15. Merila ustrezno obravnavajo načela varstva podatkov v skladu s členom 5 Splošne uredbe o varstvu podatkov. V skladu z merili mora vložnik zlasti dokazati, da so osebni podatki „ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo“ (najmanjši obseg podatkov).

2.5 Splošne obveznosti upravljavcev in obdelovalcev

16. V skladu z merili, ki izražajo obveznosti upravljavca iz člena 24 Splošne uredbe o varstvu podatkov (G.4 – Odgovornost upravljavca podatkov), je treba ovrednotiti pogodbene dogovore med obdelovalcem in upravljavcem v skladu s členom 28 Splošne uredbe o varstvu podatkov (oddelek G.5 meril – Obdelovalci ali podobdelovalci podatkov).

[4] *Pri določitvi dolžnosti vsakega od njih je treba zlasti upoštevati uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki, in naloge glede zagotavljanja informacij. Poleg tega je treba pri porazdelitvi odgovornosti upoštevati druge upravljavčeve obveznosti, kot so tiste v zvezi s splošnimi načeli varstva podatkov, pravno podlago, varnostnimi ukrepi, obveznostjo uradnega obveščanja o kršitvi varstva podatkov, ocenami učinka v zvezi z varstvom podatkov, uporabo obdelovalcev, prenosi v tretje države ter stiki s posamezniki, na katere se nanašajo osebni podatki, in nadzornimi organi.* (Smernice 07/2020 o pojmih upravljavec in obdelovalec iz splošne uredbe o varstvu podatkov).

17. V skladu z merili morajo vsi vložniki imenovati pooblaščeno osebo za varstvo podatkov, tudi kadar je vložniku ni treba imenovati v skladu s členom 37 Splošne uredbe o varstvu podatkov. V skladu z merili je treba preveriti, ali pooblaščena oseba za varstvo podatkov izpolnjuje zahteve iz členov 37 do 39 (oddelek G.9 meril – Pooblaščena oseba za varstvo podatkov).

18. V skladu z merili je treba preveriti vsebino evidence o dejavnostih obdelave v skladu s členom 30 Splošne uredbe o varstvu podatkov (oddelek G.5.3 meril – Evidenca o dejavnostih obdelave).

2.6 Pravice posameznikov, na katere se nanašajo osebni podatki

19. Merila ustrezno obravnavajo pravico posameznika, na katerega se nanašajo osebni podatki, do obveščenosti v skladu s poglavjem III Splošne uredbe o varstvu podatkov in zahtevajo uvedbo ustreznih ukrepov. V skladu z merili je treba uvesti tudi ukrepe, ki omogočajo posredovanje pri obdelavi, da se posameznikom, na katere se nanašajo osebni podatki, zagotovijo pravice in dovolijo popravki, izbris ali omejitve (oddelek G.3 meril – Pravice posameznikov, na katere se nanašajo osebni podatki).

2.7 Tveganja za pravice in svoboščine

20. V skladu z merili je treba oceniti tveganje za pravice in svoboščine posameznikov zaradi obdelave podatkov v okviru cilja ovrednotenja v skladu s členom 35 Splošne uredbe o varstvu podatkov (oddelek G.8 meril – Ocena učinka v zvezi z varstvom podatkov).

2.8 Tehnični in organizacijski ukrepi, ki jamčijo varstvo podatkov

21. V skladu z merili je treba uporabljati tehnične in organizacijske ukrepe, ki zagotavljajo zaupnost, celovitost in dostopnost dejanj obdelave. V skladu z merili je treba uporabljati tudi tehnične ukrepe za izvajanje vgrajenega in privzetega varstva podatkov v skladu s členoma 25 in 32 Splošne uredbe o varstvu podatkov (oddelek G.6 meril – Varnost obdelave in vgrajeno varstvo podatkov, oddelek T.1/T.2 meril – Osnovne varnostne zahteve/Razširjene varnostne zahteve).

22. V skladu z merili je treba uporabljati ukrep za zagotovitev, da se dolžnosti uradnega obveščanja o kršitvi varstva osebnih podatkov izpolnijo pravočasno in v ustreznem obsegu v skladu s členoma 33 in 34 Splošne uredbe o varstvu podatkov (oddelek G.7 meril – Obvladovanje kršitev varstva podatkov).

2.9 Merila za dokazovanje obstoja ustreznih zaščitnih ukrepov za prenos osebnih podatkov

23. Merila zahtevajo opredelitev vseh prenosov osebnih podatkov v tretje države in mednarodne organizacije, vključene v cilj ovrednotenja, in utemeljitev izbire mehanizma prenosa podatkov, ki zagotavlja ustrezne zaščitne ukrepe, v skladu s poglavjem V Splošne uredbe o varstvu podatkov (oddelek G.10 meril – Prenosi osebnih podatkov tretjim državam ali mednarodnim organizacijam).

3. DODATNA MERILA ZA EVROPSKI ŽIG ZA VARSTVO PODATKOV

24. V skladu s smernicami ocena vključuje vprašanje, „ali merila lahko upoštevajo zakonodajo ali scenarije držav članic na področju varstva podatkov“. V skladu z oddelkom G.1.1.3 meril mora vložnik tako oceno zagotoviti v poročilu o oceni izpolnjevanja nacionalnih obveznosti (NOCAR). Evropski odbor za varstvo podatkov poudarja, da mora tako poročilo vključevati oceno nacionalnih obveznosti, ki se uporabljajo za cilj ovrednotenja, ter dokumentirati ukrepe, ki jih je sprejel vložnik za upoštevanje veljavnih pravil in po možnosti popravljalnih ukrepov v teku. Vložnik ne sme uporabljati seznama

ključnih dodatnih nacionalnih zahtev, ki jih je zagotovil lastnik sheme za vsako državo, kot izčrpni seznam nacionalnih obveznosti za cilj ovrednotenja. Okvirni seznam minimalnih dodatnih zahtev glede preverjanj in kontrol, ki ga je zagotovil lastnik sheme, niso merila potrjevanja na področju uporabe tega mnenja.

SKLEPNE UGOTOVITVE/PRIPOROČILA

25. Glede na navedeno Evropski odbor za varstvo podatkov meni, da so merila potrjevanja Europrivacy v skladu s Splošno uredbo o varstvu podatkov, in jih odobri v skladu s svojo nalogo iz člena 70(1)(o) navedene uredbe, pri čemer je rezultat skupno potrjevanje (evropski pečat za varstvo podatkov).

26. Evropski odbor za varstvo podatkov bo vpisal mehanizem potrjevanja Europrivacy v javni register mehanizmov potrjevanja ter pečatov in označb za varstvo podatkov v skladu s členom 42(8).

KONČNE PRIPOMBE

27. To mnenje je namenjeno nadzornemu organu Luksemburga in bo v skladu s členom 64(5)(b) Splošne uredbe o varstvu podatkov na voljo javnosti.

Za Evropski odbor za varstvo podatkov

Predsednica