Smernice

Smernice 07/2022 o certificiranju kot orodju za prenose

Različica 2.0

Sprejete 14. februarja 2023

ZGODOVINA RAZLIČIC

Različica 1.0	14. junij 2022	Sprejetje smernic za javno posvetovanje
Različica 2.0	14. februar 2023	Sprejetje smernic po javnem posvetovanju

POVZETEK

Splošna uredba o varstvu podatkov v 46. členu določa, da izvozniki podatkov uvedejo ustrezne zaščitne ukrepe za prenose osebnih podatkov v tretje države ali mednarodne organizacije. Splošna uredba o varstvu podatkov zato določa različne ustrezne zaščitne ukrepe, ki jih lahko izvozniki podatkov v skladu s 46. členom uporabijo za določitev okvira za prenose v tretje države, in med drugim uvaja certificiranje kot nov mehanizem za prenose (člena 42(2) in 46(2)(f) Splošne uredbe o varstvu podatkov).

Te smernice vsebujejo navodila za uporabo člena 46(2)(f) Splošne uredbe o varstvu podatkov o prenosih osebnih podatkov v tretje države ali mednarodne organizacije na podlagi certificiranja. Dokument je sestavljen iz štirih oddelkov s Prilogo.

V prvem delu tega dokumenta („SPLOŠNO“) je pojasnjeno, da smernice dopolnjujejo že obstoječe splošne Smernice št. 1/2018 o certificiranju in obravnavajo posebne zahteve iz poglavja V Splošne uredbe o varstvu podatkov, kadar se certificiranje uporablja kot orodje za prenose. V skladu s 44. členom Splošne uredbe o varstvu podatkov mora vsak prenos osebnih podatkov v tretje države ali mednarodne organizacije poleg skladnosti s poglavjem V Splošne uredbe o varstvu podatkov izpolnjevati pogoje drugih določb Splošne uredbe o varstvu podatkov. Zato je v prvem koraku treba zagotoviti skladnost s splošnimi določbami Splošne uredbe o varstvu podatkov, v drugem koraku pa upoštevati določbe poglavja V Splošne uredbe o varstvu podatkov. Opisani so vključeni akterji in njihove osrednje vloge v tem okviru, s posebnim poudarkom na vlogi uvoznika podatkov, ki mu bo izdan certifikat, in izvoznika podatkov, ki ga bo uporabil kot orodje za določitev okvira svojih prenosov (ob upoštevanju, da je za skladnost obdelave podatkov še vedno odgovoren izvoznik podatkov). V zvezi s tem lahko certificiranje vključuje tudi ukrepe, ki dopolnjujejo orodja za prenose, za zagotovitev skladnosti z varstvom osebnih podatkov na ravni EU. Prvi del smernic vsebuje tudi informacije o postopku za pridobitev certifikata, ki se bo uporabljal kot orodje za prenose.

V drugem delu teh smernic („SMERNICE ZA IZVAJANJE ZAHTEV ZA AKREDITACIJO“) je vnovič opozorjeno, da so zahteve za akreditacijo telesa za certificiranje navedene v standardu ISO 17065 in razložene s Smernicami 4/2018 o akreditaciji teles za certificiranje na podlagi 43. člena Splošne uredbe o varstvu podatkov ter njihovo prilogo glede na poglavje V. Vendar so glede prenosa v teh smernicah dodatno pojasnjene nekatere zahteve za akreditacijo, ki veljajo za telo za certificiranje.

V tretjem delu teh smernic („POSEBNA MERILA ZA CERTIFICIRANJE“) so zagotovljena navodila za merila za certificiranje, ki so že navedena v Smernicah št. 1/2018, in določena dodatna posebna merila, ki bi jih bilo treba vključiti v mehanizem certificiranja, ki se bo uporabljal kot orodje za prenose v tretje države. Ta merila zajemajo oceno zakonodaje tretje države, splošne obveznosti izvoznikov in uvoznikov, pravila o nadaljnjih prenosih, pravnem varstvu in izvrševanju, postopek ter ukrepe za primere, v katerih nacionalna zakonodaja in prakse preprečujejo izpolnjevanje zavez, sprejetih na podlagi certifikata, in zahteve organov tretjih držav za dostop do podatkov.

Četrti del teh smernic („ZAVEZUJOČE IN IZVRŠLJIVE ZAVEZE, KI JIH JE TREBA IZVAJATI“) vsebuje elemente, ki bi morali biti obravnavani v zavezujočih in izvršljivih zavezah, ki bi jih morali sprejeti upravljavci ali obdelovalci, za katere se Splošna uredba o varstvu podatkov ne uporablja, za zagotavljanje ustreznih zaščitnih ukrepov za podatke, ki se prenašajo v tretje države. Te zaveze, ki so lahko določene v različnih instrumentih, tudi v pogodbah, vključujejo zlasti jamstvo, da uvoznik nima razloga za domnevo, da mu zakoni in prakse v tretji državi, ki se uporabljajo za zadevno obdelavo, vključno z morebitnimi zahtevami za razkritje osebnih podatkov ali ukrepi, ki dovoljujejo dostop javnim organom, preprečujejo izpolnjevanje zavez na podlagi certifikata.

V PRILOGI k tem smernicam je nekaj primerov dopolnilnih ukrepov v skladu s primeri iz Priloge II k Priporočilom 01/2020 (Priporočila 01/2020 o ukrepih, ki dopolnjujejo orodja za prenos, za zagotovitev skladnosti z ravnjo varstva osebnih podatkov na ravni EU) v okviru uporabe certificiranja kot orodja za prenos. Primeri so pripravljeni zato, da bi se opozorilo na kritične primere.

KAZALO

Evropski odbor za varstvo podatkov je –

ob upoštevanju člena 70(1)(e) 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 EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu, kakor sta bila spremenjena s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018[1],

ob upoštevanju členov 12 in 22 svojega poslovnika –

SPREJEL NASLEDNJE SMERNICE

1 SPLOŠNO

1.1 Namen in področje uporabe

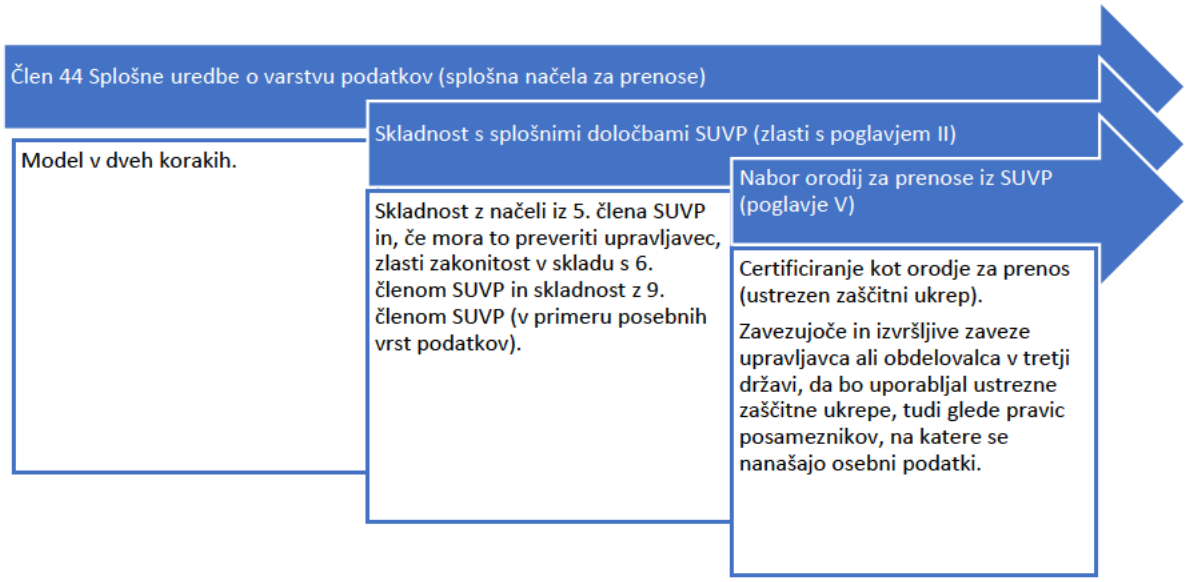
1. Namen tega dokumenta je zagotoviti smernice za uporabo člena 46(2)(f) Splošne uredbe o varstvu podatkov za prenose osebnih podatkov v tretje države ali mednarodne organizacije na podlagi certificiranja. Evropski odbor za varstvo podatkov je že objavil splošne smernice o certificiranju[2] in akreditaciji[3] na podlagi Splošne uredbe o varstvu podatkov. V teh novih smernicah so torej izraženi zgolj posebni vidiki v zvezi s certificiranjem kot orodjem za prenose. V njih je s praktičnimi navodili v zvezi s tem in z vključitvijo novih elementov v že objavljene smernice podrobneje pojasnjena uporaba členov 46(2)(f) in 42(2) Splošne uredbe o varstvu podatkov.

2. Evropski odbor za varstvo podatkov bo ocenil delovanje teh smernic glede na izkušnje, pridobljene med njihovim izvajanjem v praksi, in zagotovil dodatna navodila za pojasnitev uporabe elementov, navedenih v nadaljevanju, vključno z vlogo sporazuma o certificiranju v zvezi z zavezujočimi in izvršljivimi zavezami iz člena 46(2)(f) Splošne uredbe o varstvu podatkov.

1.2 Splošna pravila, ki se uporabljajo za mednarodne prenose

3. V skladu s 44. členom Splošne uredbe o varstvu podatkov mora vsak prenos osebnih podatkov v tretje države[4] ali mednarodne organizacije poleg skladnosti s poglavjem V Splošne uredbe o varstvu podatkov izpolnjevati pogoje drugih določb Splošne uredbe o varstvu podatkov. Zato mora biti vsak prenos med drugim skladen z načeli varstva podatkov iz 5. člena Splošne uredbe o varstvu podatkov, biti zakonit v skladu s 6. členom Splošne uredbe o varstvu podatkov in v primeru posebnih vrst podatkov skladen z 9. členom Splošne uredbe o varstvu podatkov. Zato je treba uporabiti preskus v dveh korakih. V prvem koraku je treba zagotoviti skladnost s splošnimi določbami Splošne uredbe o varstvu podatkov, v drugem koraku pa upoštevati določbe poglavja V Splošne uredbe o varstvu podatkov.

[1] Sklicevanja na „države članice“ v tem dokumentu je treba razumeti kot sklicevanja na „države članice EGP“.
[2] Smernice št. 1/2018 o certificiranju in opredelitvi meril za certificiranje v skladu s členoma 42 in 43 Uredbe [(EU) 2016/679].
[3] Smernice 4/2018 o akreditaciji teles za certificiranje na podlagi 43. člena Splošne uredbe o varstvu podatkov (2016/679).
[4] Smernice 05/2021 o medsebojnem vplivu uporabe člena 3 in določb o mednarodnih prenosih v skladu s poglavjem V Splošne uredbe o varstvu podatkov, stran 4.



4. Splošna uredba o varstvu podatkov v 46. členu določa, da „kadar sklep v skladu s členom 45(3) ni sprejet, lahko upravljavec ali obdelovalec osebne podatke prenese v tretjo državo ali mednarodno organizacijo le, če je upravljavec ali obdelovalec predvidel ustrezne zaščitne ukrepe, in pod pogojem, da imajo posamezniki, na katere se nanašajo osebni podatki, na voljo izvršljive pravice in učinkovita pravna sredstva“. V skladu s členom 46(2)(f) Splošne uredbe o varstvu podatkov se lahko taki ustrezni zaščitni ukrepi zagotovijo z odobrenim mehanizmom certificiranja skupaj z zavezujočimi in izvršljivimi zavezami upravljavca ali obdelovalca v tretji državi, da bo uporabljal ustrezne zaščitne ukrepe, tudi glede pravic posameznikov, na katere se nanašajo osebni podatki.

5. Posledično se lahko izvoznik podatkov odloči, da se bo oprl na certifikat, ki ga je pridobil uvoznik podatkov, kot element za izkazovanje izpolnjevanja obveznosti, na primer v skladu s členom 24(3) ali 28(5) Splošne uredbe o varstvu podatkov. Uvoznik podatkov se lahko odloči zaprositi za certifikat, da dokaže, da so vzpostavljeni ustrezni zaščitni ukrepi.

6. Izvoznik in uvoznik podatkov imata lahko glede na obdelavo iz poglavja V različne vloge (na primer kot upravljavec ali obdelovalec)[5], ki prinašajo različne odgovornosti:

7. Splošna uredba o varstvu podatkov v 49. členu določa, da se lahko poleg uporabe certificiranja ali katerega koli drugega orodja ali mehanizma za prenose iz členov 45 in 46 v omejenem številu posebnih primerov izvedejo mednarodni prenosi podatkov, kadar ni upoštevan noben drug mehanizem iz poglavja V[6]. Vendar, kot je pojasnjeno v prejšnjih smernicah, ki jih je izdal Evropski odbor za varstvo

[5] Glej spodaj: SMERNICE ZA IZVAJANJE MERIL ZA CERTIFICIRANJE.
[6] Za več informacij o členu 49 in njegovem medsebojnem vplivu s členom 46 na splošno glej Smernice št. 2/2018 o odstopanjih iz člena 49 v skladu z Uredbo (EU) 2016/679.

podatkov, je treba odstopanja iz 49. člena Splošne uredbe o varstvu podatkov razlagati restriktivno in se v glavnem nanašajo na dejavnosti obdelave, ki so občasne in neponavljajoče[7].

1.3 Kdo so vključeni akterji in kakšna je njihova vloga pri certificiranju kot orodju za prenose?

8. **Evropski odbor za varstvo podatkov** je pooblaščen za odobritev meril za certificiranje na ravni EGP (evropski pečat za varstvo podatkov) ter za podajanje mnenj o osnutkih sklepov nadzornih organov o merilih za certificiranje in zahtevah za akreditacijo teles za certificiranje, da se zagotovi doslednost. Pristojen je tudi za zbiranje vseh mehanizmov certificiranja ter pečatov in označb za varstvo podatkov v registru in njihovo javno objavo[8].

9. **Nadzorni organi** odobrijo merila za certificiranje, kadar mehanizem certificiranja ni evropski pečat za varstvo podatkov[9]. Lahko tudi akreditirajo telo za certificiranje, oblikujejo merila za certificiranje in izdajo certifikat, če tako določa nacionalna zakonodaja njihove države članice[10].

10. **Nacionalni akreditacijski organ** lahko akreditira tretja telesa za certificiranje, tako da uporabi standard ISO 17065 in dodatne zahteve nadzornih organov za akreditacijo, ki morajo biti v skladu z oddelkom 2 teh smernic. V nekaterih državah članicah lahko akreditacijo izda pristojni nadzorni organ ali nacionalni akreditacijski organ ali jo izdata oba.

11. **Lastnik sheme** je organizacija, ki je določila merila in metodološke zahteve za certificiranje, na podlagi katerih se ugotavlja skladnost. Organizacija, ki izvaja ocenjevanja, bi lahko bila organizacija, ki je razvila shemo in je njena lastnica, lahko pa bi bile sprejete ureditve, po katerih je ena organizacija lastnica sheme, druga (ali več drugih) pa izvaja ocenjevanje kot telo za certificiranje.

12. Glede na nacionalno zakonodajo lahko certifikate namesto nadzornega organa izdaja **telo za certificiranje**, akreditirano, kot je navedeno zgoraj[11]. Oblikuje lahko merila za certificiranje in je tako lastnik sheme (glej odstavek 11 zgoraj). Sedež mora imeti v EGP, zlasti zato, da omogoči učinkovito izvajanje popravljalnih pooblastil, opredeljenih v členu 58(2)(f) Splošne uredbe o varstvu podatkov. Vendar lahko telo za certificiranje dejavnosti odda v podizvajanje lokalnim strokovnjakom ali ustanovitvam zunaj EGP, ki bodo izvajali revizijske dejavnosti v njegovem imenu[12]. Kljub temu telo za certificiranje odločitve o tem, ali se certifikat izda ali ne, ne prepusti podizvajalcu.

13. **Uvoznik podatkov** je subjekt (upravljavec ali obdelovalec) v tretji državi, ki prejema podatke od izvoznika podatkov.

14. **Izvoznik podatkov** je subjekt (upravljavec ali obdelovalec), ki prenaša podatke iz EGP do uvoznika podatkov. Izvoznik podatkov mora zagotoviti skladnost s poglavjem V.

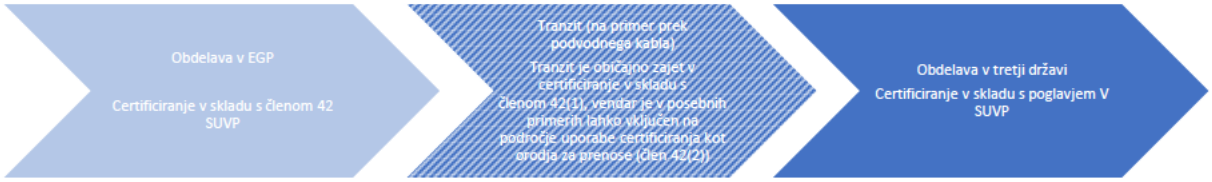
1.4 Kakšna sta področje uporabe in predmet certificiranja kot orodja za prenose?

15. Cilj mehanizma certificiranja kot orodja za prenose v skladu s členom 42(2) mora biti zagotavljanje ustreznih zaščitnih ukrepov za obdelavo osebnih podatkov v skladu s pogoji iz točke (f) člena 46(2).

[7] Smernice št. 2/2018 o odstopanjih iz člena 49 v skladu z Uredbo (EU) 2016/679, stran 5.
[8] Člen 42(8) Splošne uredbe o varstvu podatkov.
[9] Smernice št. 1/2018 o certificiranju in opredelitvi meril za certificiranje v skladu s členoma 42 in 43 Uredbe, točka 2.2.
[10] Člena 42(5) in 43(1) Splošne uredbe o varstvu podatkov.
[11] Člen 42(5) Splošne uredbe o varstvu podatkov.
[12] Telesa za certificiranje morajo svoje lokalne strokovnjake oceniti v skladu s standardom ISO 17065 in dodatnimi zahtevami za akreditacijo, ki jih določi nadzorni organ (člen 43(1)(b) Splošne uredbe o varstvu podatkov).

Certifikat dokazuje, da obstajajo ustrezni zaščitni ukrepi, ki so jih zagotovili upravljavci ali obdelovalci, ki so zunaj EGP ali del mednarodne organizacije, ki prejema podatke od upravljavcev ali obdelovalcev iz EGP, za odpravljanje posebnih tveganj pri prenosu osebnih podatkov.

16. Na splošno je dejanje prenosa osebnih podatkov iz države članice v tretjo državo samo po sebi obdelava osebnih podatkov v smislu člena 4(2) Splošne uredbe o varstvu podatkov, ki se izvaja v državi članici[13], in ga je zato mogoče certificirati v skladu s členom 42(1) Splošne uredbe o varstvu podatkov. Vendar je lahko v nekaterih primerih, glede na okoliščine, na področje uporabe certificiranja kot orodja za prenose vključen tranzit. Zato bi morala biti predmet certificiranja – ki se med certificiranjem ujema s ciljem vrednotenja (*Target of Evaluation* – ToE) [14] – na splošno obdelava podatkov, ki jih uvoznik podatkov v tretji državi prejme iz EGP, in tranzit, če ga upravlja uvoznik.



17. Predmet certificiranja je lahko posamezno dejanje obdelave ali sklop dejanj. Ta lahko vključujejo postopke upravljanja v smislu organizacijskih ukrepov, torej kot sestavni deli dejanja obdelave[15].

18. Subjekt, ki vloži zahtevek, bi bil v zvezi s predmetom certificiranja torej uvoznik v tretji državi.

1.5 Kakšna bi morala biti vloga izvoznika pri uporabi certificiranja kot orodja za prenose?

19. Prenos, ki ga opravi izvoznik podatkov, kot tak na splošno spada neposredno na področje uporabe Splošne uredbe o varstvu podatkov. To pomeni, da mora izvoznik izpolnjevati svoje obveznosti na podlagi Splošne uredbe o varstvu podatkov in zlasti zagotoviti, da se podatki prenašajo varno v skladu z 32. členom in poglavjem V za zagotovitev, da ni ogrožena raven varstva posameznikov, ki jo zagotavlja navedena uredba (44. člen Splošne uredbe o varstvu podatkov)[16]. To se seveda lahko certificira v skladu s členom 42(1).

20. Poleg tega je izvoznik podatkov, ki želi uporabiti certificiranje kot ustrezni zaščitni ukrep v skladu s členom 46(2)(f) Splošne uredbe o varstvu podatkov, zlasti obvezan preveriti, ali je certificiranje, na katero se namerava opreti, učinkovito glede na značilnosti predvidene obdelave. V ta namen mora izvoznik podatkov preveriti, ali je izdani certifikat veljaven in ni potekel, ali zajema poseben prenos, ki

[13] Sodba Sodišča Evropske unije v zadevi C-311/18, *Data Protection Commissioner/Facebook Ireland Ltd in Maximillian Schrems*, točka 83.

[14] Smernice št. 1/2018 o certificiranju in opredelitvi meril za certificiranje v skladu s členoma 42 in 43 Uredbe, stran 17.

[15] Smernice št. 1/2018 o certificiranju in opredelitvi meril za certificiranje v skladu s členoma 42 in 43 Uredbe, stran 16 (na primer mehanizem za obravnavo pritožb).

[16] Glede tega je treba opozoriti, da je v 44. členu Splošne uredbe o varstvu podatkov jasno predvideno, da lahko prenos izvaja tudi obdelovalec in ne le upravljavec. Prenos se bo torej zgodil, kadar obdelovalec pošlje podatke drugemu obdelovalcu ali celo upravljavcu v tretji državi po navodilih svojega upravljavca (člen 28(3)(a) Splošne uredbe o varstvu podatkov). V takih primerih obdelovalec deluje kot izvoznik podatkov v imenu upravljavca in mora zagotoviti, da so za zadevni prenos po navodilih upravljavca upoštevane določbe poglavja V, vključno z uporabo ustreznega orodja za prenose. Glede na to, da je prenos dejavnost obdelave, ki se izvaja v imenu upravljavca, je tudi upravljavec odgovoren in bi lahko odgovarjal v skladu s poglavjem V ter mora tudi zagotoviti, da obdelovalec zagotovi zadostna jamstva v skladu z 28. členom.

se bo izvedel, in ali tranzit osebnih podatkov spada na področje uporabe certifikata ter ali so vključeni nadaljnji prenosi in zagotovljena ustrezna dokumentacija o njih. Izvoznik mora tudi preveriti, ali je telo za certificiranje, ki je izdalo certifikat, akreditiral nacionalni akreditacijski organ ali pristojni nadzorni organ. Poleg tega bi se moral izvoznik podatkov sklicevati na uporabo certificiranja kot orodja za prenos v pogodbi o obdelavi podatkov v skladu z 28. členom Splošne uredbe o varstvu podatkov v primeru prenosov od upravljavca k obdelovalcu ali v pogodbi o izmenjavi podatkov z uvoznikom podatkov v primeru prenosov od upravljavca k upravljavcu.

21. Glede na to, da je izvoznik odgovoren za uporabo vseh določb iz poglavja V, mora tudi oceniti, ali je certificiranje, na katero se namerava opreti kot na orodje za prenose, učinkovito glede na veljavno zakonodajo in prakse v tretji državi, ki so pomembne za zadevni prenos. Za namen te ocene in kot pomemben element za dokazovanje, da izvoznik podatkov izpolnjuje svojo odgovornost, se lahko izvoznik podatkov opre na preverjanje uvoznikove dokumentirane ocene zakonodaje in praks tretje države, ki ga je opravilo telo za certificiranje.

22. Če je uvoznikova ocena pokazala, da morata uvoznik in/ali izvoznik podatkov morda zagotoviti dopolnilne ukrepe, predvidene s certificiranjem, za zagotovitev v bistvu enakovredne ravni zaščite, kot je zagotovljena v EGP, mora izvoznik podatkov preveriti dopolnilne ukrepe, ki jih zagotavlja uvoznik podatkov s certifikatom, in ali je sposoben izpolniti obveznosti iz tehničnih in (če obstajajo) dopolnilnih ukrepov, ki jih zahteva uvoznik podatkov.

23. Če navedena določila niso izpolnjena, bo moral izvoznik podatkov od uvoznika zahtevati, da uvede prilagojene dopolnilne ukrepe, ali jih sprejeti sam.

1.6 Kakšen je postopek za certificiranje kot orodje za prenose?

24. Certificiranje je prostovoljno, vendar mora biti, kadar se zahteva, odobreno s preglednim postopkom, ki temelji na obveznih pravilih. Splošna uredba o varstvu podatkov precej zaupa zasebnim mehanizmom certificiranja kot „regulirani samoregulaciji“. V skladu s tem morajo navedeni mehanizmi zagotavljati, da certifikati dejansko izpolnjujejo zahteve za ustrezne zaščitne ukrepe, kot so opredeljeni v 46. členu Splošne uredbe o varstvu podatkov.

25. Zato mora certificiranje temeljiti na oceni meril za certificiranje v skladu z zavezujočo revizijsko metodologijo. Navedena merila bodo odobrili nacionalni nadzorni organi ali Evropski odbor za varstvo podatkov, kot je opisano v členu 42(5) Splošne uredbe o varstvu podatkov. Merila za certificiranje vključujejo zahteve za oceno obdelave, ki jo izvede uvoznik podatkov, vključno z nadaljnjimi prenosi, in ustreznega pravnega okvira tretje države, da bi se izognili temu, da bi pravila in prakse tretje države uvozniku preprečevala izpolnjevanje njegovih obveznosti na podlagi certifikata.

26. Telo za certificiranje, ki ga je akreditiral nacionalni akreditacijski organ ali pristojni nadzorni organ, med postopkom certificiranja v skladu z merili za certificiranje preveri cilj vrednotenja[17].

27. V skladu s členom 43(1) Splošne uredbe o varstvu podatkov certifikat izda in podaljša telo za certificiranje, ki ima ustrezno raven strokovnega znanja v zvezi z varstvom podatkov, in sicer potem, ko obvesti nadzorni organ, da se mu po potrebi dovoli izvajanje pooblastil v skladu s točko (h) člena 58(2) Splošne uredbe o varstvu podatkov.

28. V skladu s členom 43(5) Splošne uredbe o varstvu podatkov telesa za certificiranje pristojnim nadzornim organom utemeljijo dodelitev ali preklic zahtevanega certifikata. To ne pomeni, da telo za

[17] Smernice 4/2018 o akreditaciji teles za certificiranje na podlagi 43. člena Splošne uredbe o varstvu podatkov (2016/679), str. 9.

certificiranje potrebuje dovoljenje nadzornega organa za izdajo certifikata. Telo za certificiranje bo spremljalo, ali njegove stranke izpolnjujejo merila za certificiranje.

29. Nadzorni organ ima popravljalno pooblastilo, da prekliče certifikat ali telesu za certificiranje odredi preklic certifikata, izdanega v skladu s členoma 42 in 43 Splošne uredbe o varstvu podatkov, ali da telesu za certificiranje odredi, naj ne izda certifikata, kadar zahteve v zvezi s certifikatom niso ali niso več izpolnjene.

30. Evropski pečat za varstvo podatkov za mednarodne prenose podatkov se lahko uporablja kot orodje, ki skupaj z zavezujočimi in izvršljivimi zavezami zajema prenose v tretje države[18].

31. Kljub temu se lahko certifikati, ki se bodo uporabljali kot orodje za prenose, izdajo tudi v skladu z nacionalnimi odobrenimi shemami certificiranja v državah EGP. Kot taki veljajo le za prenose v tretje države od izvoznikov v državi članici EGP, kjer je bila shema certificiranja odobrena, saj se certifikati različnih držav EGP ne priznavajo vzajemno. Vendar lahko nadzorni organi v različnih državah EGP svobodno odobrijo isti mehanizem certificiranja za prenose[19].

2 SMERNICE ZA IZVAJANJE ZAHTEV ZA AKREDITACIJO

32. Zahteve za akreditacijo telesa za certificiranje v zvezi s certificiranji kot orodji za prenose so navedene v standardu ISO 17065 in razložene s Smernicami 4/2018[20] glede na poglavje V, kot je pojasnjeno v nadaljevanju.

33. Po mnenju Evropskega odbora za varstvo podatkov dodatne zahteve za akreditacijo, pripravljene na podlagi Smernic 4/2018 in standarda ISO 17065 ter sprejete v skladu s členom 64(1)(c) Splošne uredbe o varstvu podatkov, že zajemajo posebne zahteve, potrebne za akreditacijo telesa za certificiranje v zvezi s certificiranji kot orodjem za prenose. Vendar pa je treba v primeru prenosa nekatere zahteve nekoliko izboljšati s pojasnjevalnimi opombami in razlago.

34. V zvezi z zahtevami glede virov (glej zahtevo 6 iz Priloge 1 k Smernicam 4/2018) telo za certificiranje zagotovi, da ima potrebne vire, da lahko preveri, kot to zahtevajo merila za certificiranje, ali je uvoznik ustrezno in pravilno izvedel potrebno oceno pravnega položaja in praks tretjih držav, kjer ima sedež ali deluje[21]. To oceno je treba izvesti v zvezi z dejavnostmi obdelave, ki jih je treba certificirati kot del cilja vrednotenja glede na ustrezne zaščitne ukrepe iz 46. člena Splošne uredbe o varstvu podatkov, in vključuje dopolnilne ukrepe, ki jih je po potrebi opredelil ter jih izvaja uvoznik. To vključuje tudi na primer dobro poznavanje zadevnih lokalnih zakonov in praks ter ustrezno znanje jezikov tretjih držav.

35. V zvezi z zahtevami glede postopka (glej zahtevo 7 iz Priloge 1 k Smernicam 4/2018) telo za certificiranje zagotovi, da se lahko postopek certificiranja podpre z morebitnimi revizijami na kraju

[18] Glej člen 42(5) Splošne uredbe o varstvu podatkov in odstavek 35 Smernic Evropskega odbora za varstvo podatkov št. 1/2018 o certificiranju in opredelitvi meril za certificiranje v skladu s členoma 42 in 43 Uredbe.

[19] Če nadzorni organ v okviru svoje nacionalne pobude sprejme merila za certificiranje X, nato pa želijo druge države ob upoštevanju meril sheme in veljavnih posebnih nacionalnih predpisov sprejeti enaka merila za certificiranje, jih lahko sprejmejo, ne da bi bilo potrebno mnenje Evropskega odbora za varstvo podatkov v skladu s 64. členom Splošne uredbe o varstvu podatkov, in se oprejo na mnenje, izdano za prvi nadzorni organ, v skladu s členom 64(3) Splošne uredbe o varstvu podatkov (v zvezi s tem glej Sklicevanje na smernice – Dodatek (Priloga k Smernicam št. 1/2018 o certificiranju in opredelitvi meril za certificiranje v skladu s členoma 42 in 43 Uredbe), odstavek 66).

[20] Smernice 4/2018 o akreditaciji teles za certificiranje na podlagi 43. člena Splošne uredbe o varstvu podatkov (2016/679) in Priloga k smernicam.

[21] Glej odstavek 12 zgoraj.

samem, da se izvaja v zvezi z obdelavo, ki bo potekala v tretjih državah, in da ocena zajema tudi dejansko izvajanje veljavnih zakonov in politik v tretjih državah.

36. V zvezi z zahtevami glede sprememb, ki vplivajo na certificiranje (glej zahtevo 7.10 iz Priloge 1 k Smernicam 4/2018), telo za certificiranje spremlja spremembe zakonodaje in/ali sodne prakse v tretji državi, ki lahko vplivajo na obdelavo, ki spada na področje uporabe cilja vrednotenja.

3 POSEBNA MERILA ZA CERTIFICIRANJE

37. V okviru upoštevanja posebnih meril za certificiranje te smernice temeljijo na Smernicah št. 1/2018 o certificiranju in opredelitvi meril za certificiranje v skladu s členoma 42 in 43 Uredbe (različica 3.0), ustrezni Prilogi 2 o pregledu in ocenjevanju meril za certificiranje v skladu s členom 42(5) in Smernicah o ocenjevanju meril za certificiranje – Dodatek.

38. Evropski odbor za varstvo podatkov meni, da merila za certificiranje, pripravljena na podlagi Priloge 2 k Smernicam št. 1/2018 in Smernic o ocenjevanju meril za certificiranje – Dodatek, že zajemajo večino meril za certificiranje, ki jih je treba upoštevati pri pripravi osnutka sheme certificiranja, ki se bo uporabljala kot orodje za prenose. Vendar bo morda treba podrobneje opredeliti nekatera od teh obstoječih meril, da se prilagodijo posebnemu primeru prenosa (glej odstavek 3.1). Poleg tega bo morda treba oblikovati dodatna merila za namen uporabe ustreznih zaščitnih ukrepov, vključno v zvezi s pravicami posameznikov, na katere se nanašajo osebni podatki (glej odstavek 3.2).

3.1 SMERNICE ZA IZVAJANJE MERIL ZA CERTIFICIRANJE

39. Področje uporabe mehanizma certificiranja in cilja vrednotenja (glej Prilogo 2, oddelek 2.a) bi moralo biti jasno opisano v ustrezni dokumentaciji, tudi glede prenosa osebnih podatkov v tretjo državo ali s tem, ali naj bi zajemalo tudi njihov tranzit.

40. V zvezi s področjem uporabe mehanizma certificiranja in ciljem vrednotenja (glej Prilogo 2, oddelek 2.b) bi moralo biti v ustrezni dokumentaciji konkretno opisano, za katero vrsto subjekta (na primer za upravljavca in/ali obdelovalca) se uporablja mehanizem certificiranja.

41. V zvezi s področjem uporabe mehanizma certificiranja in ciljem vrednotenja (glej Prilogo 2, oddelek 2.f) bi bilo treba z merili zahtevati, da je cilj vrednotenja natančno opredeljen, da se preprečijo nesporazumi. To bi moralo vključevati vsaj:

42. dejanja obdelave, tudi če so predvideni nadaljnji prenosi;

    a) namen;

    b) vrsto subjekta (na primer upravljavec in/ali obdelovalec);

    c) vrsto podatkov, ki se prenašajo, pri čemer se upošteva, ali so vključene posebne vrste osebnih podatkov, opredeljene v 9. členu Splošne uredbe o varstvu podatkov;

    d) kategorije posameznikov, na katere se nanašajo osebni podatki;

    e) države, v katerih poteka obdelava podatkov.

43. V zvezi s preglednostjo in pravicami posameznikov, na katere se nanašajo osebni podatki (glej Prilogo 2, oddelek 8), bi bilo treba z merili za certificiranje:

a) zahtevati, da se informacije o dejavnostih obdelave zagotovijo posameznikom, na katere se nanašajo osebni podatki, tudi, kadar je to ustrezno, o prenosu osebnih podatkov v tretjo državo ali mednarodno organizacijo (glej člene 12, 13 in 14 Splošne uredbe o varstvu podatkov);

b) zahtevati, da so posameznikom, na katere se nanašajo osebni podatki, zagotovljene pravice do dostopa, popravka, izbrisa, omejitve, obveščanja v zvezi s popravkom, izbrisom ali omejitvijo, ugovora zoper obdelavo in pravica, da zanje ne veljajo odločitve, ki temeljijo zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov, ki so v bistvu enakovredne pravicam, določenim v členih 15 do 19 ter 21 in 22 Splošne uredbe o varstvu podatkov;

c) zahtevati, da uvoznik podatkov, ki ima certifikat, vzpostavi ustrezen postopek obravnave pritožb za zagotovitev učinkovitega izvajanja pravic posameznikov, na katere se nanašajo osebni podatki;

d) zahtevati oceno, ali in v kakšnem obsegu so te pravice izvršljive za posameznike, na katere se nanašajo osebni podatki, v zadevni tretji državi, in morebitnih dodatnih ustreznih ukrepov, ki jih bo morda treba uvesti za njihovo izvrševanje, na primer zahteve, da bo uvoznik upošteval pristojnost nadzornega organa, pristojnega za izvoznike, in sodeloval z njim v vseh postopkih za zagotavljanje skladnosti s temi pravicami ter zlasti, da se strinja, da bo odgovarjal na poizvedbe, privolil v izvajanje revizij in spoštoval ukrepe, ki jih je sprejel navedeni nadzorni organ, vključno s popravnimi in izravnalnimi ukrepi.

44. V zvezi s tehničnimi in organizacijskimi ukrepi, ki zagotavljajo varstvo (Priloga 2, oddelek 10.q), bi bilo treba z merili za certificiranje od uvoznika zahtevati, da obvesti izvoznika in, če uvoznik deluje kot upravljavec, obvesti nadzorni organ v EGP, pristojen za izvoznike podatkov, o kršitvah varstva podatkov in jih sporoči posameznikom, na katere se nanašajo osebni podatki, kadar je verjetno, da bo kršitev povzročila veliko tveganje za njihove pravice in svoboščine, v skladu z zahtevami iz 34. člena Splošne uredbe o varstvu podatkov.

3.2 DODATNA POSEBNA MERILA ZA CERTIFICIRANJE

45. Glede na zaščitne ukrepe, opredeljene za druge instrumente za prenose v skladu s 46. členom Splošne uredbe o varstvu podatkov (kot so zavezujoča poslovna pravila ali kodeksi ravnanja), in za zagotovitev skladne ravni varstva ter ob upoštevanju sodbe Sodišča Evropske unije *Schrems II* Evropski odbor za varstvo podatkov meni, da bi moral mehanizem certificiranja, ki se bo uporabljal kot orodje za prenos v tretje države, vključevati tudi spodaj navedena merila.

1. Ocena zakonodaje tretje države

a) Ali merila od uvoznika zahtevajo, da oceni pravila in prakse tretje države, v kateri deluje, in ali uvozniku preprečujejo izpolnjevanje njegovih zavez na podlagi certifikata?

b) Ali merila od uvoznika zahtevajo, da dokumentira oceno pravil in praks tretje države, v kateri deluje, in da dokumentacijo na voljo telesu za certificiranje ter na zahtevo nadzornemu organu v EGP, pristojnemu za izvoznika podatkov, in izvozniku podatkov?

c) Ali merila od uvoznika zahtevajo, da opredeli in izvede organizacijske in tehnične ukrepe za zagotovitev ustreznih zaščitnih ukrepov v skladu s 46. členom Splošne uredbe o varstvu podatkov ob upoštevanju Priporočil 01/2020 o ukrepih, ki dopolnjujejo orodja za prenos, za zagotovitev skladnosti z ravnjo varstva osebnih podatkov na ravni EU?

d) Ali merila zahtevajo, da uvoznik dokumentira organizacijske in tehnične ukrepe, ki se dejansko izvajajo za zagotovitev ustreznih zaščitnih ukrepov v skladu s 46. členom Splošne uredbe o varstvu podatkov, in da dokumentacijo na voljo telesu za certificiranje ter na zahtevo pristojnim organom za varstvo podatkov in izvozniku podatkov?

e) Ali merila od uvoznika zahtevajo, da opredeli in izvede organizacijske in tehnične ukrepe za zagotovitev varnosti osebnih podatkov, ki se prenašajo, ob upoštevanju Priporočil 01/2020 o ukrepih, ki dopolnjujejo orodja za prenos, za zagotovitev skladnosti z ravnjo varstva osebnih podatkov na ravni EU, če je tranzit vključen na področje uporabe certificiranja kot orodja za prenos?
f) Ali merila zahtevajo jamstvo za telo za certificiranje in izvoznika, da uvoznik nima razloga za domnevo, da mu zakonodaja in prakse, ki se uporabljajo zanj, lahko preprečijo izpolnjevanje obveznosti na podlagi certifikata?

2. Splošne obveznosti izvoznikov in uvoznikov

a) Ali merila zahtevajo, da se v pogodbenih dogovorih (na primer v obstoječi pogodbi o storitvah) med izvozniki in uvozniki opiše poseben prenos, za katerega se uporablja certifikat, in da se zadevnim posameznikom, na katere se nanašajo osebni podatki, priznajo pravice upravičenih tretjih oseb?

b) Če merila zahtevajo posebno vsebino za te pogodbene dogovore ali instrumente in je predloga zagotovljena, ali merila zahtevajo, da so tudi ti predmet ocenjevanja?

3. Pravila o nadaljnjih prenosih

a) Ali merila zahtevajo, da so nadaljnji prenosi predmet posebnih zaščitnih ukrepov v skladu z zahtevami iz poglavja V Splošne uredbe o varstvu podatkov, da se zagotovi, da raven varstva, zagotovljena v EGP, ne bo ogrožena, in ali merila zahtevajo, da se ustrezna dokumentacija da na voljo telesu za certificiranje ter nadzornemu organu v EGP, pristojnemu za izvoznike podatkov, in izvozniku podatkov na zahtevo?

4. Pravno varstvo in izvrševanje

a) Ali merila določajo, da lahko posamezniki, na katere se nanašajo osebni podatki, kot upravičene tretje osebe uveljavljajo svoje pravice proti uvozniku podatkov pred sodiščem EGP v kraju običajnega prebivališča posameznika, na katerega se nanašajo osebni podatki, ali pri mednarodni organizaciji, vključno za nadomestilo za škodo, ki jo utrpi posameznik, na katerega se nanašajo osebni podatki, če uvoznik ne upošteva ustrezne sheme certificiranja?
b) Ali merila omogočajo ustrezno ocenjevanje, ali je uvoznik v EGP v primeru neupoštevanja ustrezne sheme certificiranja odgovoren za škodo, ki jo utrpi posameznik, na katerega se nanašajo osebni podatki?
c) Ali merila zahtevajo, da lahko posamezniki, na katere se nanašajo osebni podatki, vložijo pritožbo zoper uvoznika pri nadzornem organu v EGP, zlasti v državi EGP, v kateri imajo običajno prebivališče, v kateri je njihov kraj dela ali v državi, ki je pristojna za izvoznike podatkov?
d) Ali merila zahtevajo, da bo uvoznik sodeloval z nadzornim organom v EGP, pristojnim za izvoznike podatkov, se strinjal, da se pri njem opravijo revizije in pregledi, ter upošteval njegove nasvete in spoštoval njegove odločitve?

5. Postopek in ukrepi za primere, v katerih nacionalna zakonodaja preprečuje izpolnjevanje zavez, sprejetih na podlagi certifikata

a) Ali merila zahtevajo zavezo, da uvoznik podatkov v tretji državi ali mednarodni organizaciji v primeru, ko ima razloge za domnevo, da mu spremembe zakonodaje in praks, ki se

uporabljajo zanj, lahko preprečijo izpolnjevanje obveznosti na podlagi certifikata, o tem nemudoma obvesti telo za certificiranje in izvoznika podatkov, da lahko slednji oceni, ali naj takoj ustavi prenose?

b) Ali merila zahtevajo opis korakov, ki jih je treba opraviti (vključno z obveščanjem izvoznika v EGP in sprejetjem ustreznih dodatnih ukrepov), če se uvoznik podatkov seznani z zakonodajo ali praksami tretje države, ki preprečujejo izpolnjevanje obveznosti na podlagi certifikata, ter ukrepov, ki jih je treba sprejeti, če organi tretjih držav zahtevajo informacije (vključno z obveznostjo pregleda in po potrebi izpodbijanja zakonitosti zahteve ter zmanjšanja obsega razkritih informacij)?

6. Obravnava zahtev organov tretjih držav za dostop do podatkov

a) Ali merila zahtevajo, da uvoznik podatkov nemudoma obvesti izvoznika podatkov v primeru zahtev organov tretjih držav za dostop in sprejme ustrezne dodatne ukrepe?

b) Ali merila zahtevajo, da se prenosi na podlagi zahtev javnih organov tretjih držav za nesorazmeren dostop, zlasti zahtev za obsežne in neselektivne prenose osebnih podatkov, ne smejo izvajati?

7. Dodatni zaščitni ukrepi, ki se nanašajo na izvoznika

46. Ali merila zahtevajo, da uvoznik podatkov, kjer je tako predvideno, tudi z zavezujočimi zahtevami v zvezi s tem, izvozniku podatkov zagotovi, da se dopolnilni ukrepi, ki jih je opredelil, ujemajo z ustreznimi dopolnilnimi ukrepi izvoznika podatkov, ob upoštevanju Priporočil Evropskega odbora za varstvo podatkov 01/2020 in primerov uporabe, za zagotovitev učinkovitega izvajanja dopolnilnih ukrepov uvoznika?

4 ZAVEZUJOČE IN IZVRŠLJIVE ZAVEZE, KI SE MORAJO IZVAJATI

47. Splošna uredba o varstvu podatkov v členu 42(2) zahteva, da upravljavci in obdelovalci, za katere se Splošna uredba o varstvu podatkov ne uporablja in ki so zavezani k mehanizmu certificiranja za prenose, s pogodbenimi ali drugimi pravno zavezujočimi instrumenti[22] dodatno sprejmejo zavezujoče in izvršljive zaveze, da bodo uporabljali ustrezne zaščitne ukrepe iz mehanizma certificiranja, tudi glede pravic posameznikov, na katere se nanašajo osebni podatki.

48. Kot je navedeno v Splošni uredbi o varstvu podatkov, se take zaveze lahko sprejmejo s pogodbo, kar se zdi najpreprostejša rešitev. Uporabijo se lahko tudi drugi instrumenti, če lahko upravljavec oziroma obdelovalci, ki so zavezani k mehanizmu certificiranja, dokažejo zavezujočo in izvršljivo naravo takih drugih sredstev.

49. V vsakem primeru mora biti zavezujoča in izvršljiva narava zagotovljena v skladu z zakonodajo EU, zaveze pa bi morale biti zavezujoče in izvršljive tudi za posameznike, na katere se nanašajo osebni podatki, kot upravičene tretje osebe.

50. Preprosta možnost bi bila vključitev zavezujočih in izvršljivih zavez v pogodbo med izvoznikom podatkov in uvoznikom podatkov. V praksi bi lahko stranki uporabili obstoječo pogodbo (na primer sporazum o storitvah med izvoznikom in uvoznikom podatkov, sporazum o obdelavi podatkov v skladu z 28. členom Splošne uredbe o varstvu podatkov med upravljavci in obdelovalci ali pogodbo o izmenjavi

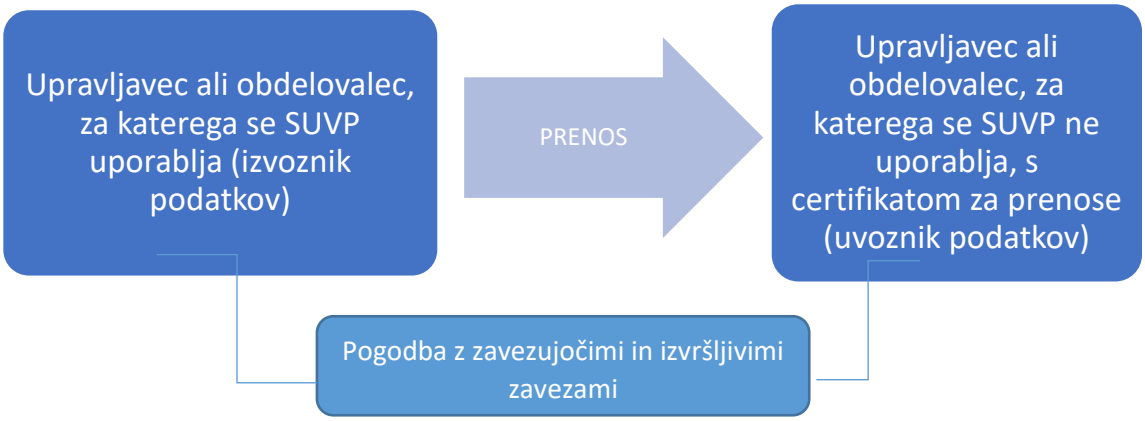
[22] Ta pravno zavezujoč instrument ni še eno orodje iz poglavja V (kot so na primer standardna pogodbena določila), saj morajo biti te zavezujoče in izvršljive zaveze iz člena 46(2)(f) zasnovane tako, da se zagotovi, da bo uvoznik spoštoval merila za certificiranje.

podatkov med ločenimi upravljavci), v katero bi se lahko vključile zavezujoče in izvršljive zaveze. Te zaveze bi se morale jasno razlikovati od vseh drugih določb. Druga možnost bi lahko bila uporaba ločene pogodbe, na primer tako, da se mehanizmu certificiranja za prenose doda vzorčna pogodba, ki bi jo morali nato podpisati upravljavci oziroma obdelovalci v tretji državi ter vsi njihovi izvozniki podatkov.

51. Obstajati bi morala prožnost izbire najustreznejše možnosti glede na posamezen primer.

52. Kadar se bo mehanizem certificiranja uporabljal za prenose in nadaljnje prenose s strani obdelovalca k podobdelovalcem, bi morala biti mehanizem certificiranja in instrument, ki določa zavezujoče in izvršljive zaveze, navedena tudi v sporazumu o obdelavi, ki ga podpišeta obdelovalec in njegov upravljavec.

Primer zavezujočih in izvršljivih zavez, vključenih v pogodbo med izvoznikom podatkov in uvoznikom podatkov:



53. Na splošno mora biti v pogodbi ali drugem pravno zavezujočem instrumentu določeno, da se upravljavec oziroma obdelovalec, ki ima certifikat in deluje kot uvoznik, zavezuje, da bo pri obdelavi zadevnih podatkov, ki jih prejme iz EGP, ravnal v skladu s pravili, navedenimi v certifikatu za prenose, in jamči, da nima razloga za domnevo, da mu zakoni in prakse v tretji državi, ki se uporabljajo za zadevno obdelavo, vključno z morebitnimi zahtevami za razkritje osebnih podatkov ali ukrepi, ki dovoljujejo dostop javnim organom, preprečujejo izpolnjevanje zavez na podlagi certifikata, in da bo obvestil izvoznika o morebitnih pomembnih spremembah zakonodaje ali praks v zvezi s tem.

54. V pogodbi ali drugem instrumentu so navedeni tudi mehanizmi, ki omogočajo izvrševanje takih zavez, če upravljavec oziroma obdelovalec, ki deluje kot uvoznik, ne upošteva pravil na podlagi certifikata, zlasti v zvezi s pravicami posameznikov, na katere se nanašajo osebni podatki, katerih podatki se prenašajo na podlagi certifikata.

55. Natančneje, pogodba ali drug instrument bi morala obravnavati:

— obstoj pravice posameznikov, na katere se nanašajo osebni podatki in katerih podatki se prenašajo na podlagi certifikata, da kot upravičene tretje osebe uveljavljajo zaveze, ki jih je uvoznik podatkov s certifikatom sprejel v okviru certificiranja;

— vprašanje odgovornosti, če uvoznik podatkov s certifikatom zunaj EGP ne upošteva pravil na podlagi certifikata. Posamezniki, na katere se nanašajo osebni podatki, imajo v primeru, ko uvoznik podatkov s certifikatom zunaj EGP ne upošteva pravil na podlagi certifikata, možnost vložiti zahtevek, vključno z odškodninskim, zoper navedeni subjekt pri nadzornem organu EGP in sodišču EGP v kraju običajnega prebivališča posameznika, na katerega se nanašajo osebni podatki, pri čemer se sklicujejo na svojo pravico upravičene tretje osebe. Uvoznik s certifikatom sprejme

odločitev posameznika, na katerega se nanašajo osebni podatki, o vložitvi zahtevka. Če bi neupoštevanje s strani uvoznika lahko povzročilo odgovornost izvoznika podatkov, imajo posamezniki, na katere se nanašajo osebni podatki, tudi možnost vložitve zahtevka zoper izvoznika podatkov pri nadzornem organu ali sodišču v kraju sedeža izvoznika podatkov ali običajnega prebivališča posameznika, na katerega se nanašajo osebni podatki[23]. Uvoznik podatkov in izvoznik podatkov bi morala sprejeti tudi dejstvo, da lahko posameznika, na katerega se nanašajo osebni podatki, zastopa tudi neprofitno telo, organizacija ali združenje v skladu s pogoji iz člena 80(1) Splošne uredbe o varstvu podatkov.

— obstoj pravice izvoznika, da kot upravičena tretja oseba uveljavi pravila na podlagi certifikata zoper uvoznika podatkov;

— obstoj obveznosti uvoznika podatkov s certifikatom, da obvesti izvoznika in nadzorni organ, pristojen za izvoznika podatkov, o morebitnih ukrepih, ki jih sprejme telo za certificiranje v odziv na odkrito neupoštevanje pravil iz certifikata s strani navedenega uvoznika podatkov.

[23] Ta odgovornost ne bi smela posegati v mehanizme, ki jih je treba izvajati na podlagi certifikata in ki so na voljo telesu za certificiranje, ki lahko prav tako ukrepa zoper certificirane upravljavce oziroma obdelovalce v skladu s certifikatom tako, da uvede popravljalne ukrepe;

PRILOGA

A. PRIMERI DOPOLNILNIH UKREPOV, KI JIH MORA IZVESTI UVOZNIK, ČE JE NA PODROČJE UPORABE CERTIFICIRANJA VKLJUČEN TRANZIT

Primer uporabe 1: Hramba podatkov za namene varnostnega kopiranja in druge namene, za katere se ne zahteva dostop do nešifriranih podatkov

Določiti je treba merila v zvezi s standardi šifriranja in varnostjo dešifrirnega ključa, zlasti merila v zvezi s pravnim položajem v tretji državi. Če je uvoznika mogoče prisiliti, da posreduje dešifrirne ključe, dodatnega ukrepa ni mogoče šteti za učinkovitega[24].

Primer uporabe 2: Prenos psevdonimiziranih podatkov

V primeru psevdonimiziranih podatkov se določijo merila glede varnosti dodatnih informacij, potrebnih za pripisovanje prenesenih podatkov določeni ali določljivi osebi, zlasti:

— merila glede pravnega položaja v tretji državi. Če je uvoznika mogoče prisiliti, da dostopa do dodatnih podatkov ali jih uporablja, da bi podatke pripisal določeni ali določljivi osebi, ukrepa ni mogoče šteti za učinkovitega[25];

— merila, ki se nanašajo na opredelitev dodatnih informacij, ki so na voljo organom tretje države, ki bi lahko zadostovale za pripis podatkov določeni ali določljivi osebi.

Primer uporabe 3: Varovanje podatkov s šifriranjem pred dostopom s strani javnih organov tretje države uvoznika, ko so v tranzitu med izvoznikom in njegovim uvoznikom

V primeru šifriranih podatkov se vključijo vsa merila za varnost tranzita. Če je uvoznika mogoče prisiliti, da posreduje kriptografske ključe za dešifriranje ali avtentikacijo ali da spremeni komponento, ki se uporablja za tranzit, tako da so ogrožene njene varnostne lastnosti, dodatnega ukrepa ni mogoče šteti za učinkovitega[26].

Primer uporabe 4: Varovani prejemnik

V primeru varovanih prejemnikov je treba opredeliti omejitve privilegijev. Obdelava podatkov mora ostati v mejah varovanja zaupnosti. To se uporablja tudi za obdelavo s strani (pod)obdelovalcev in nadaljnje prenose, katerih prejemniki morajo biti prav tako privilegirani[27].

B. PRIMERI DOPOLNILNIH UKREPOV, ČE TRANZIT NI ZAJET S CERTIFICIRANJEM IN JIH MORA ZAGOTOVITI IZVOZNIK

Primer uporabe 2: Prenos psevdonimiziranih podatkov

[24] Priloga 2 k Priporočilom 01/2020 o ukrepih, ki dopolnjujejo orodja za prenos, za zagotovitev skladnosti z ravnjo varstva osebnih podatkov na ravni EU, različica 2.0, Primer uporabe 1: hramba podatkov za namene varnostnega kopiranja in druge namene, za katere se ne zahteva dostop do nešifriranih podatkov, str. 85; https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_sl.pdf.

[25] Glej zgoraj, odstavki 86–89.

[26] Glej zgoraj, odstavek 90.

[27] Glej zgoraj, odstavek 91.

Zagotovijo se merila, ki se nanašajo na dodatne informacije, ki so na voljo organom tretje države in bi lahko zadostovale za pripis podatkov določeni ali določljivi osebi.

Primer uporabe 3: Varovanje podatkov s šifriranjem pred dostopom s strani javnih organov tretje države uvoznika, ko so v tranzitu med izvoznikom in njegovim uvoznikom

Zagotovijo se merila, ki se nanašajo na zanesljivost uporabljenega telesa za certificiranje javnih ključev ali infrastrukture, varnost kriptografskih ključev, ki se uporabljajo za avtentikacijo ali dešifriranje, ter zanesljivost upravljanja ključev in uporabo pravilno vzdrževane programske opreme brez znanih ranljivosti.

Če je uvoznika mogoče prisiliti, da razkrije kriptografske ključe, primerne za dešifriranje ali avtentikacijo, ali da spremeni komponento, ki se uporablja za tranzit, da bi se ogrozile njene varnostne lastnosti, ukrepa ni mogoče šteti za učinkovitega[28].

Primer uporabe 4: Varovani prejemnik

V primeru varovanih prejemnikov je treba opredeliti omejitve privilegijev. Obdelava podatkov mora ostati v mejah varovanja zaupnosti. To se uporablja tudi za obdelavo s strani (pod)obdelovalcev in nadaljnje prenose, katerih prejemniki morajo biti prav tako privilegirani[29].

[28] Glej zgoraj navedena priporočila, odstavek 90.
[29] Glej zgoraj navedena priporočila, odstavek 91.