Smernice

Smernice št. 1/2018 o certificiranju in opredelitvi meril za certificiranje v skladu s členoma 42 in 43 Uredbe

Različica 3.0

4. junij 2019

Sprejeto

Zgodovina različic

Različica 3.0	4. junij 2019	vključitev Priloge 2 (različica 2.0 Priloge 2, sprejeta 4. junija 2019 po javnem posvetovanju)
Različica 2.1	9. april 2019	sprejetje popravka smernic (odstavek 45)
Različica 2.0	23. januar 2019	sprejetje smernic po javnem posvetovanju – istega dne je bila za javno posvetovanje sprejeta Priloga 2 (različica 1.0)
Različica 1.0	25. maj 2018	sprejetje smernic za javno posvetovanje

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 nadaljnjem besedilu: Splošna uredba o varstvu podatkov),

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu EGP, kakor sta bila spremenjena s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018,

ob upoštevanju členov 12 in 22 svojega poslovnika z dne 25. maja 2018,

ob upoštevanju rezultatov javnega posvetovanja o smernicah, ki je potekalo od 30. maja 2018 do 12. julija 2018, in javnega posvetovanja o Prilogi 2, ki je potekalo od 15. februarja do 29. marca 2019, v skladu s členom 70(4) Splošne uredbe o varstvu podatkov –

SPREJEL NASLEDNJE SMERNICE

1 UVOD

1. Splošna uredba o varstvu podatkov (Uredba (EU) 2016/279, v nadaljnjem besedilu: Splošna uredba o varstvu podatkov ali Uredba) zagotavlja posodobljen okvir odgovornosti za varstvo podatkov v Evropi, ki je skladen s temeljnimi pravicami. V središču tega novega okvira je sklop ukrepov, ki omogočajo skladnost z določbami Splošne uredbe o varstvu podatkov. Med temi ukrepi so obvezne zahteve, ki veljajo v posebnih okoliščinah (vključno z imenovanjem pooblaščenih oseb za varstvo podatkov in izvajanjem ocen učinka v zvezi z varstvom podatkov), ter prostovoljni ukrepi, kot so kodeksi ravnanja in mehanizmi certificiranja.

2. Delovna skupina iz člena 29 je pred sprejetjem Splošne uredbe o varstvu podatkov ugotovila, da bi lahko certificiranje imelo pomembno vlogo v okviru odgovornosti za varstvo podatkov.[1] Da bi se s certificiranjem zagotovili zanesljivi dokazi o skladnosti varstva podatkov, bi morala biti vzpostavljena jasna pravila, ki bi določala zahteve glede zagotavljanja certificiranja.[2] Člen 42 Splošne uredbe o varstvu podatkov zagotavlja pravno podlago za oblikovanje takšnih pravil.

3. Člen 42(1) Splošne uredbe o varstvu podatkov določa:

   „Države članice, nadzorni organi, [Evropski] odbor [za varstvo podatkov] in Komisija zlasti na ravni Unije spodbujajo vzpostavitev mehanizmov certificiranja za varstvo podatkov ter pečatov in označb za varstvo podatkov za izkazovanje, da so dejanja obdelave s strani upravljavcev in obdelovalcev v skladu s to uredbo. Upoštevajo se posebne potrebe mikro, malih in srednjih podjetij.“

[1] Delovna skupina iz člena 29, Mnenje št. 3/2010 o načelu odgovornosti, WP173, 13. julij 2010, odstavki 69–71.
[2] Delovna skupina iz člena 29, Mnenje št. 3/2010 o načelu odgovornosti, WP173, odstavek 69.

4. Z mehanizmi certificiranja[3] se lahko izboljša preglednost za posameznike, na katere se nanašajo osebni podatki, pa tudi v razmerjih med podjetji, na primer med upravljavci in obdelovalci. V uvodni izjavi 100 Splošne uredbe o varstvu podatkov je navedeno, da je mogoče z uvedbo mehanizmov certificiranja povečati preglednost in skladnost s Splošno uredbo o varstvu podatkov ter posameznikom, na katere se nanašajo osebni podatki, omogočiti, da ocenijo raven varstva podatkov zadevnih proizvodov in storitev.[4]

5. S Splošno uredbo o varstvu podatkov se ne uvaja pravica ali obveznost upravljavcev in obdelovalcev, da pridobijo certifikat; v skladu s členom 42(3) je certificiranje prostovoljni postopek, ki pomaga pri dokazovanju skladnosti z navedeno uredbo. Države članice in nadzorni organi so pozvani kspodbujanju uvedbo mehanizmov certificiranja, ter bodo določili sodelovanje deležnikov v postopku certificiranja in njegovem življenjskem ciklu.

6. Poleg tega je upoštevanje odobrenih mehanizmov certificiranja dejavnik, ki ga morajo nadzorni organi pri odločanju o naložitvi upravne globe in njeni višini upoštevati kot oteževalni ali olajševalni dejavnik (člen 83(2)(j)).[5]

1.1 Področje uporabe smernic

7. Te smernice imajo omejeno področje uporabe; niso postopkovni priročnik za certificiranje v skladu s Splošno uredbo o varstvu podatkov. Njihov glavni namen je opredeliti krovne zahteve in merila, ki so lahko pomembna za vse vrste mehanizmov certificiranja, izdanih v skladu s členoma 42 in 43 Splošne uredbe o varstvu podatkov. V ta namen se s smernicami:

    - preučujejo razlogi za certificiranje kot orodje za zagotavljanje odgovornosti;
    - pojasnjujejo ključni pojmi iz določb o certificiranju iz členov 42 in 43; ter
    - pojasnjuje, kaj je mogoče certificirati v skladu s členoma 42 in 43, ter namen certificiranja;
    - omogoča, da je rezultat certificiranja smiseln, nedvoumen, čim bolj ponovljiv in primerljiv ne glede na izvajalca certificiranja (primerljivost).

8. V skladu s Splošno uredbo o varstvu podatkov lahko države članice in nadzorni organi člena 42 in 43 izvajajo na različne načine. Te smernice zagotavljajo nasvete glede razlage in izvajanja določb členov 42 in 43 ter bodo državam članicam, nadzornim organom in nacionalnim akreditacijskim organom pomagale vzpostaviti doslednejši in bolj usklajen pristop za izvajanje mehanizmov certificiranja v skladu s Splošno uredbo o varstvu podatkov.

9. Nasveti v teh smernicah bodo pomembni za:

[3] V teh smernicah se mehanizmi certificiranja ter pečati in označbe za varstvo podatkov skupaj imenujejo „mehanizmi certificiranja“ (glej oddelek 1.3.2).
[4] V uvodni izjavi 100 je navedeno, da bi bilo treba za povečanje preglednosti in skladnosti z Uredbo spodbujati uvedbo mehanizmov certificiranja, „ki bi posameznikom, na katere se nanašajo osebni podatki, omogočili, da hitro ocenijo raven varstva podatkov zadevnih proizvodov in storitev“.
[5] Glej Smernice o uporabi in določanju upravnih glob za namene Uredbe 2016/679 (WP 253), ki jih je pripravila Delovna skupina iz člena 29.

- pristojne nadzorne organe in Evropski odbor za varstvo podatkov pri odobritvi meril za certificiranje v skladu s členom 42(5), členom 58(3)(f) in členom 70(1)(o);
- telesa za certificiranje pri pripravi in pregledovanju meril za certificiranje pred predložitvijo pristojnemu nadzornemu organu v odobritev v skladu s členom 42(5);
- Evropski odbor za varstvo podatkov pri odobritvi evropskega pečata za varstvo podatkov v skladu s členom 42(5) in členom 70(1)(o);
- nadzorne organe pri pripravi lastnih meril za certificiranje;
- Evropsko komisijo, na katero je v skladu s členom 43(8) preneseno pooblastilo za sprejemanje delegiranih aktov, s katerimi določi zahteve, ki se upoštevajo za mehanizme certificiranja;
- Evropski odbor za varstvo podatkov pri predložitvi mnenja o zahtevah glede certificiranja Evropski komisiji v skladu s členom 70(1)(q) in členom 43(8);
- nacionalne akreditacijske organe, ki bodo morali pri akreditaciji teles za certificiranje v skladu s standardom EN-ISO/IEC 17065/2012 in dodatnimi zahtevami v skladu s členom 43 upoštevati merila za certificiranje; ter
- upravljavce in obdelovalce pri opredelitvi lastne strategije za skladnost s Splošno uredbo o varstvu podatkov in preučitvi certificiranja kot sredstva za dokazovanje skladnosti.

10. Evropski odbor za varstvo podatkov bo objavil ločene smernice za obravnavo opredelitve meril za odobritev mehanizmov certificiranja kot orodij za prenos v tretje države ali mednarodne organizacije v skladu s členom 42(2).

1.2 Namen certificiranja na podlagi Splošne uredbe o varstvu podatkov

11. Člen 42(1) določa, da se vzpostavijo mehanizmi certificiranja „za izkazovanje, da so dejanja obdelave s strani upravljavcev in obdelovalcev v skladu s to uredbo“.
12. Splošna uredba o varstvu podatkov ponazarja okvir, v katerem se lahko odobreni mehanizmi certificiranja uporabljajo kot element za izkazovanje izpolnjevanja obveznosti upravljavcev in obdelovalcev v zvezi z:
    - izvajanjem in dokazovanjem ustreznih tehničnih in organizacijskih ukrepov iz člena 24(1) in (3), člena 25 ter člena 32(1) in (3);
    - zadostnimi jamstvi, kot so navedena v odstavkih 1 (jamstva, ki jih obdelovalec zagotovi upravljavcu) in 4 (jamstva, ki jih podrejeni obdelovalec zagotovi obdelovalcu), iz člena 28(5).
13. Ker certifikat sam po sebi ne dokazuje skladnosti, temveč je element, ki ga je mogoče uporabiti za dokazovanje skladnosti, bi ga bilo treba pregledno pripraviti. Za dokazovanje skladnosti so potrebna dokazila, zlasti pisna poročila, ki ne le ponavljajo merila, ampak tudi opisujejo, kako so ta merila izpolnjena, če pa na začetku niso izpolnjena, opisujejo popravke in popravljalne ukrepe ter njihovo ustreznost, s čimer zagotavljajo razloge za odobritev in ohranjanje

veljavnosti certifikata. To vključuje povzetek posamezne odločitve o dodelitvi, podaljšanju ali preklicu certifikata. V njem bi bilo treba navesti razloge, argumente in dokaze, ki izhajajo iz uporabe meril, ter ugotovitve, mnenja ali sklepe na podlagi dejstev ali predpostavk, zbranih med certificiranjem.

1.3 Ključni pojmi

14. V naslednjem oddelku so obravnavani ključni pojmi iz členov 42 in 43. Na podlagi te analize se razvija razumevanje osnovnih pojmov in obsega certificiranja na podlagi Splošne uredbe o varstvu podatkov.

1.3.1 Razlaga „certificiranja“

15. V Splošni uredbi o varstvu podatkov pojem „certificiranje“ ni opredeljen. Mednarodna organizacija za standardizacijo (ISO) je določila univerzalno opredelitev certificiranja kot „zagotovitev pisnega zagotovila (certifikata) s strani neodvisnega organa, da zadevni proizvod, storitev ali sistem izpolnjuje določene zahteve“. Certificiranje je znano tudi kot „ugotavljanje skladnosti s strani tretjih oseb“, telesa za certificiranje pa se lahko imenujejo tudi „organi za ugotavljanje skladnosti“. V standardu EN-ISO/IEC 17000:2004 – Ugotavljanje skladnosti – Slovar in splošna načela (na katerega se nanaša standard ISO 17065) je certificiranje opredeljeno kot „potrjevanje, ki ga izvede tretja oseba [...] v zvezi s proizvodi, postopki in storitvami“.

16. Potrjevanje je „izdaja izjave na podlagi odločitve, sprejete po opravljenem pregledu, da je bilo dokazano izpolnjevanje posebnih zahtev“ (oddelek 5.2, ISO 17000:2004).

17. V okviru certificiranja na podlagi členov 42 in 43 Splošne uredbe o varstvu podatkov certificiranje pomeni potrjevanje, ki ga izvede tretja oseba v zvezi z dejanji obdelave s strani upravljavcev in obdelovalcev.

1.3.2 Mehanizmi certificiranja, pečati in označbe

18. Pojmi „mehanizmi certificiranja, pečati ali označbe“ v Splošni uredbi o varstvu podatkov niso opredeljeni in se uporabljajo skupaj. Certifikat je izjava o skladnosti. Pečat ali označba se lahko uporabljata kot znak, da je bil postopek certificiranja uspešno končan. Pečat ali označba se običajno nanaša na logotip ali simbol, katerega prisotnost (poleg certifikata) kaže, da je bil predmet certificiranja v postopku certificiranja neodvisno ocenjen in izpolnjuje določene zahteve, navedene v normativnih dokumentih, kot so predpisi, standardi ali tehnične specifikacije. Te zahteve v zvezi s certificiranjem na podlagi Splošne uredbe o varstvu podatkov so določene v dodatnih zahtevah, ki dopolnjujejo pravila za akreditacijo teles za certificiranje iz standarda EN-ISO/IEC 17065/2012 in merila za certificiranje, ki jih odobri pristojni nadzorni organ ali odbor. Certifikat, pečat ali označba v skladu s Splošno uredbo o varstvu podatkov se

lahko izda šele, ko akreditirano telo za certificiranje ali pristojni nadzorni organ izda neodvisno oceno dokazov in navede, da so merila za certificiranje izpolnjena.

19. V preglednici je prikazan splošen primer postopka certificiranja.

Vložitev vloge s strani upravljavca ali obdelovalca	Uradno preverjanje s strani telesa za certificiranje	Ocena Predhodno vrednotenje	Ocena Vrednotenje cilja vrednotenja	Ocena Potrditev rezultatov	Informacije za pristojni nadzorni organ	Certificiranje	Spremljanje	Podaljšanje certifikata
Ali je opis cilja vrednotenja nedvoumen in popoln, vključno z vmesniki?	Ali je mogoče sprejeti opis cilja vrednotenja?	Katera merila se uporabljajo?	Ali cilj vrednotenja izpolnjuje merila?	Ali vsa ustrezna določena merila upoštevajo cilj vrednotenja?	Ali so bili predloženi razlogi za dodelitev ali preklic certifikata?	Ali je mogoče podeliti certifikat?	Ali cilj vrednotenja še vedno izpolnjuje merila?	Ali obdelava še vedno izpolnjuje merila za certificiranje?
Ali je mogoče odobriti dostop do dejavnosti obdelave v okviru cilja vrednotenja?	Ali so vsi dokumenti popolni in posodobljeni?	Katere metode vrednotenja se uporabljajo?	Ali je dokumentacija o cilju vrednotenja točna?	Ali je bilo vrednotenje ustrezno dokumentirano?		Ali so poročila pripravljena za objavo?	Ali se certifikat/pečat /označba zaupanja pravilno uporablja?	Ali so bila področja razvoja zadovoljivo obravnavana?
Člen 42(6)	Člen 43(4)	Člen 43(4)	Člen 42(5), člen 43(4)	Člen 43(4)	Člen 43(1) in (5)	Člen 43(1), člen 42(7)	Člen 42(7)	Člen 42(7)

2 VLOGA NADZORNIH ORGANOV

20. Člen 42(5) določa, da certifikat izda akreditirano telo za certificiranje ali pristojni nadzorni organ. Splošna uredba o varstvu podatkov ne določa, da je izdajanje certifikatov obvezna naloga nadzornih organov. Namesto tega omogoča uporabo različnih modelov. Nadzorni organ se lahko na primer odloči za eno ali več naslednjih možnosti:

    - sam izdaja certifikate glede na lastni sistem certificiranja;
    - sam izdaja certifikate glede na lastni sistem certificiranja, vendar postopek ugotavljanja skladnosti delno ali v celoti prenese na tretje osebe;
    - vzpostavi lastni sistem certificiranja, postopek certificiranja pa zaupa telesom za certificiranje, ki izdajajo certifikate, ter
    - spodbuja trg, naj razvije mehanizme certificiranja.

21. Nadzorni organ bo moral svojo vlogo preučiti tudi ob upoštevanju odločitev glede mehanizmov akreditacije na nacionalni ravni – zlasti če je sam pristojen za akreditacijo teles za certificiranje v skladu s členom 43(1) Splošne uredbe o varstvu podatkov. Tako bo vsak nadzorni organ določil, kateri pristop bo sprejel za uresničitev širšega namena certificiranja v skladu s Splošno uredbo o varstvu podatkov. To bo določeno v okviru nalog in pooblastil iz členov 57 in 58, pa

tudi za utemeljitev certificiranja kot dejavnika, ki ga je treba upoštevati pri določitvi upravnih glob, in splošneje kot sredstva za dokazovanje skladnosti.

2.1 Nadzorni organ kot telo za certificiranje

22. Če se nadzorni organ odloči, da bo izvajal certificiranje, bo moral skrbno preučiti svojo vlogo v zvezi z nalogami, ki so mu dodeljene v skladu s Splošno uredbo o varstvu podatkov. Svoje naloge bi moral opravljati pregledno. Posebno pozornost bo moral nameniti ločitvi pooblastil v zvezi s preiskavami in izvrševanjem, da bi preprečil morebitna navzkrižja interesov.

23. Kadar nadzorni organ deluje kot telo za certificiranje, mora zagotoviti ustrezno vzpostavitev mehanizma certificiranja in oblikovati lastna ali sprejeti druga merila za certificiranje. Poleg tega mora vsak nadzorni organ, ki izdaja certifikate, te redno pregledovati (člen 57(1)(o)), je pa tudi pooblaščen za njihov preklic, kadar zahteve v zvezi s certifikatom niso ali niso več izpolnjene (člen 58(2)(h)). Za izpolnjevanje teh zahtev je koristno vzpostaviti postopek certificiranja in postopkovne zahteve ter s posamezno organizacijo, ki vloži vlogo, skleniti pravno izvršljiv sporazum za izvajanje dejavnosti certificiranja, če ni drugače določeno, na primer z nacionalno zakonodajo. Zagotoviti bi bilo treba, da se s tem sporazumom o certificiranju od vložnika zahteva, da izpolnjuje vsaj merila za certificiranje, vključno s potrebnimi ureditvami za izvedbo vrednotenja, spremljanjem izpolnjevanja meril in rednim pregledovanjem, ki vključuje dostop do informacij in/ali prostorov, dokumentacijo ter objavo poročil in rezultatov, pa tudi preiskovanje pritožb. Poleg tega se pričakuje, da bo nadzorni organ poleg zahtev iz člena 43(2) upošteval zahteve iz smernic za akreditacijo teles za certificiranje.

2.2 Dodatne naloge nadzornega organa v zvezi s certificiranjem

24. V državah članicah, v katerih začnejo delovati telesa za certificiranje, je nadzorni organ ne glede na svoje dejavnosti pooblaščen in pristojen za:

    - ocenjevanje meril sistema certificiranja in pripravo osnutka odločitve (člen 42(5));
    - obveščanje odbora o osnutku odločitve, ko je namenjen odobritvi meril za certificiranje (člen 64(1)(c) in (7)), in upoštevanje mnenja odbora (člen 64(1)(c) in člen 70(1)(t));
    - odobritev meril za certificiranje (člen 58(3)(f)), preden sta mogoča akreditacija in certificiranje (člen 42(5) in člen 43(2)(b));
    - objavo meril za certificiranje (člen 43(6));
    - delovanje kot pristojni organ za sisteme certificiranja na ravni EU, rezultat katerih so lahko evropski pečati za varstvo podatkov, ki jih potrdi Evropski odbor za varstvo podatkov (člen 42(5) in člen 70(1)(o)), ter
    - odreditev telesu za certificiranje, (a) naj certifikata ne izda ali (b) naj certifikat prekliče, če zahteve v zvezi s certifikatom (postopki ali merila za certificiranje) niso ali niso več izpolnjene (člen 58(2)(h)).

25. S Splošno uredbo o varstvu podatkov je nadzornemu organu dodeljena naloga odobritve meril za certificiranje, ne pa tudi naloga oblikovanja meril. Nadzorni organ bi moral za odobritev meril za certificiranje na podlagi člena 42(5) jasno razumeti, kaj pričakovati, zlasti glede obsega in vsebine za dokazovanje skladnosti s Splošno uredbo o varstvu podatkov ter v zvezi s svojo nalogo spremljanja in zagotavljanja uporabe Splošne uredbe o varstvu podatkov. Priloga vsebuje smernice za zagotavljanje usklajenega pristopa pri ocenjevanju meril za namen odobritve.

26. V skladu s členom 43(1) morajo telesa za certificiranje svoj nadzorni organ obvestiti, preden izdajo ali podaljšajo certifikat, da se pristojnemu nadzornemu organu dovoli izvajanje popravljalnih pooblastil v skladu s točko (h) člena 58(2). Poleg tega morajo telesa za certificiranje v skladu s členom 43(5) pristojnemu nadzornemu organu tudi utemeljiti dodelitev ali preklic zahtevanega certifikata. Čeprav je s Splošno uredbo o varstvu podatkov nadzornim organom omogočeno, da določijo operativne načine prejemanja, potrjevanja, pregledovanja in obravnavanja teh informacij (to lahko vključuje na primer tehnološke rešitve, ki omogočajo poročanje teles za certificiranje), se lahko vzpostavijo postopek in merila za obdelavo informacij in poročil, ki jih v skladu s členom 43(1) telo za certificiranje predloži za vsak uspešen projekt certificiranja. Nadzorni organ lahko na podlagi teh informacij izvaja svoja pooblastila, da telesu za certificiranje odredi, naj certifikat prekliče ali ga ne izda (člen 58(2)(h)), ter spremlja in zagotavlja uporabo zahtev in meril za certificiranje v skladu s Splošno uredbo o varstvu podatkov (člen 57(1)(a) in člen 58(2)(h)). To bo podprlo usklajen pristop in primerljivost pri certificiranju, ki ga izvajajo različna telesa za certificiranje, ter pripomoglo k temu, da nadzorni organi poznajo status certifikata organizacije.

3 VLOGA TELESA ZA CERTIFICIRANJE

27. Telo za certificiranje izdaja, pregleduje, podaljšuje in preklicuje certifikate (člen 42(5) in (7)) na podlagi mehanizma certificiranja in odobrenih meril (člen 43(1)). Zato mora telo za certificiranje ali lastnik sistema certificiranja določiti in uvesti merila in postopke za certificiranje, vključno s postopki za spremljanje skladnosti, pregledovanje, obravnavo pritožb in preklic. Merila za certificiranje se pregledujejo v okviru postopka akreditacije, pri katerem se upoštevajo pravila in postopki, v skladu s katerimi se izdajajo certifikati, pečati ali označbe (člen 43(2)(c)).

28. Da bi bilo telo za certificiranje akreditirano v skladu s členom 43, mora imeti vzpostavljen mehanizem certificiranja in merila za certificiranje. Dejavnosti telesa za certificiranje so močno odvisne od področja uporabe in vrste meril za certificiranje, ki vplivajo na postopke certificiranja in obratno. V skladu s posebnimi merili se lahko na primer zahtevajo posebne metode vrednotenja, kot so pregledi na kraju samem in pregled kodeksa. Ti postopki so obvezni za akreditacijo in so dodatno pojasnjeni v smernicah o akreditaciji.

29. V skladu s Splošno uredbo o varstvu podatkov mora telo za certificiranje nadzornim organom zagotoviti informacije, zlasti o posameznih certifikatih, potrebne za spremljanje uporabe mehanizma certificiranja (člen 42(7), člen 43(5) in člen 58(2)(h)).

4 ODOBRITEV MERIL ZA CERTIFICIRANJE

30. Merila za certificiranje so sestavni del vsakega mehanizma certificiranja. Zato se s Splošno uredbo o varstvu podatkov zahteva, naj merila za certificiranje za mehanizem certificiranja odobri pristojni nadzorni organ (člen 42(5) in člen 43(2)(b)). V primeru evropskega pečata za varstvo podatkov pa merila za certificiranje odobri Evropski odbor za varstvo podatkov (člen 42(5) in člen 70(1)(o)). V nadaljevanju sta pojasnjena oba načina odobritve meril za certificiranje.

31. Evropski odbor za varstvo podatkov priznava naslednje namene za odobritev meril za certificiranje:

    - ustrezno upoštevanje zahtev in načel v zvezi z varstvom posameznikov pri obdelavi osebnih podatkov iz Uredbe (EU) 2016/679 ter
    - prispevanje k dosledni uporabi Splošne uredbe o varstvu podatkov.

32. Merila za certificiranje se odobrijo, če v celoti upoštevajo zahtevo Splošne uredbe o varstvu podatkov, da mehanizem certificiranja upravljavcem in obdelovalcem omogoča dokazovanje skladnosti z navedeno uredbo.

4.1 Odobritev meril s strani pristojnega nadzornega organa

33. Pristojni nadzorni organ mora merila za certificiranje odobriti pred postopkom akreditacije telesa za certificiranje ali med tem postopkom. Odobriti je treba tudi posodobljene ali dodatne sisteme ali sklope meril istega telesa za certificiranje, ki temeljijo na standardu ISO 17065, in sicer pred uporabo spremenjenih mehanizmov certificiranja (člen 42(5) in člen 43(2)(b)). Nadzorni organi vse zahteve za odobritev meril za certificiranje obravnavajo pošteno in nediskriminatorno ter v skladu z javno objavljenim postopkom, ki določa splošne pogoje, ki jih je treba izpolniti, in opis postopka odobritve.

34. Telo za certificiranje lahko v posamezni državi članici certifikat izda le v skladu z merili, ki jih je odobril nadzorni organ v tej državi članici. Drugače rečeno, merila za certificiranje mora odobriti pristojni nadzorni organ v državi, v kateri želi telo za certificiranje izvajati certificiranje in v kateri pridobi akreditacijo. Za sisteme certificiranja na ravni Evrope glej spodnji oddelek.

4.2 Odobritev meril za evropski pečat za varstvo podatkov s strani Evropskega odbora za varstvo podatkov

35. Telo za certificiranje lahko certifikat izda tudi v skladu z merili, ki jih je Evropski odbor za varstvo podatkov odobril za evropski pečat za varstvo podatkov. Rezultat meril za certificiranje, ki jih v skladu s členom 63 odobri Evropski odbor za varstvo podatkov, je lahko evropski pečat za varstvo podatkov (člen 42 (5)). Evropski odbor za varstvo podatkov ob upoštevanju obstoječih dogovorov o certificiranju in akreditaciji priznava, da je zaželeno preprečiti razdrobljenost trga certifikatov za varstvo podatkov. Poudarja, da morajo države članice, nadzorni organi, odbor

in Komisija v skladu s členom 42(1) spodbujati vzpostavitev mehanizmov certificiranja, zlasti na ravni Unije.

4.2.1 Vloga za odobritev

36. Vlogo za odobritev meril v skladu s členom 42(5) in členom 70(1)(o) s strani Evropskega odbora za varstvo podatkov je treba predložiti prek pristojnega nadzornega organa, v njej pa bi morala biti navedena namera lastnika sistema, kandidata ali akreditiranega telesa za certificiranje za ponujanje meril v okviru mehanizma certificiranja, ki zadevajo upravljavce in obdelovalce v vseh državah članicah. Pristojni nadzorni organ bo Evropskemu odboru za varstvo podatkov predložil osnutek, ko bo menil, da bi lahko odbor merila odobril.

37. Izbira kraja vložitve vloge za odobritev meril bo odvisna od sedeža lastnikov sistemov certificiranja ali teles za certificiranje.

38. Če bi telo za certificiranje vložilo vlogo, bi bilo običajno v postopku vložitve vloge za akreditacijo ali pa bi ga prej že akreditiral pristojni nadzorni organ ali nacionalni akreditacijski organ njegove države članice. Če je telo za certificiranje že akreditirano za mehanizem certificiranja v skladu s Splošno uredbo o varstvu podatkov, lahko to pomaga poenostaviti postopek odobritve.

4.2.2 Merila za evropski pečat za varstvo podatkov

39. Evropski odbor za varstvo podatkov bo usklajeval postopek ocenjevanja in po potrebi odobril merila za evropski pečat za varstvo podatkov. V okviru ocene bodo obravnavana področja, kot so: področje uporabe meril in možnost uporabe za skupno certificiranje. Če merila odobri Evropski odbor za varstvo podatkov, se od nadzornega organa, pristojnega za sedež telesa za certificiranje v EU, pričakuje, da bo obravnaval pritožbe glede samega mehanizma in o tem obveščal druge nadzorne organe. Ta nadzorni organ je pristojen tudi za sprejemanje ukrepov proti telesu za certificiranje. Odvisno od primera bo pristojni nadzorni organ uradno obvestil druge nadzorne organe in Evropski odbor za varstvo podatkov.

40. Za merila za certificiranje, s katerimi se obravnava skupno certificiranje, veljajo zahteve na ravni EU; zagotavljati bi morala poseben mehanizem za izpolnjevanje teh zahtev. Evropski mehanizmi certificiranja morajo biti namenjeni uporabi v vseh državah članicah. V skladu s členom 42(5) morajo biti mehanizem za evropski pečat za varstvo podatkov in njegova merila prilagodljivi, tako da po potrebi upoštevajo nacionalne področne predpise, na primer za obdelavo podatkov v šolah, poleg tega mora mehanizem predvidevati uporabo po vsej Evropi.

41. Primer: mednarodna šola, ki v Uniji ponuja izobraževanje posameznikom, na katere se nanašajo osebni podatki, ima sedež v državi članici „A“. Šola želi certificirati svoj postopek spletne prijave s sistemom certificiranja na ravni EU, da bi pridobila evropski pečat za varstvo podatkov. Zaprositi namerava za izdajo certifikata za dejanja obdelave, ki ga ponuja telo za certificiranje, ustanovljeno v državi članici „B“, na podlagi evropskega pečata za varstvo podatkov. Za merila za pečat, oblikovana in dokumentirana v ustreznem mehanizmu, se zahteva, da morajo biti zmožna upoštevati predpise za šole, ki se uporabljajo v državi članici „A“. Z merili bi bilo treba zahtevati tudi, da se v postopku za spletne prijave šole zagotovijo

informacije in upoštevajo veljavne zahteve držav članic glede varstva podatkov, ki se lahko v drugih državah članicah razlikujejo. Primer so nabori osebnih podatkov, ki jih je treba predložiti za namene prijave, na primer ocene ali rezultati preskusov v vrtcu, različna obdobja hrambe podatkov, zbiranje ali obdelava finančnih ali biometričnih podatkov in dodatne omejitve glede obdelave.

- Merila na visoki ravni za odobritev mehanizma za evropski pečat za varstvo podatkov vključujejo:
  - merila, ki jih je odobril odbor;
  - uporabo v različnih jurisdikcijah, pri čemer se po potrebi upoštevajo ustrezne nacionalne pravne zahteve in področni predpisi;
  -
- usklajena merila, ki jih je mogoče prilagoditi nacionalnim zahtevam;
  - opis mehanizma za certificiranje z navedbo;
  - sporazumov o certificiranju, ki priznavajo vseevropske zahteve;
  - postopke za zagotavljanje rešitev za nacionalne razlike in zagotavljanje, da pečat pomaga pri dokazovanju skladnosti s Splošno uredbo o varstvu podatkov; ter
  - jezik poročil, naslovljenih na vse zadevne nadzorne organe.

42. Priloga vsebuje tudi nasvete glede meril za evropski pečat za varstvo podatkov.

4.2.3 Vloga akreditacije

43. Kot je navedeno v oddelku 4.2.1, se lahko telesa za certificiranje po tem, ko so merila opredeljena kot ustrezna za skupno certificiranje in jih je odbor v skladu s členom 42(5) odobril kot taka, akreditirajo za izvajanje certificiranja na podlagi teh meril na ravni Unije.

44. Sistemi, ki naj bi bili na voljo samo v nekaterih državah članicah, ne bodo kandidati za pečate EU. Za akreditacijo za področje uporabe evropskega pečata za varstvo podatkov bo potrebna akreditacija v državi članici sedeža telesa za certificiranje, ki namerava upravljati sistem, tj. telesa, odgovornega za izdajanje certifikatov in upravljanje dejavnosti certificiranja, ki jih opravljajo njegovi subjekti in podružnice v drugih državah članicah. Če certificiranje samostojno upravljajo in izvajajo druge enote ali uradi, bo treba vsako od teh enot ali uradov posebej akreditirati v državi članici, v katerih imajo sedež. Drugače rečeno, akreditacija je nujna samo v državi članici, v kateri ima telo za certificiranje sedež, če certifikate izdaja samo njegov sedež. Če pa certifikate izdajajo tudi druge enote telesa za certificiranje, morajo biti te prav tako akreditirane.

45. Če telo za certificiranje ni bilo akreditirano za certificiranje na podlagi evropskega pečata za varstvo podatkov, pa ne more uporabljati meril, ki jih je odobril Evropski odbor za varstvo podatkov, in ne more ponujati izdajanja pečatov.

5 OBLIKOVANJE MERIL ZA CERTIFICIRANJE

46. S Splošno uredbo o varstvu podatkov je vzpostavljen okvir za oblikovanje meril za certificiranje. Temeljne zahteve glede postopka certificiranja so obravnavane v členih 42 in 43 ter hkrati zagotavljajo bistvena merila za postopke certificiranja, podlaga za merila za certificiranje pa mora biti izpeljana iz načel in pravil Splošne uredbe o varstvu podatkov ter mora pomagati zagotoviti njihovo izpolnjevanje.

47. Oblikovanje meril za certificiranje bi moralo biti osredotočeno na preverljivost, pomen in primernost teh meril za dokazovanje skladnosti z Uredbo. Merila za certificiranje bi morala biti oblikovana tako, da so jasna in razumljiva ter omogočajo praktično uporabo.

48. Pri pripravi meril za certificiranje se med drugim po potrebi upoštevajo naslednji vidiki skladnosti, ki podpirajo oceno dejanj obdelave:

    - zakonitost obdelave v skladu s členom 6;
    - načela v zvezi z obdelavo podatkov v skladu s členom 5;
    - pravice posameznikov, na katere se nanašajo osebni podatki, v skladu s členi 12 do 23;
    - obveznost uradnega obveščanja o kršitvah varstva osebnih podatkov v skladu s členom 33;
    - obveznost vgrajenega in privzetega varstva podatkov v skladu s členom 25;
    - ali je bila opravljena ocena učinka v zvezi z varstvom podatkov v skladu s členom 35(7)(d), če je ustrezno; ter
    - tehnični in organizacijski ukrepi, vzpostavljeni v skladu s členom 32.

49. Obseg, v katerem se ti vidiki upoštevajo pri merilih, se lahko razlikuje glede na obseg certificiranja, ki lahko vključuje vrsto dejanj obdelave in področje certificiranja (npr. zdravstveni sektor).

5.1 Kaj je mogoče certificirati v skladu s Splošno uredbo o varstvu podatkov?

50. Evropski odbor za varstvo podatkov meni, da Splošna uredba o varstvu podatkov omogoča široko razlago, kaj vse je mogoče certificirati na podlagi navedene uredbe, dokler je poudarek na pomoči pri dokazovanju skladnosti dejanj obdelave upravljavcev in obdelovalcev s to uredbo (člen 42(1)).

51. Pri ocenjevanju dejanja obdelave je treba po potrebi upoštevati naslednje tri osrednje sestavne dele:

    1. osebne podatke (stvarno področje uporabe Splošne uredbe o varstvu podatkov);

2. tehnične sisteme – infrastrukturo, kot sta strojna in programska oprema, ki se uporablja za obdelavo osebnih podatkov; ter

3. procese in postopke, povezane z dejanji obdelave.

52. Vsak sestavni del, ki se uporablja pri dejanjih obdelave, je treba oceniti glede na določena merila. Na certificiranje lahko vplivajo vsaj štirje različni pomembni dejavniki: (1) organizacija in pravna struktura upravljavca ali obdelovalca; (2) oddelek, okolje in ljudje, vključeni v dejanja obdelave; (3) tehnični opis elementov, ki jih je treba oceniti, in nazadnje (4) infrastruktura informacijske tehnologije, ki podpira dejanje obdelave, vključno z operacijskimi sistemi, virtualnimi sistemi, podatkovnimi zbirkami, sistemi za avtentikacijo in avtorizacijo, usmerjevalniki in požarnimi zidovi, sistemi za shranjevanje, komunikacijsko infrastrukturo ali dostopom do interneta ter z njimi povezanimi tehničnimi ukrepi.

53. Vsi trije osrednji sestavni deli so pomembni za oblikovanje postopkov certificiranja in meril za certificiranje. Koliko se upoštevajo, se lahko razlikuje glede na predmet certificiranja. V nekaterih primerih nekaterih sestavnih delov tako ni treba upoštevati, če se oceni, da za predmet certificiranja niso pomembni.

54. Splošna uredba o varstvu podatkov vsebuje dodatne smernice za podrobnejšo opredelitev tega, kaj se lahko certificira v skladu z njo. Iz člena 42(7) izhaja, da se certifikati na podlagi Splošne uredbe o varstvu podatkov izdajo samo upravljavcem in obdelovalcem podatkov, kar izključuje na primer certificiranje pooblaščenih oseb za varstvo podatkov. V členu 43(1)(b) je naveden standard ISO 17065, ki določa akreditacijo teles za certificiranje, ki ocenjujejo skladnost proizvodov, storitev in postopkov. Rezultat dejanja obdelave ali niza dejanj je lahko po terminologiji standarda ISO 17065 proizvod ali storitev in se kot tak lahko certificira. Obdelava podatkov o zaposlenih za namene izplačevanja plač ali upravljanja dopustov je na primer niz dejanj v smislu Splošne uredbe o varstvu podatkov, katerega rezultat po terminologiji ISO je lahko proizvod, postopek ali storitev.

55. Na podlagi teh premislekov Evropski odbor za varstvo podatkov meni, da je obseg certificiranja na podlagi Splošne uredbe o varstvu podatkov usmerjen v dejanja obdelave ali nize dejanj. Ti lahko obsegajo postopke upravljanja v smislu organizacijskih ukrepov, torej kot sestavni deli dejanja obdelave (npr. postopek upravljanja, vzpostavljen za obravnavanje pritožb, v okviru obdelave podatkov o zaposlenih za namene izplačevanja plač).

56. Za oceno skladnosti dejanja obdelave z merili za certificiranje je treba zagotoviti primer uporabe. Skladnost uporabe tehnične infrastrukture, uporabljene pri dejanju obdelave, je na primer odvisna od kategorij podatkov, za obdelavo katerih je zasnovana. Organizacijski ukrepi so odvisni od kategorij in količine podatkov ter tehnične infrastrukture, ki se uporablja za obdelavo, ob upoštevanju narave, obsega, vsebine in namenov obdelave ter tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki.

57. Poleg tega je treba upoštevati, da se lahko aplikacije informacijske tehnologije zelo razlikujejo, tudi če se uporabljajo za iste namene obdelave. Zato je treba to upoštevati pri opredelitvi področja uporabe mehanizmov certificiranja in pripravi meril za certificiranje, tj. obseg certificiranja in meril za certificiranje ne bi smel biti tako ozek, da bi izključeval različno zasnovane aplikacije informacijske tehnologije.

5.2 Določitev predmeta certificiranja

58. Področje uporabe mehanizma certificiranja je treba razlikovati od predmeta – imenovanega tudi cilj vrednotenja (*target of evaluation* – ToE) – v posameznih projektih certificiranja na podlagi mehanizma certificiranja. Mehanizem certificiranja lahko svoje področje uporabe opredeljuje na splošno ali glede na posebno vrsto ali področje dejanj obdelave, s čimer lahko že določa predmete certificiranja, ki spadajo na področje uporabe mehanizma certificiranja (npr. varno shranjevanje in varstvo osebnih podatkov v digitalnem trezorju). Vsekakor se lahko zanesljiva in smiselna ocena skladnosti izvede le, če je posamezni predmet projekta certificiranja natančno opisan. Jasno je treba opisati, katera dejanja obdelave so vključena v predmet certificiranja, nato pa, kateri osrednji sestavni deli, tj. kateri podatki, postopki in tehnična infrastruktura, bodo ocenjeni in kateri ne. Pri tem je treba vedno upoštevati in opisati tudi vmesnike za druge postopke. Jasno je, da tisto, kar ni znano, ne more biti del ocene, zato tega ni mogoče certificirati. Vsekakor mora biti posamezni predmet certificiranja smiseln glede na sporočilo ali trditev, navedeno s certifikatom oziroma na certifikatu, in ne bi smel zavajati uporabnika, stranke ali potrošnika.

59. [Primer 1]

    Banka svojim strankam ponuja spletišče za namene spletnega bančništva. V okviru te storitve je mogoče opravljati nakazila, kupovati delnice, odpreti trajne naloge in upravljati račun. Banka želi na podlagi mehanizma certificiranja za varstvo podatkov s splošnim obsegom, ki temelji na splošnih merilih, certificirati v nadaljevanju navedene elemente.

    a) Varna prijava

       Varna prijava je dejanje obdelave, ki je končnemu uporabniku razumljivo in je pomembno z vidika varstva podatkov, saj ima pomembno vlogo pri zagotavljanju varnosti zadevnih osebnih podatkov. Zato je to dejanje obdelave potrebno za varno prijavo, torej lahko pomeni smiseln cilj vrednotenja, če je v certifikatu jasno navedeno, da je certificirana le prijava kot dejanje obdelave.

    b) Čelni sistem spletnih aplikacij

       Čelni sistem spletnih aplikacij je lahko pomemben z vidika varstva podatkov, ga končni uporabnik pa ga ne razume, zato ne more biti smiseln cilj vrednotenja. Poleg tega uporabnik ne ve, katere storitve na spletišču in torej katera dejanja obdelave so zajeti s certifikatom.

    c) Spletno bančništvo

       Čelni sistemi spletnih aplikacij skupaj z zalednimi sistemi pomenijo dejanja obdelave, zagotovljena v okviru storitve spletnega bančništva, ki so lahko pomembna za uporabnika. V tem okviru je treba oba sistema vključiti v cilj vrednotenja. Dejanja obdelave, ki niso neposredno povezana z zagotavljanjem storitve spletnega bančništva, kot so dejanja obdelave za namene preprečevanja pranja denarja, pa se lahko izključijo iz cilja vrednotenja.

Med storitvami spletnega bančništva, ki jih banka ponuja na svojem spletišču, pa so lahko tudi druge storitve, za katere so potrebna ločena dejanja obdelave. V tem okviru lahko druge storitve vključujejo na primer zavarovalni produkt. Ker ta dodatna storitev ni neposredno povezana z namenom zagotavljanja storitev spletnega bančništva, se lahko izključi iz cilja vrednotenja. Če je ta dodatna storitev (zavarovanje) izključena iz cilja vrednotenja, so vmesniki za to storitev, vgrajeni v spletišče, del cilja vrednotenja in jih je zato treba opisati, da je mogoče jasno razlikovati med storitvami. Takšen opis je potreben za opredelitev in oceno možnih prenosov podatkov med dvema storitvama.

60. [Primer 2]

    Banka svojim strankam ponuja storitev, ki jim omogoča združevanje informacij v zvezi z različnimi računi in kreditnimi karticami pri več bankah (združevanje računov). Banka želi, da bi bila njena storitev certificirana v skladu s Splošno uredbo o varstvu podatkov. Pristojni nadzorni organ je odobril poseben sklop meril za certificiranje, osredotočen na to vrsto dejavnosti. Področje uporabe mehanizma certificiranja se nanaša samo na naslednje vidike skladnosti:

    - avtentikacijo uporabnika in
    - sprejemljive načine za pridobitev podatkov, ki naj bi se združili, od drugih bank/storitev.

    Ker področje uporabe tega mehanizma certificiranja samo po sebi opredeljuje cilj vrednotenja, tega cilja v okviru predlaganega področja uporabe ni mogoče smiselno omejiti in certificirati samo posebnih značilnosti ali ene same dejavnosti obdelave. V tem primeru mora biti cilj vrednotenja enak posameznemu področju uporabe.

5.3 Metode vrednotenja in metodologija ocenjevanja

61. Za oceno skladnosti za pomoč pri dokazovanju skladnosti dejanj obdelave je treba določiti in opredeliti metode vrednotenja in metodologijo ocenjevanja. Pomembno je, ali se informacije za oceno zbirajo samo iz dokumentacije (kar samo po sebi ne bi zadostovalo) ali pa se dejavno zbirajo na kraju samem in z neposrednim ali posrednim dostopom. Način zbiranja informacij ima posledice za pomen certificiranja, zato bi ga bilo treba opredeliti in opisati.

    Postopki za izdajo in redno pregledovanje certifikatov bi morali vključevati specifikacije za opredelitev ustrezne ravni vrednotenja (kako poglobljeno in podrobno mora biti), da bi se izpolnila merila za certificiranje, ter zagotavljanje:

    - informacij in specifikacij o uporabljenih metodah ocenjevanja ter ugotovitev, zbranih na primer med revizijami na kraju samem ali iz dokumentacije;
    - metod vrednotenja, osredotočenih na dejanja obdelave (podatki, sistemi, postopki) in namen obdelave;
    - opredelitve kategorij podatkov in potreb po varstvu ter pojasnil, ali so vključeni obdelovalci ali tretje osebe;

- opredelitve vlog in obstoja mehanizma za nadzor dostopa, opredeljenega na podlagi vlog in odgovornosti.

62. Poglobljenost vrednotenja vpliva na pomen in vrednost certifikata. Z zmanjšanjem poglobljenosti vrednotenja zaradi pragmatičnih namenov ali znižanja stroškov se bo pomen certifikata o varstvu podatkov zmanjšal. Po drugi strani lahko odločitve o podrobnosti vrednotenja presegajo finančne zmožnosti vložnika ter pogosto tudi zmožnosti ocenjevalcev in revizorjev. Za dokazovanje skladnosti ni vedno nujna zelo podrobna analiza uporabljenih sistemov informacijske tehnologije, da certifikat ostane smiseln.

5.4 Dokumentiranje ocene

63. Dokumentacija v zvezi s certificiranjem bi morala biti podrobna in izčrpna. Če je dokumentacija pomanjkljiva, ustrezna ocena ni mogoča. Bistvena naloga dokumentacije v zvezi s certificiranjem je, da zagotavlja preglednost v postopku vrednotenja na podlagi mehanizma certificiranja. Dokumentacija daje odgovore na vprašanja v zvezi z zakonsko določenimi zahtevami. Z mehanizmi certificiranja bi bilo treba zagotavljati standardizirano metodologijo dokumentiranja. Nato bo vrednotenje omogočilo primerjavo dokumentacije v zvezi s certificiranjem z dejanskim stanjem na mestu samem in glede na merila za certificiranje.

64. Izčrpna dokumentacija o tem, kaj je bilo certificirano, in o uporabljeni metodologiji pripomore k preglednosti. V skladu s členom 43(2)(c) bi bilo treba z mehanizmi certificiranja vzpostaviti postopke, ki omogočajo preglede certifikatov. Da bi lahko nadzorni organ ocenil, ali in koliko je mogoče certificiranje potrditi v formalnih preiskavah, je podrobna dokumentacija morda najprimernejši način obveščanja. Zato bi morala biti dokumentacija, pripravljena med vrednotenjem, osredotočena na tri glavne vidike:

    - doslednost in skladnost uporabljenih metod vrednotenja;
    - metode vrednotenja, usmerjene v dokazovanje skladnosti predmeta certificiranja z merili za certificiranje in s tem s Splošno uredbo o varstvu podatkov; ter
    - dejstvo, ali je rezultate vrednotenja potrdilo neodvisno in nepristransko telo za certificiranje.

5.5 Dokumentiranje rezultatov

65. V uvodni izjavi 100 so navedene informacije o ciljih, ki naj bi se dosegli z uvedbo certificiranja.

„Za povečanje preglednosti in skladnosti s to uredbo bi bilo treba spodbujati uvedbo mehanizmov [certificiranja] ter pečatov in označb za varstvo podatkov, ki bi posameznikom, na katere se nanašajo osebni podatki, omogočili, da hitro ocenijo raven varstva podatkov zadevnih proizvodov in storitev.“

66. Dokumentiranje in sporočanje rezultatov imata pomembno vlogo pri povečanju preglednosti. Telesa za certificiranje, ki uporabljajo mehanizme certificiranja, pečate ali označbe, namenjene posameznikom, na katere se nanašajo osebni podatki (v vlogi potrošnikov ali strank), bi morali

zagotavljati lahko dostopne, razumljive in smiselne informacije o certificiranih dejanjih obdelave. Te javne informacije bi morale vključevati vsaj:

- opis cilja vrednotenja;
- sklic na odobrena merila, uporabljena za določen cilj vrednotenja;
- metodologijo za vrednotenje meril (vrednotenje na kraju samem, dokumentacija itd.); in
- trajanje veljavnosti certifikata;
- poleg tega bi morale omogočati primerljivost rezultatov za nadzorne organe in javnost.

6 SMERNICE ZA OPREDELITEV MERIL ZA CERTIFICIRANJE

67. Merila za certificiranje so sestavni del mehanizma certificiranja. Postopek certificiranja vključuje zahteve glede tega, kdo izvede oceno, ki se izvede v posameznih projektih certificiranja, ki zadevajo konkreten predmet ali cilj vrednotenja, kako in v kakšnem obsegu jo izvede ter kako podrobna je ta ocena. Merila za certificiranje določajo nominalne zahteve, na podlagi katerih se oceni dejansko dejanje obdelave, opredeljeno v cilju vrednotenja. Te smernice za opredelitev meril za certificiranje zagotavljajo splošne nasvete, ki bodo olajšali ocenjevanje meril za certificiranje za namen odobritve.

    - Pri odobritvi ali opredelitvi meril za certificiranje bi bilo treba upoštevati naslednje splošne pomisleke. Merila za certificiranje bi morala:
    - biti enotna in preverljiva;
    - biti takšna, da jih je mogoče revidirati, da se olajša vrednotenje dejanj obdelave v skladu s Splošno uredbo o varstvu podatkov, zlasti z opredelitvijo ciljev in smernic za izvajanje za doseganje navedenih ciljev;
    - biti ustrezna glede na ciljno skupino (npr. udeleženci v poslovanju med podjetji (B2B) ter med podjetji in strankami (B2C));
    - upoštevati druge standarde (kot so standardi ISO, standardi na nacionalni ravni) in biti po potrebi interoperabilna z njimi; ter
    - biti prilagodljiva in nadgradljiva, da se lahko uporabljajo za različno velike organizacije različnih vrst, vključno z mikro, malimi in srednjimi podjetji, v skladu s členom 42(1) in za pristop, ki temelji na analizi tveganja, v skladu z uvodno izjavo 77.

68. Majhno lokalno podjetje, na primer trgovec na drobno, bo običajno izvajalo manj zapletena dejanja obdelave kot velika večnacionalna družbaza prodajo na drobno. Zahteve za zakonitost dejanj obdelave so enake, upoštevati pa je treba obseg in zapletenost obdelave podatkov; iz tega sledi, da je treba zagotoviti možnost, da se mehanizmi certificiranja in njihova merila stopnjujejo glede na zadevno dejavnost obdelave.

6.1 Veljavni standardi

69. Telesa za certificiranje bodo morala preučiti, kako se pri posameznih merilih upoštevajo ustrezni veljavni instrumenti, kot so kodeksi ravnanja, tehnični standardi ali nacionalne regulativne in pravne pobude. V idealnem primeru bodo merila interoperabilna z veljavnimi standardi, ki lahko upravljavcu ali obdelovalcu pomagajo izpolniti njegove obveznosti iz Splošne uredbe o varstvu podatkov. Toda, panožni standardi so pogosto osredotočeni na zaščito in varnost organizacije pred grožnjami, Splošna uredba o varstvu podatkov pa je usmerjena k varstvu temeljnih pravic posameznikov. Ta drugačni vidik je treba upoštevati pri oblikovanju meril ali odobritvi meril ali mehanizmov certificiranja, ki temeljijo na panožnih standardih.

6.2 Opredelitev meril

70. Merila za certificiranje morajo ustrezati izjavi o certificiranju (sporočilu ali trditvi) mehanizma ali sistema certificiranja in pričakovanjem, ki jih vzbuja. Že iz imena mehanizma certificiranja lahko izhaja področje uporabe in ima posledice za določitev meril.

71. [Primer 3]

    Področje uporabe mehanizma, imenovanega „HealthPrivacyMark“, bi moralo biti omejeno na zdravstveni sektor. Ime pečata vzbuja pričakovanje, da so bile preučene zahteve glede varstva podatkov v zvezi s podatki o zdravstvenem stanju. Zato morajo biti merila tega mehanizma primerna za ocenjevanje zahtev glede varstva podatkov v tem sektorju.

72. [Primer 4]

    Mehanizem, ki se nanaša na certificiranje dejanj obdelave, ki vključujejo sisteme upravljanja na področju obdelave podatkov, bi moral določati merila, ki omogočajo priznavanje in ocenjevanje postopkov upravljanja ter podpornih tehničnih in organizacijskih ukrepov.

73. [Primer 5]

    Pri merilih za mehanizem, povezan z računalništvom v oblaku, je treba upoštevati posebne tehnične zahteve, potrebne za uporabo storitev v oblaku. Če se na primer uporabljajo strežniki zunaj EU, je treba pri merilih upoštevati pogoje iz poglavja V Splošne uredbe o varstvu podatkov v zvezi s prenosi podatkov v tretje države.

74. Merila, oblikovana tako, da ustrezajo različnim ciljem vrednotenja v različnih sektorjih in/ali državah članicah, bi morala: omogočati uporabo v različnih scenarijih, omogočati opredelitev ustreznih ukrepov, da ustrezajo dejanjem obdelave majhnega, srednjega ali velikega obsega, ter upoštevati različno verjetna in različno velika tveganja za pravice in svoboščine posameznikov v skladu s Splošno uredbo o varstvu podatkov. Zato morajo postopki certificiranja (npr. za dokumentacijo, preskušanje ali metodo in temeljitost vrednotenja), ki dopolnjujejo merila, izpolnjevati te potrebe ter omogočati in imeti vzpostavljena pravila, na primer za uporabo ustreznih meril v posameznih projektih certificiranja. Merila morajo omogočati oceno, ali so bila zagotovljena zadostna jamstva za izvajanje ustreznih tehničnih in organizacijskih ukrepov.

6.3 Življenjska doba meril za certificiranje

75. Čeprav morajo merila za certificiranje skozi čas ostati zanesljiva, ne bi smela biti nespremenljiva. Revidirati jih je treba na primer, kadar:

    - se spremeni pravni okvir;
    - Sodišče v sodbah razloži pogoje in določbe; ali
    - tehnika napreduje.

Za Evropski odbor za varstvo podatkov

Predsednica

(Andrea Jelinek)

PRILOGA 1: NALOGE IN POOBLASTILA NADZORNIH ORGANOV V ZVEZI S CERTIFICIRANJEM V SKLADU S SPLOŠNO UREDBO O VARSTVU PODATKOV

	Določbe	Zahteve
Naloge	Člen 43(6)	Od nadzornega organa zahteva, da merila iz člena 42(5) objavi v lahko dostopni obliki in jih pošlje odboru.
	Člen 57(1)(n)	Od nadzornega organa zahteva, da odobri merila za certificiranje v skladu s členom 42(5).
	Člen 57(1)(o)	Določa, da nadzorni organ izvaja redne preglede certifikatov, izdanih v skladu s členom 42(7), kadar je to ustrezno (tj. če izdaja certifikate).
	Člen 64(1)(c)	Od nadzornega organa zahteva, da odboru posreduje osnutek odločitve, če je ta namenjen odobritvi meril za certificiranje iz člena 42(5).
Pooblastila	Člen 58(1)(c)	Določa, da ima nadzorni organ pooblastila za izvajanje pregledov certifikatov, izdanih v skladu s členom 42(7).
	Člen 58(2)(h)	Določa, da ima nadzorni organ pooblastila, da prekliče certifikat ali telesu za certificiranje odredi preklic certifikata ali mu odredi, naj ne izda certifikata.
	Člen 58(3)(e)	Določa, da ima nadzorni organ pooblastila za akreditacijo teles za certificiranje.
	Člen 58(3)(f)	Določa, da ima nadzorni organ pooblastila, da izdaja certifikate in odobri merila za certificiranje.

PRILOGA 2

1 UVOD

V Prilogi 2 so smernice za pregled in oceno meril za certificiranje v skladu s členom 42(5). V njej so opredeljene teme, ki jih bodo nadzorni organi za varstvo podatkov in Evropski odbor za varstvo podatkov obravnavali in uporabili pri odobritvi meril za certificiranje za mehanizem certificiranja. Telesa za certificiranje in lastniki sistemov, ki želijo pripraviti merila in jih predložiti v odobritev, bi morali upoštevati ta vprašanja. Seznam ni izčrpen, temveč vsebuje tiste teme, ki jih je nujno treba upoštevati. Vsa vprašanja ne bodo relevantna, vendar bi jih bilo treba upoštevati pri pripravi meril, mogoče pa bo treba tudi pojasniti, zakaj merila ne zajemajo določenih vidikov. Nekatera vprašanja se ponavljajo, ker se nanašajo na različne vidike. Te smernice bi bilo treba upoštevati v skladu s pravnimi zahtevami iz Splošne uredbe o varstvu podatkov in, če je to ustrezno, iz nacionalne zakonodaje.

2 PODROČJE UPORABE MEHANIZMA CERTIFICIRANJA IN CILJ VREDNOTENJA

a. Ali je področje uporabe mehanizma certificiranja (za katerega se uporabljajo merila varstva podatkov) jasno opisano?

b. Ali je področje uporabe mehanizma certificiranja smiselno za njegovo ciljno občinstvo in ni zavajajoče?

- *Primer: pečat zaupanja vrednega podjetja nakazuje, da so bile revidirane dejavnosti obdelave celotnega podjetja, čeprav so dejansko predmet certifikacije le določena dejanja obdelave, na primer postopek spletnega plačila. Področje uporabe je torej zavajajoče.*

c. Ali področje uporabe mehanizma certificiranja odraža vse relevantne vidike dejanj obdelave?

- *Primer: oznaka o varstvu zaupnosti v zdravstvu mora vsebovati vse podatke o vrednotenju v zvezi z zdravjem, da so izpolnjene zahteve iz člena 9.*

d. Ali področje uporabe mehanizma certificiranja omogoča smiselno certificiranje varstva podatkov ob upoštevanju narave, vsebine in tveganja povezanih dejanj obdelave?

- *Primer: če se področje uporabe mehanizma certificiranja osredotoča samo na določene vidike dejanj obdelave, kot je zbiranje podatkov, ne pa na nadaljnja dejanja obdelave, kot je obdelava za namene oblikovanja oglaševalskih profilov ali upravljanja pravic posameznika, na katerega se nanašajo osebni podatki, to za posameznike, na katere se nanašajo osebni podatki, ni smiselno.*

e. Ali področje uporabe mehanizma certificiranja zajema obdelavo osebnih podatkov v posamezni državi uporabe ali pa velja za čezmejno obdelavo in/ali prenose?

f. Ali je v merilih za certificiranje zadostno opisano, kako bi moral biti opredeljen cilj vrednotenja?

- *Primer: pečat zaupnosti s splošnim področjem uporabe, ki zahteva samo „specifikacijo obdelave, ki je predmet certifikacije“, ne bi zagotovil dovolj jasnih smernic o tem, kako določiti in opisati cilj vrednotenja.*
- *Primer: (posebno) področje uporabe pečata zaupnosti za varno hrambo osebnih podatkov v digitalnem trezorju bi moralo vsebovati podroben opis meril, ki morajo biti izpolnjena,*

npr. opredelitev digitalnega trezorja, zahteve sistema, obvezni tehnični in organizacijski ukrepi. V tem primeru lahko področje uporabe jasno opredeli cilj vrednotenja.

(1) Ali merila zahtevajo, da cilj vrednotenja vključuje navedbo vseh relevantnih dejanj obdelave, prikaz tokov podatkov in opredelitev področja uporabe cilja vrednotenja?

- *Primer: mehanizem certificiranja zagotavlja certificiranje dejanj obdelave upravljavcev v skladu s Splošno uredbo o varstvu podatkov, ne da bi bilo področje uporabe podrobneje opredeljeno (splošno področje uporabe). Merila, ki se uporabljajo v okviru mehanizma, od upravljavca vložnika zahtevajo, da določi ciljno dejanje obdelave (cilj vrednotenja) v smislu vrst podatkov ter uporabljenih sistemov in postopkov.*

(2) Ali merila zahtevajo, da mora vlagatelj jasno navesti, kje se obdelava, ki je predmet vrednotenja, začne in konča? Ali merila zahtevajo, da cilj vrednotenja vključuje vmesnike, če soodvisna dejanja obdelave niso vključena kot del cilja vrednotenja? Ali je to ustrezno utemeljeno?

- *Primer: cilj vrednotenja, ki dovolj podrobno opisuje dejanje obdelave spletne storitve, kot so registracija uporabnikov, zagotavljanje storitev, izdajanje računov, beleženje naslovov IP ter vmesniki za uporabnike in tretje osebe, ne pa gostovanje strežnika (toda vključno s sporazumi o obdelavi ter tehničnih in organizacijskih ukrepih).*

g. Ali merila zagotavljajo, da so (posamezni) cilji vrednotenja razumljivi za ciljno občinstvo, vključno s posamezniki, na katere se nanašajo osebni podatki, kadar je to ustrezno?

3 SPLOŠNE ZAHTEVE

a. Ali so vsi relevantni pojmi, ki se uporabljajo v katalogu meril (tj. celoten sklop meril za certificiranje), navedeni, pojasnjeni in opisani?

b. Ali so navedeni vsi normativni sklici?

c. Ali merila vključujejo opredelitev odgovornosti, postopkov in obdelave na področju varstva podatkov, ki jih zajema področje uporabe mehanizma certificiranja?

4 DEJANJA OBDELAVE, ČLEN 42(1)

Ali merila glede (splošnega ali posebnega) področja uporabe mehanizma certificiranja obravnavajo vse relevantne sestavne dele dejanj obdelave (podatki, sistemi in postopki)?

a. Ali merila glede cilja vrednotenja zahtevajo navedbo veljavnih pravnih podlag za obdelavo?

b. Ali merila glede cilja vrednotenja upoštevajo relevantne faze obdelave in celoten življenjski cikel podatkov, vključno z izbrisom in/ali anonimizacijo?

c. Ali merila glede cilja vrednotenja zahtevajo prenosljivost podatkov?

d. Ali merila glede cilja vrednotenja omogočajo navedbo in upoštevanje posebnih vrst dejanj obdelave, na primer avtomatizirano odločanje, oblikovanje profilov?

e. Ali merila glede cilja vrednotenja omogočajo opredelitev posebnih kategorij podatkov?

f. Ali merila omogočajo in zahtevajo oceno tveganja posameznih dejanj obdelave in potreb po varstvu pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki?

g. Ali merila omogočajo in zahtevajo ustrezno upoštevanje tveganj za pravice in svoboščine fizičnih oseb?

…

5 ZAKONITOST OBDELAVE

a. Ali merila zahtevajo preverjanje zakonitosti posameznih dejanj obdelave glede na namen in nujnost obdelave?

b. Ali merila zahtevajo preverjanje vseh zahtev pravne podlage za posamezna dejanja obdelave?

6 NAČELA, ČLEN 5

a. Ali merila ustrezno upoštevajo vsa načela varstva podatkov v skladu s členom 5?

b. Ali merila zahtevajo dokaz najmanjšega obsega podatkov za posamezni cilj vrednotenja?

…

7 SPLOŠNE OBVEZNOSTI UPRAVLJAVCEV IN OBDELOVALCEV

a. Ali merila zahtevajo dokaz o pogodbah, sklenjenih med obdelovalci in upravljavci?

b. Ali so pogodbe med upravljavcem in obdelovalcem predmet vrednotenja?

c. Ali merila odražajo obveznosti upravljavca v skladu s poglavjem IV?

d. Ali merila zahtevajo dokaz o pregledu in posodobitvi tehničnih in organizacijskih ukrepov, ki jih izvaja upravljavec v skladu s členom 24(1)?

e. Ali se z merili preverja, ali je organizacija ocenila, ali bi bilo treba imenovati pooblaščeno osebo za varstvo podatkov, kot je določeno v členu 37? Ali pooblaščena oseba za varstvo podatkov, kadar je to ustrezno, izpolnjuje zahteve iz členov 37 do 39?

f. Ali merila predvidevajo, da je treba v skladu s členom 30(5) voditi evidence dejavnosti obdelave in da morajo biti zahteve iz člena 30 ustrezno izpolnjene?

8 PRAVICE POSAMEZNIKOV, NA KATERE SE NANAŠAJO OSEBNI PODATKI

a. Ali merila ustrezno obravnavajo pravico posameznika, na katerega se nanašajo osebni podatki, do obveščenosti in zahtevajo vzpostavitev ustreznih ukrepov?

b. Ali merila zahtevajo, da se posameznikom, na katere se nanašajo osebni podatki, odobri ustrezen ali celo večji dostop do njihovih podatkov in nadzor nad njimi, vključno s prenosljivostjo podatkov?

c. Ali merila zahtevajo vzpostavitev ukrepov, ki omogočajo poseg v dejanje obdelave, da se zagotovijo pravice posameznikov, na katere se nanašajo osebni podatki, in omogočijo popravki, izbris ali omejitve?

…

9 TVEGANJA ZA PRAVICE IN SVOBOŠČINE FIZIČNIH OSEB

a. Ali merila omogočajo in zahtevajo oceno tveganj za pravice in svoboščine fizičnih oseb?

b. Ali merila določajo ali zahtevajo priznano metodologijo za oceno tveganja? Ali je ta metodologija, če je ustrezna, tudi sorazmerna?

c. Ali merila omogočajo in zahtevajo oceno učinka predvidenih dejanj obdelave na pravice in svoboščine fizičnih oseb?

d. Ali merila zahtevajo predhodno posvetovanje o preostalih tveganjih, ki jih ni mogoče ublažiti, na podlagi rezultatov ocene učinka o varstvu podatkov?

10 TEHNIČNI IN ORGANIZACIJSKI UKREPI, KI ZAGOTAVLJAJO ZAŠČITO

a. Ali merila zahtevajo uporabo tehničnih in organizacijskih ukrepov, ki zagotavljajo zaupnost dejanj obdelave?

b. Ali merila zahtevajo uporabo tehničnih in organizacijskih ukrepov, ki zagotavljajo celovitost dejanj obdelave?

c. Ali merila zahtevajo uporabo tehničnih in organizacijskih ukrepov, ki zagotavljajo razpoložljivost dejanj obdelave?

d. Ali merila zahtevajo uporabo ukrepov, ki zagotavljajo preglednost dejanj obdelave v zvezi z

e. odgovornostjo?

f. pravicami posameznikov, na katere se nanašajo osebni podatki?

g. oceno posameznih dejanj obdelave, npr. za algoritemsko preglednost?

h. Ali merila zahtevajo uporabo tehničnih in organizacijskih ukrepov, ki zagotavljajo pravice posameznikov, na katere se nanašajo osebni podatki, npr. možnost zagotavljanja informacij ali prenosljivost podatkov?

i. Ali merila zahtevajo uporabo tehničnih in organizacijskih ukrepov, ki omogočajo poseg v dejanje obdelave, da se zagotovijo pravice posameznikov, na katere se nanašajo osebni podatki, in omogočijo popravki, izbris ali omejitve?

j. Ali merila zahtevajo uporabo ukrepov, ki omogočajo poseg v dejanje obdelave, da se posamezni sistem ali postopek popravi ali preveri?

k. Ali merila zahtevajo uporabo tehničnih in organizacijskih ukrepov za zagotovitev najmanjšega obsega podatkov, kot so odprava povezav na podatke ali ločevanje podatkov od posameznika, na katerega se nanašajo osebni podatki, anonimizacija ali psevdonimizacija ali izolacija podatkovnih sistemov?

l. Ali merila zahtevajo tehnične ukrepe za izvajanje privzetega varstva podatkov?

m. Ali merila zahtevajo tehnične in organizacijske ukrepe za izvajanje vgrajenega varstva podatkov, npr. sistem upravljanja varstva podatkov, ki zahteve glede varstva podatkov prikaže, o njih obvešča, jih nadzira in izvršuje?

n. Ali merila zahtevajo tehnične in organizacijske ukrepe za izvajanje ustreznega rednega usposabljanja in izobraževanja za osebje, ki ima stalen ali reden dostop do osebnih podatkov?

o. Ali merila zahtevajo pregled ukrepov?

p. Ali merila zahtevajo samooceno/notranjo revizijo?

q. Ali merila zahtevajo ukrepe, s katerimi se zagotovi, da se dolžnosti obveščanja o kršitvah varstva osebnih podatkov izvajajo v predpisanem času in obsegu?

r. Ali merila zahtevajo vzpostavitev in preverjanje postopkov za obvladovanje incidentov?

s. Ali merila zahtevajo spremljanje novih vprašanj v zvezi z zasebnostjo in tehnologijo ter po potrebi posodobitev sistema?

…

11 DRUGE POSEBNE ZNAČILNOSTI, KI SO PRIJAZNE VARSTVU PODATKOV

a. Ali merila zahtevajo izvajanje tehnik za izboljšanje varstva podatkov? To bi lahko vključevalo merila, ki zahtevajo boljše varstvo podatkov z odpravo ali zmanjšanjem osebnih podatkov in/ali tveganja v zvezi z varstvom podatkov.

- *Primer: merila, ki zahtevajo boljšo odpravo povezav na osebne podatke z uporabo uporabniško usmerjenega upravljanja identitete, kot so poverilnice na podlagi atributov, in ne organizacijsko usmerjenega upravljanja identitete, bi odražala tehniko za izboljšanje varstva podatkov.*

b. Ali merila zahtevajo izvajanje boljših kontrol posameznikov, na katere se nanašajo osebni podatki, za izboljšanje možnosti samoodločanja in izbire?

…

12 MERILA ZA DOKAZOVANJE OBSTOJA USTREZNIH ZAŠČITNIH UKREPOV PRI PRENOSU OSEBNIH PODATKOV

Merila bodo obravnavana v prihodnjih smernicah o členu 42(2).

13 DODATNA MERILA ZA EVROPSKI PEČAT ZA VARSTVO PODATKOV

a. Ali merila predvidevajo vključitev vseh držav članic?

b. Ali se v merilih lahko upoštevajo zakonodaja ali scenariji držav članic na področju varstva podatkov?

c. Ali merila zahtevajo vrednotenje posameznih ciljev vrednotenja v zvezi s področno zakonodajo držav članic o varstvu podatkov?

d. Ali merila zahtevajo, da upravljavec ali obdelovalec posameznikom, na katere se nanašajo osebni podatki, in zainteresiranim stranem v jezikih držav članic zagotovi:

e. informacije o obdelavi/cilju vrednotenja?

f. dokumentacijo v zvezi z obdelavo/ciljem vrednotenja?

g. rezultate vrednotenja?

…

14 CELOVITO VREDNOTENJE MERIL

a. Ali merila v celoti zajemajo področje uporabe mehanizma certificiranja (tj. celovita merila), da bi se zagotovila zadostna jamstva, da je certifikacija zaupanja vredna?

- *Primer: če se področje uporabe mehanizma certificiranja osredotoča na dejanja obdelave zdravstvenih podatkov, bi bilo treba zagotoviti visoko raven varstva podatkov z opredelitvijo meril, ki zagotavljajo na primer poglobljeno oceno ter uporabo načel vgrajene in privzete zasebnosti.*

b. Ali so merila sorazmerna z obsegom dejanja obdelave, ki ga zajema področje uporabe mehanizma certificiranja, občutljivostjo informacij in tveganjem, ki ga predstavlja obdelava?

c. Ali je verjetno, da bodo merila izboljšala upoštevanje varstva podatkov s strani upravljavcev in obdelovalcev?

d. Ali bodo posamezniki, na katere se nanašajo osebni podatki, imeli koristi v zvezi s svojo pravico do obveščenosti ter ali jim bodo med drugim pojasnjeni želeni rezultati?