Mnenje odbora (člen 64)

Mnenje št. 19/2024 o merilih za certificiranje EuroPrise v zvezi z njihovo odobritvijo s strani odbora kot evropskega pečata za varstvo podatkov v skladu s petim odstavkom 42. člena Splošne uredbe o varstvu podatkov

Sprejeto 16. julija 2024

Kazalo

Evropski odbor za varstvo podatkov je –

ob upoštevanju 63. člena, drugega odstavka 64. člena in 42. člena 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 10. in 22. člena 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 certificiranja za varstvo podatkov (v nadaljevanju: mehanizmi certificiranja) 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 certificiranja poveča preglednost in posameznikom, na katere se nanašajo osebni podatki, omogoči, da ocenijo raven varstva podatkov zadevnih proizvodov in storitev.[3]

(2) Merila za certificiranje so sestavni del mehanizma certificiranja. Splošna uredba o varstvu podatkov zato zahteva odobritev meril nacionalnega mehanizma certificiranja s strani pristojnega nadzornega organa (peti odstavek 42. člena in točka b drugega odstavka 43. člena Splošne uredbe o varstvu podatkov) ali v primeru evropskega pečata za varstvo podatkov s strani Evropskega odbora za varstvo podatkov (peti odstavek 42. člena in točka o prvega odstavka 70. člena Splošne uredbe o varstvu podatkov).

(3) Kadar namerava nadzorni organ predlagati odobritev evropskega pečata za varstvo podatkov s strani Evropskega odbora za varstvo podatkov v skladu s petim odstavkom 42. člena Splošne uredbe o varstvu podatkov, mora navesti namen lastnika sheme, da bo mehanizem certificiranja 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 63., 64. in 65. člena navedene uredbe. V tem okviru Evropski odbor za varstvo podatkov v skladu z drugim odstavkom 64. člena Splošne uredbe o varstvu podatkov odobri merila za certificiranje.

(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 certificiranja. 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 za

[1] Sklice na „države članice“ v tem mnenju je treba razumeti kot sklice na „države članice EGP“.
[2] Prvi odstavek 60. člena Splošne uredbe o varstvu podatkov.
[3] Uvodna izjava 100 Splošne uredbe o varstvu podatkov.

certificiranje (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 certificiranja obravnavati posamično in brez poseganja v oceno drugih mehanizmov certificiranja.

(6) Mehanizmi certificiranja 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 pripomoči k njeni dosledni uporabi.

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

(8) Certifikati bi zato morali 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 certificiranja, 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 certifikati prostovoljna orodja, ki zagotavljajo odgovornost, ter da upoštevanje mehanizma certificiranja 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 osredotočeno na merila za certificiranje. 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 Evropski odbor za varstvo podatkov se sprejme v skladu z drugim odstavkom 64. člena Splošne uredbe o varstvu podatkov v povezavi z drugim odstavkom 10. člena poslovnika Evropskega odbora za varstvo podatkov v osmih tednih od prvega delovnega dne po odločitvi predsednice in pristojnega nadzornega organa, da je dokumentacija popolna. Po predsedničini 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:

1. POVZETEK DEJSTEV

1. V skladu s petim odstavkom 42. člena Splošne uredbe o varstvu podatkov in smernic je osnutek „Kataloga meril EuroPrise za certificiranje dejanj obdelave s strani obdelovalcev (področje uporabe: EU) v1.5“ (v nadaljevanju: osnutek meril za certificiranje, merila za certificiranje ali merila) pripravila družba EuroPrise Cert GmbH (v nadaljevanju: lastnik sheme), ki je pravna oseba v Nemčiji, in ga predložila Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, tj. pristojnemu nemškemu nadzornemu organu v Severnem Porenju-Vestfaliji (v nadaljevanju: DE-NRW SA).

2. Nemški federalni nadzorni organ (v nadaljevanju: DE SA) je osnutek meril za certificiranje 29. aprila 2024 predložil v odobritev Evropskemu odboru za varstvo podatkov v skladu z drugim odstavkom 64. člena Splošne uredbe o varstvu podatkov. Sklep o popolnosti dokumentacije je bil sprejet 29. maja 2024.

3. Mehanizem certificiranja EuroPrise ni certificiranje za mednarodne prenose osebnih podatkov iz točke f drugega odstavka 46. člena 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 drugega odstavka 46. člena. 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 za certificiranje za njihovo odobritev na podlagi petega odstavka 42. člena Splošne uredbe o varstvu podatkov v skladu s strukturo iz Priloge 2 k smernicam (v nadaljevanju: priloga) in njihovega dodatka.

2.1 Področje uporabe mehanizma certificiranja in cilj vrednotenja

5. Mehanizem certificiranja EuroPrise vsebuje merila za certificiranje vseevropske sheme certificiranja za certificiranje obdelave s strani obdelovalcev. Predmet certificiranja, za katerega se uporablja katalog meril, so dejanja obdelave, ki se izvajajo v produktih, postopkih in storitvah ali s pomočjo (tudi več) proizvodov in storitev in v zvezi s katerimi vložnik zahtevka za certificiranje deluje kot obdelovalec. Glavna merila tega mehanizma certificiranja so razdeljena v tri sklope zahtev, in sicer: s pravnega vidika (sklop 1), z vidika tehničnih in organizacijskih ukrepov (sklop 2) ter z vidika pravic posameznikov, na katere se nanašajo osebni podatki (sklop 3).

6. Vložniki zahtevka za certificiranje v okviru te sheme morajo biti obdelovalci. To vključuje obdelovalce, ki jim upravljavec neposredno zaupa obdelavo osebnih podatkov v smislu sedmega odstavka 4. člena Splošne uredbe o varstvu podatkov. Vendar so lahko vložniki zahtevka za certificiranje tudi obdelovalci v smislu drugega in četrtega odstavka 28. člena Splošne uredbe o varstvu podatkov (podobdelovalci).

7. Kadar obdelovalec – certificiran v okviru sheme certificiranja EuroPrise – uporablja podobdelovalca, slednji ne more trditi, da je bil certificiran v okviru sheme certificiranja EuroPrise. Certificiranje v takem primeru zajema samo dejanja obdelave, ki jih izvaja prvotni in certificirani obdelovalec. Vendar lahko zahtevek za certificiranje vložijo tudi podobdelovalci, kar bi pomenilo samostojen in neodvisen postopek.

8. Odbor v dokumentaciji v zvezi s področjem uporabe mehanizma certificiranja, ki jo je zagotovil nemški nadzorni organ, ugotavlja, da se shema EuroPrise uporablja za obdelovalce s sedežem v Evropski uniji (EU) ali v Evropskem gospodarskem prostoru (EGP).

2.2 Dejanja obdelave

9. Področje uporabe teh meril ni omejeno na konkretne vrste dejanj obdelave. Gre bolj za metodologijo, na kateri temelji vrednotenje sheme EuroPrise, ki omogoča certificiranje vseh dejanj obdelave, ki jih izvajajo obdelovalci. Gre torej za univerzalen metodološki pristop, na podlagi katerega je mogoče

certificirati veliko zelo različnih dejanj obdelave. Zato je bistveno, da se upoštevajo metodološke zahteve, saj je to edini način za zagotovitev enotne uporabe meril za certificiranje in primerljive ravni preizkušanja v različnih postopkih certificiranja. Cilj je zagotoviti primerljivost in ponovljivost izdanih certifikatov in njihovih rezultatov.

2.3 Zakonitost in načela obdelave podatkov

10. Merila zahtevajo preverjanje, ali so dejanja obdelave, ki jih je treba certificirati, skladna z načeli vgrajenega in privzetega varstva podatkov (oddelek 1.5 meril), kar vključuje sodelovanje vložnika zahtevka pri pomoči upravljavcu pri izvajanju teh načel. To omogoča oceno skladnosti s 25. členom Splošne uredbe o varstvu podatkov v povezavi z njenim 5. členom. Čeprav ni meril, ki bi bila neposredno usmerjena v skladnost s 6. členom Splošne uredbe o varstvu podatkov – glede na to, da je za zakonitost obdelave odgovoren upravljavec –, je cilj meril zagotoviti, da obdelovalci – vložniki vlog načrtujejo dejanja obdelave, ki jih je treba certificirati, na način, ki upravljavcem olajša izvajanje načel varstva podatkov iz 5. člena Splošne uredbe o varstvu podatkov, vključno z načelom zakonitosti obdelave.

2.4 Splošne obveznosti upravljavcev in obdelovalcev

11. Merila odražajo razmerje med obdelovalcem in upravljavcem. Merila zlasti določajo obveznost obdelovalca, da ima z upravljavcem vzpostavljeno predlogo pogodbe o obdelavi podatkov, ki vključuje vse zahteve iz 28. člena Splošne uredbe o varstvu podatkov (oddelek 1.2 meril).

12. V skladu z merili morajo vložniki zahtevka imenovati pooblaščeno osebo za varstvo podatkov v skladu s 37. členom Splošne uredbe o varstvu podatkov in predložiti dokazilo o njenem imenovanju (na primer certifikat o imenovanju). Z merili se preverja, ali pooblaščena oseba za varstvo podatkov izpolnjuje zahteve iz 37. do 39. člena (sklop 1, oddelek 1.1 meril).

13. Z merili se preverja vsebina evidenc dejanj obdelave v skladu s 30. členom Splošne uredbe o varstvu podatkov (sklop 1, oddelek 1.1 meril).

2.5 Pravice posameznikov, na katere se nanašajo osebni podatki

14. Z merili se ustrezno obravnava pravica posameznika, na katerega se nanašajo osebni podatki, do obveščenosti v skladu s poglavjem III Splošne uredbe o varstvu podatkov in zahteva uvedba 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 (sklop 3 meril).

2.6 Tveganja za pravice in svoboščine

15. V skladu z merili se mora obdelovalec zavedati možnih tveganj za pravice in svoboščine posameznikov pri obdelavi podatkov, ki je vključena v cilj vrednotenja. Če je verjetno, da bo obdelava osebnih podatkov povzročila veliko tveganje za pravice in svoboščine posameznikov, več meril zagotavlja, da vložnik zahtevka dokaže, da so zahteve iz 35. člena Splošne uredbe o varstvu podatkov izpolnjene v skladu s tem istim členom (oddelek 1.2.2 meril, zahteva št. 6, oddelek 1.3.2 meril, oddelek 1.3.3 meril, oddelek 2.1.5.1 meril, oddelek 2.1.5.9 meril).

2.7 Tehnični in organizacijski ukrepi, ki jamčijo varstvo podatkov

16. 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 tehnične ukrepe uporabljati tudi za

izvajanje vgrajenega in privzetega varstva podatkov v skladu s 25. in 32. členom Splošne uredbe o varstvu podatkov (oddelek 1.5 meril, oddelek 2.1 meril/drugi dokumenti).

17. 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 33. členom Splošne uredbe o varstvu podatkov (oddelek 1.2.2 meril, zahteva št. 6).

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

18. V skladu z merili je treba opredeliti vse prenose osebnih podatkov v tretje države in mednarodne organizacije, vključene v cilj vrednotenja, in utemeljiti izbire mehanizma prenosa podatkov, ki zagotavlja ustrezne zaščitne ukrepe, v skladu s poglavjem V Splošne uredbe o varstvu podatkov (oddelek 1.4. meril).

3. DODATNA MERILA ZA EVROPSKI PEČAT ZA VARSTVO PODATKOV

19. V skladu s smernicami ocena vključuje vprašanje, „ali merila lahko upoštevajo zakonodajo ali scenarije držav članic na področju varstva podatkov“. Skladno z oddelkom 4 meril mora vložnik zahtevka ravnati v skladu z veljavno nacionalno zakonodajo in ustrezno zakonodajo o varstvu podatkov, ki je značilna za sektor. Poleg tega odbor razume, da „poročilo o skladnosti z nacionalno zakonodajo“, v katerem se oceni zlasti skladnost cilja vrednotenja z veljavnimi zahtevami nacionalne zakonodaje o varstvu podatkov, pripravijo pravni strokovnjaki, če dokažejo potrebno raven strokovnega znanja na področju veljavne nacionalne zakonodaje.

SKLEPNE UGOTOVITVE/PRIPOROČILA

20. Glede na navedeno Evropski odbor za varstvo podatkov meni, da je osnutek meril za certificiranje skladen s Splošno uredbo o varstvu podatkov, in jih odobri v skladu z nalogo odbora iz točke o prvega odstavka 70. člena navedene uredbe, pri čemer je rezultat skupno certificiranje (evropski pečat za varstvo podatkov).

21. Evropski odbor za varstvo podatkov bo v skladu z osmim odstavkom 42. člena v javnem registru mehanizmov certificiranja ter pečatov in označb za varstvo podatkov evidentiral mehanizem certificiranja „Katalog meril EuroPrise za certificiranje dejanj obdelave s strani obdelovalcev“.

KONČNE OPOMBE

22. To mnenje je namenjeno nemškemu nadzornemu organu v Severnem Porenju-Vestfaliji in bo v skladu s točko b petega odstavka 64. člena Splošne uredbe o varstvu podatkov na voljo javnosti.

Za Evropski odbor za varstvo podatkov

Predsednica
Anu Talus