Smjernice

Smjernice 1/2018 o certificiranju i utvrđivanju kriterija certificiranja u skladu s člancima 42. i 43. Uredbe

Verzija 3.0

4. lipnja 2019.

Doneseno

Povijest verzija

Verzija 3.0	4. lipnja 2019.	Uključivanje Priloga 2. (verzija 2.0 Priloga 2. donesena 4. lipnja 2019. nakon javnog savjetovanja)
Verzija 2.1	9. travnja 2019.	Donošenje ispravka Smjernica (stavak 45.)
Verzija 2.0	23. siječnja 2019.	Donošenje Smjernica nakon javnog savjetovanja – na isti je dan donesen Prilog 2. (verzija 1.0) za javno savjetovanje
Verzija 1.0	25. svibnja 2018.	Donošenje Smjernica za javno savjetovanje

Sadržaj

1 Uvod 5

1.1 Područje primjene Smjernica 6

1.2 Svrha certificiranja na temelju Opće uredbe o zaštiti podataka 7

1.3 Ključni koncepti 8

1.3.1 Tumačenje „certificiranja" 8

1.3.2 Mehanizmi certificiranja, pečati i oznake 8

2 Uloga nadzornih tijela 9

2.1 Nadzorno tijelo kao certifikacijsko tijelo 10

2.2 Dodatne zadaće nadzornog tijela u pogledu certificiranja 10

3 Uloga certifikacijskog tijela 11

4 Odobravanje kriterija certificiranja 12

4.1 Odobravanje kriterija koje provodi nadležno nadzorno tijelo 12

4.2 Odobravanje kriterija za Europski pečat za zaštitu podataka koje provodi Europski odbor za zaštitu podataka 13

4.2.1 Zahtjev za odobrenje 13

4.2.2 Kriteriji za Europski pečat za zaštitu podataka 13

4.2.3 Uloga akreditiranja 14

5 Izrada kriterija certificiranja 15

5.1 Što se može certificirati na temelju Opće uredbe o zaštiti podataka? 16

5.2 Određivanje predmeta certificiranja 17

5.3 Metode evaluacije i metodologija ocjenjivanja 19

5.4 Dokumentiranje ocjenjivanja 19

5.5 Dokumentiranje rezultata 20

6 Smjernice za utvrđivanje kriterija certificiranja 20

6.1 Postojeće norme 21

6.2 Utvrđivanje kriterija 21

6.3 Vijek trajanja kriterija certificiranja 22

Prilog 1.: Zadaće i ovlasti nadzornih tijela u odnosu na certificiranje u skladu s Općom uredbom o zaštiti podataka 23

Prilog 2. 24

1 Uvod 24

2 Opseg mehanizma certificiranja i predmet evaluacije 24

3 Opći zahtjevi 25

4 Postupak obrade, članak 42. stavak 1. 25

5 Zakonitost obrade 26
6 Načela, članak 5 26
7 Opće obveze voditelja i izvršitelja obrade 26
8 Prava ispitanika 26
9 Rizici za prava i slobode pojedinaca 27
10 Tehničke i organizacijske mjere kojima se jamči zaštita 27
11 Druge posebne značajke pogodne za zaštitu podataka 28
12 Kriteriji kojima se dokazuje postojanje odgovarajućih zaštitnih mjera pri prijenosu osobnih podataka 28
13 Dodatni kriteriji za Europski pečat za zaštitu podataka 28
14 Cjelovita evaluacija kriterija 29

Europski odbor za zaštitu podataka

uzimajući u obzir članak 70. stavak 1. točku (e) Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (dalje u tekstu „Opća uredba o zaštiti podataka”),

uzimajući u obzir Sporazum o EGP-u, a posebno njegov Prilog XI. i Protokol 37., kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.,

uzimajući u obzir članke 12. i 22. svojeg Poslovnika od 25. svibnja 2018.,

nakon što je razmotrio rezultate javnog savjetovanja o Smjernicama održanog u razdoblju od 30. svibnja 2018. do 12. srpnja 2018. i o Prilogu 2. održanog u razdoblju od 15. veljače 2019. do 29. ožujka 2019. u skladu s člankom 70. stavkom 4. Opće uredbe o zaštiti podataka,

DONIO JE SLJEDEĆE SMJERNICE:

1 UVOD

1. Općom uredbom o zaštiti podataka (Uredba (EU) 2016/279 ili „Uredba”) utvrđuje se modernizirani okvir za zaštitu podataka u Europi koji se temelji na odgovornosti i poštovanju temeljnih prava. Za taj novi okvir važno je donijeti niz mjera kojima se olakšava poštovanje odredbi Opće uredbe o zaštiti podataka. Tim su mjerama obuhvaćeni obvezni zahtjevi u posebnim okolnostima (uključujući imenovanje službenika za zaštitu podataka i provedbu procjena učinka na zaštitu podataka) i dobrovoljne mjere kao što su kodeksi ponašanja i mehanizmi certificiranja.

2. Prije donošenja Opće uredbe o zaštiti podataka Radna skupina iz članka 29. utvrdila je da bi certificiranje moglo imati važnu ulogu u okviru za zaštitu podataka koji se temelji na odgovornosti1. Kako bi se certificiranjem pružili pouzdani dokazi o sukladnosti sa zaštitom podataka, potrebno je uvesti jasna pravila kojima se utvrđuju zahtjevi u pogledu certificiranja2. U članku 42. Opće uredbe o zaštiti podataka utvrđena je pravna osnova za izradu takvih pravila.

3. U članku 42. stavku 1. Opće uredbe o zaštiti podataka propisuje se sljedeće:

   „Države članice, nadzorna tijela, Odbor i Komisija potiču, osobito na razini Unije, uspostavu mehanizama certificiranja zaštite podataka te pečata i oznaka za zaštitu podataka u svrhu dokazivanja da su postupci obrade koje provode voditelj obrade i izvršitelj obrade u skladu s ovom Uredbom. Uzimaju se u obzir posebne potrebe mikro, malih i srednjih poduzeća.”

[1] Radna skupina iz članka 29., Mišljenje 3/2010 o načelu odgovornosti, WP173, 13. srpnja 2010., točke od 69. do 71.
[2] Radna skupina iz članka 29., Mišljenje 3/2010 o načelu odgovornosti (WP173), točka 69.

4. Mehanizmima certificiranja3 može se povećati transparentnost za ispitanike, ali i transparentnost u odnosima među poduzećima, primjerice, između voditelja obrade i izvršitelja obrade. U uvodnoj izjavi 100. Opće uredbe o zaštiti podataka navodi se da se uvođenjem mehanizama certificiranja mogu povećati transparentnost i usklađenost s tom uredbom te se ispitanicima može omogućiti procjena razine zaštite podataka za relevantne proizvode i usluge4.

5. Općom uredbom o zaštiti podataka ne uvodi se pravo na certificiranje ili obveza certificiranja za voditelje i izvršitelje obrade. U skladu s člankom 42. stavkom 3., certificiranje je dobrovoljan postupak kojim se pomaže u dokazivanju usklađenosti s Općom uredbom o zaštiti podataka. Države članice i nadzorna tijela pozivaju se da potiču uvođenje mehanizama certificiranja te da uključe dionike u postupak certificiranja i njegov vijek trajanja.

6. Nadalje, nadzorna tijela moraju poštovanje odobrenih mehanizama certificiranja uzeti u obzir kao otegotne ili olakotne čimbenike kada odlučuju o izricanju upravne novčane kazne i o njezinu iznosu (članak 83. stavak 2. točka (j))5.

1.1 Područje primjene Smjernica

7. Područje primjene ovih Smjernica ograničeno je i one nisu postupovni priručnik za certificiranje u skladu s Općom uredbom o zaštiti podataka. Glavni je cilj ovih Smjernica utvrditi najvažnije zahtjeve i kriterije koji mogu biti relevantni za sve vrste mehanizama certificiranja izdanih u skladu s člancima 42. i 43. Opće uredbe o zaštiti podataka. U tu se svrhu u ovim Smjernicama:

   - razmatra logička osnova za certificiranje kao instrument za osiguranje odgovornosti,
   - objašnjavaju ključni koncepti odredaba o certificiranju iz članaka 42. i 43. i
   - objašnjava opseg onoga što se može certificirati na temelju članaka 42. i 43. te svrha certificiranja,
   - olakšava postizanje ishoda certificiranja koji je smislen, jednoznačan, u najvećoj mogućoj mjeri ponovljiv te usporediv neovisno o certifikatoru (usporedivost).

8. Općom uredbom o zaštiti podataka državama članicama i nadzornim tijelima omogućuje se više načina za provedbu članaka 42. i 43. U Smjernicama se daju savjeti o tumačenju i provedbi odredaba članaka 42. i 43. te se državama članicama, nadzornim tijelima i nacionalnim akreditacijskim tijelima pomaže u utvrđivanju dosljednijeg, usklađenijeg pristupa za provedbu mehanizama certificiranja u skladu s Općom uredbom o zaštiti podataka.

9. Savjeti koji se nalaze u ovim Smjernicama bit će relevantni za:

[3] U ovim se Smjernicama mehanizmi certificiranja te pečati i oznake za zaštitu podataka zajednički nazivaju „mehanizmi certificiranja"; vidjeti odjeljak 1.3.2.
[4] U uvodnoj izjavi 100. navodi se da bi se uvođenje mehanizama certificiranja trebalo poticati kako bi se povećala transparentnost i usklađenost s tom uredbom te omogućilo ispitanicima da brzo procjene razinu zaštite podataka za relevantne proizvode i usluge.
[5] Vidjeti Smjernice o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679 (WP 253) Radne skupine iz članka 29.

- nadležna nadzorna tijela i Europski odbor za zaštitu podataka, pri odobravanju kriterija certificiranja na temelju članka 42. stavka 5., članka 58. stavka 3. točke (f) i članka 70. stavka 1. točke (o),
- certifikacijska tijela, pri izradi i reviziji kriterija certificiranja prije njihova podnošenja na odobrenje nadležnom nadzornom tijelu u skladu s člankom 42. stavkom 5.,
- Europski odbor za zaštitu podataka, pri odobravanju Europskog pečata za zaštitu podataka na temelju članka 42. stavka 5. i članka 70. stavka 1. točke (o),
- nadzorna tijela, pri izradi vlastitih kriterija certificiranja,
- Europsku komisiju, koja je ovlaštena donositi delegirane akte za potrebe određivanja zahtjeva koji se trebaju uzeti u obzir za mehanizme certificiranja na temelju članka 43. stavka 8.,
- Europski odbor za zaštitu podataka, kada daje mišljenje Europskoj komisiji o zahtjevima za certificiranje u skladu s člankom 70. stavkom 1. točkom (q) i člankom 43. stavkom 8.,
- nacionalna akreditacijska tijela, koja će kriterije certificiranja trebati uzeti u obzir s obzirom na akreditaciju certifikacijskih tijela u skladu s normom EN-ISO/IEC 17065/2012 i dodatnim zahtjevima u skladu s člankom 43. i
- voditelje i izvršitelje obrade, pri utvrđivanju njihovih strategija za usklađivanje s Općom uredbom o zaštiti podataka i razmatranju certificiranja kao načina dokazivanja sukladnosti.

10. Europski odbor za zaštitu podataka objavit će posebne smjernice za rješavanje pitanja utvrđivanja kriterija za odobravanje mehanizama certificiranja kao instrumenata za prijenos trećim zemljama ili međunarodnim organizacijama u skladu s člankom 42. stavkom 2.

1.2 Svrha certificiranja na temelju Opće uredbe o zaštiti podataka

11. U članku 42. stavku 1. propisuje se da se mehanizmi certificiranja uspostavljaju „u svrhu dokazivanja da su postupci obrade koje provode voditelj obrade i izvršitelj obrade u skladu s ovom Uredbom".

12. U Općoj uredbi o zaštiti podataka navode se primjeri u kojima se odobreni mehanizmi certificiranja mogu koristiti kao element za dokazivanje toga da se voditelji i izvršitelji obrade pridržavaju svojih obveza kad je riječ o:

    - provedbi i dokazivanju odgovarajućih tehničkih i organizacijskih mjera iz članka 24. stavaka 1. i 3., članka 25. i članka 32. stavaka 1. i 3.,
    - dostatnim jamstvima iz članka 28. stavka 1. (koje izvršitelj obrade daje voditelju obrade) i stavka 4. (koje podizvršitelj obrade daje izvršitelju obrade), a u vezi sa stavkom 5. tog članka.

13. Budući da se certificiranjem samim po sebi ne dokazuje usklađenost, nego ono čini element koji se može koristiti za dokazivanje usklađenosti, trebalo bi se provesti na transparentan

način. Za dokazivanje usklađenosti potrebna je popratna dokumentacija, osobito pisana izvješća u kojima se ne samo ponavlja da su kriteriji ispunjeni, nego se opisuje i kako su ispunjeni, a ako kriteriji na početku nisu bili ispunjeni, opisuju se ispravci i korektivne mjere te njihova primjerenost, čime se navode razlozi za dodjeljivanje i održavanje certifikata. To uključuje opis pojedinačne odluke o dodjeljivanju, obnavljanju ili povlačenju certifikata. U njemu bi se trebali navesti razlozi, argumenti i dokazi koji proizlaze iz primjene kriterija te zaključci, prosudbe ili indicije koje proizlaze iz činjenica ili pretpostavki prikupljenih tijekom postupka certificiranja.

1.3 Ključni koncepti

14. U sljedećem se odjeljku razmatraju ključni koncepti iz članaka 42. i 43. U toj se analizi razrađuje shvaćanje osnovnih pojmova i opsega certificiranja na temelju Opće uredbe o zaštiti podataka.

1.3.1 Tumačenje „certificiranja"

15. U Općoj uredbi o zaštiti podataka ne definira se pojam „certificiranje". Prema općoj definiciji Međunarodne organizacije za normizaciju (ISO) certificiranje je „pisano jamstvo (certifikat) koje daje neovisno tijelo o tome da predmetni proizvod, usluga ili sustav ispunjava određene zahtjeve". Certificiranje se naziva i „ocjenjivanjem sukladnosti koje provodi treća strana", a certifikacijska se tijela mogu nazivati i „tijelima za ocjenjivanje sukladnosti". U normi EN-ISO/IEC 17000:2004 – Ocjenjivanje sukladnosti – Pojmovi i opća načela (na koju se odnosi norma ISO17065) – certificiranje se definira na sljedeći način: „potvrđivanje treće strane... koje se odnosi na proizvode, postupke i usluge".

16. Potvrđivanje je „izdavanje izjave, na temelju odluke donesene nakon preispitivanja, o tome da je dokazano ispunjavanje određenih zahtjeva" (odjeljak 5.2. norme ISO 17000:2004).

17. U kontekstu certificiranja na temelju članaka 42. i 43. Opće uredbe o zaštiti podataka, certificiranje se odnosi na potvrđivanje treće strane koje se odnosi na postupke obrade koje provode voditelji i izvršitelji obrade.

1.3.2 Mehanizmi certificiranja, pečati i oznake

18. U Općoj uredbi o zaštiti podataka ne definira se pojam „mehanizmi certificiranja, pečati ili oznake" te se ti pojmovi koriste kolektivno. Certifikat je izjava o sukladnosti. Pečat ili oznaka mogu se koristiti za označivanje uspješnog dovršetka postupka certificiranja. Pečat ili oznaka obično se odnose na logotip ili simbol čije postojanje (uz certifikat) označava da je predmet certificiranja neovisno ocijenjen u postupku certificiranja te da je sukladan određenim zahtjevima koji su navedeni u normativnim dokumentima kao što su propisi, norme ili tehničke specifikacije. Ti zahtjevi, u kontekstu certificiranja na temelju Opće uredbe o zaštiti podataka, utvrđeni su u dodatnim zahtjevima kojima se dopunjuju pravila za akreditaciju

certifikacijskih tijela u normi EN-ISO/IEC 17065/2012 te u kriterijima certificiranja koje je odobrilo nadležno nadzorno tijelo ili Odbor. Certifikat, pečat ili oznaka na temelju Opće uredbe o zaštiti podataka mogu se izdati samo nakon neovisne ocjene dokaza koju provodi akreditirano certifikacijsko tijelo ili nadležno nadzorno tijelo u i kojoj se navodi da su ispunjeni kriteriji certificiranja.

19. U tablici je prikazan opći primjer postupka certificiranja.

Voditelj ili izvršitelj obrade podnose zahtjev	Formalna provjera koju provodi certifikacijsko tijelo	Ocjenjivanje Predevaluacija	Ocjenjivanje Evaluacija predmeta evaluacije	Ocjenjivanje Potvrđivanje rezultata	Informacije namijenjene nadležnom nadzornom tijelu	Certificiranje	Praćenje	Obnavljanje certifikata
Je li opis predmeta evaluacije jednoznačan i potpun, uključujući sučelja?	Može li se prihvatiti opis predmeta evaluacije?	Koji se kriteriji primjenjuju?	Ispunjava li predmet evaluacije kriterije?	Jesu li određeni svi relevantni kriteriji koji se odražavaju na predmet evaluacije?	Jesu li navedeni razlozi za dodjeljivanje ili povlačenje certifikacije?	Može li se izdati certifikat?	Ispunjava li predmet evaluacije i dalje relevantne kriterije?	Ispunjava li obrada još uvijek kriterije certificiranja?
Može li se odobriti pristup aktivnostima obrade u slučaju predmeta evaluacije?	Jesu li svi dokumenti potpuni i ažurirani?	Koje se metode evaluacije primjenjuju?	Je li dokumentacija za predmet evaluacije ispravna?	Je li evaluacija u dovoljnoj mjeri dokumentirana?		Jesu li izvješća spremna za objavljivanje?	Koristi li se certifikat / pečat / oznaka pouzdanosti na ispravan način?	Jesu li pitanja u kojima je došlo do promjena riješena na zadovoljavajući način?
Čl. 42. st. 6.	Čl. 43. st. 4.	Čl. 43. st. 4.	Čl. 42. st. 5., čl. 43. st. 4.	Čl. 43. st. 4.	Čl. 43. st. 1. i 5.	Čl. 43. st. 1., čl. 42. st. 7.	Čl. 42. st. 7.	Čl. 42. st. 7.

2 ULOGA NADZORNIH TIJELA

20. U članku 42. stavku 5. propisuje se da certifikat izdaje akreditirano certifikacijsko tijelo ili nadležno nadzorno tijelo. Općom uredbom o zaštiti podataka ne propisuje se da je izdavanje certifikata obvezna zadaća nadzornih tijela. Umjesto toga, tom se uredbom dopušta niz različitih modela. Primjerice, nadzorno tijelo može se odlučiti za jednu od sljedećih opcija ili više njih:

- može samo izdavati certifikate na temelju vlastitog programa certificiranja,
- može samo izdavati certifikate na temelju vlastitog programa certificiranja, ali pritom može, u potpunosti ili djelomično, trećim stranama delegirati provođenje postupka ocjenjivanja,
- može izraditi vlastiti program certificiranja te povjeriti postupak certificiranja certifikacijskim tijelima koja izdaju certifikate i
- poticati razvoj mehanizama certificiranja na tržištu.

21. Nadzorno tijelo morat će razmotriti i svoju ulogu s obzirom na odluke o mehanizmima akreditiranja donesene na nacionalnoj razini, osobito ako je samo nadzorno tijelo ovlašteno za akreditaciju certifikacijskih tijela u skladu s člankom 43. stavkom 1. Opće uredbe o zaštiti podataka. Stoga će svako nadzorno tijelo odrediti koji će pristup primijeniti kako bi se ostvarila opća svrha certificiranja na temelju Opće uredbe o zaštiti podataka. To će se utvrditi ne samo u kontekstu zadaća i ovlasti iz članaka 57. i 58., nego i pri vođenju računa o certificiranju kao čimbeniku koji je potrebno uzeti u obzir pri određivanju upravnih novčanih kazni te općenitije kao sredstvu za dokazivanje sukladnosti.

2.1 Nadzorno tijelo kao certifikacijsko tijelo

22. Ako nadzorno tijelo odabere provoditi certificiranje morat će pažljivo procijeniti svoju ulogu s obzirom na zadaće koje su mu dodijeljene na temelju Opće uredbe o zaštiti podataka. Njegova uloga u izvršavanju svojih funkcija trebala bi biti transparentna. Morat će posebno razmotriti pitanja podjele ovlasti koje se odnose na istrage i provedbu kako bi se izbjegli bilo kakvi potencijalni sukobi interesa.

23. Kad djeluje kao certifikacijsko tijelo, nadzorno tijelo morat će osigurati ispravno uspostavljanje mehanizma certificiranja te izraditi ili donijeti vlastite kriterije certificiranja. Osim toga, svako nadzorno tijelo koje izdaje certifikate ima zadaću da ih periodično preispituje (članak 57. stavak 1. točka (o)) te ovlast da ih povuče ako nisu ispunjeni zahtjevi za certificiranje ili ako oni više nisu ispunjeni (članak 58. stavak 2. točka (h)). Kako bi se ti zahtjevi ispunili, korisno je uspostaviti postupak certificiranja i postupovne zahtjeve te, ako npr. nacionalnim pravom nije drugačije propisano, uspostaviti pravno provediv sporazum o pružanju aktivnosti certificiranja s pojedinačnom organizacijom koja podnosi zahtjev. Trebalo bi osigurati da se u tom sporazumu o certificiranju od podnositelja zahtjeva zahtijeva da bude usklađen barem s kriterijima certificiranja, uključujući neophodne aranžmane za provođenje evaluacije, praćenje pridržavanja kriterija i periodično preispitivanje, među ostalim pristup informacijama i/ili poslovnim prostorima, dokumentaciju i objavljivanje izvješća i rezultata te istrage povodom pritužbi. Nadalje, očekuje se da će se nadzorno tijelo, osim zahtjeva u skladu s člankom 43. stavkom 2., pridržavati i zahtjeva iz smjernica za akreditaciju certifikacijskih tijela.

2.2 Dodatne zadaće nadzornog tijela u pogledu certificiranja

24. U državama članicama u kojima certifikacijska tijela postanu aktivna, nadzorno tijelo, neovisno o vlastitim aktivnostima, ima ovlast i zadaću da:

    - ocjenjuje kriterije iz programa certificiranja i izrađuje nacrt odluke (članak 42. stavak 5.)
    - dostavi nacrt odluke Odboru kada namjerava odobriti kriterije certificiranja (članak 64. stavak 1. točka (c) i članak 64. stavak 7.) i razmotri mišljenje Odbora (članak 64. stavak 1. točka (c) i članak 70. stavak 1. točka (t)),
    - odobrava kriterije certificiranja (članak 58. stavak 3. točka (f)) prije provođenja akreditiranja i certificiranja (članak 42. stavak 5. i članak 43. stavak 2. točka (b)),

- objavljuje kriterije certificiranja (članak 43. stavak 6.),
- djeluje kao nadležno tijelo za programe certificiranja na razini EU-a iz kojih mogu proizaći europski pečati za zaštitu podataka koje je odobrio Europski odbor za zaštitu podataka (članak 42. stavak 5. i članak 70. stavak 1. točka (o)) i
- naredi sljedeće certifikacijskom tijelu: (a) da ne izda certifikat ili (b) da povuče certifikat ako zahtjevi za certificiranje (postupci ili kriteriji certificiranja) nisu ispunjeni ili više nisu ispunjeni (članak 58. stavak 2. točka (h)).

25. Na temelju Opće uredbe o zaštiti podataka nadzorno tijelo ima zadaću odobravanja kriterija certificiranja, ali ne i zadaću izrade tih kriterija. Kako bi odobrilo kriterije certificiranja na temelju članka 42. stavka 5., nadzorno tijelo trebalo bi dobro razumjeti ono što se može očekivati, osobito u smislu opsega i sadržaja za dokazivanje sukladnosti s Općom uredbom o zaštiti podataka i s obzirom na svoju zadaću praćenja i provođenja primjene te uredbe. U Prilogu se daju smjernice za osiguravanje usklađenog pristupa u ocjenjivanju kriterija za potrebe davanja odobrenja.

26. U članku 43. stavku 1. zahtijeva se da certifikacijska tijela obavijeste svoje nadzorno tijelo prije izdavanja ili obnavljanja certifikata kako bi se nadležnom nadzornom tijelu omogućilo izvršavanje njegovih korektivnih ovlasti iz članka 58. stavka 2. točke (h). Osim toga, u članku 43. stavku 5. od certifikacijskih se tijela zahtijeva i da nadležnom nadzornom tijelu navedu razloge za davanje ili povlačenje zatraženog certifikata. Iako se Općom uredom o zaštiti podataka nadzornim tijelima dopušta da odrede način na koji će u operativnom smislu zaprimati, potvrđivati i preispitivati te informacije i postupati s njima (primjerice, to bi moglo uključivati tehnološka rješenja koja omogućuju izvješćivanje koje provode certifikacijska tijela), moguće je uvođenje postupka i kriterija obrade informacija i izvješća koji su dostavljeni u slučaju svakog uspješnog projekta certificiranja koje je provelo certifikacijsko tijelo u skladu s člankom 43. stavkom 1. Na temelju tih informacija nadzorno tijelo može izvršiti svoju ovlast naređivanja certifikacijskom tijelu da povuče ili da ne izda certifikat (članak 58. stavak 2. točka (h)) te praćenja i provođenja primjene zahtjeva za certificiranje i kriterija certificiranja na temelju Opće uredbe o zaštiti podataka (članak 57. stavak 1. točka (a) i članak 58. stavak 2. točka (h)). Time će se podupirati usklađeni pristup i usporedivost u certificiranju koje provode različita certifikacijska tijela te će se osigurati da nadzorna tijela imaju informacije o certifikacijskom statusu određene organizacije.

3 ULOGA CERTIFIKACIJSKOG TIJELA

27. Certifikacijsko tijelo izdaje, preispituje, obnavlja i povlači certifikate (članak 42. stavci 5. i 7.) na temelju mehanizma certificiranja i odobrenih kriterija (članak 43. stavak 1.). Time se od certifikacijskog tijela ili vlasnika programa certificiranja zahtijeva da odredi i uspostavi kriterije certificiranja i postupke certificiranja, uključujući postupke za praćenje pridržavanja, preispitivanje, postupanje povodom pritužbi i povlačenje. Kriteriji certificiranja preispituju se

u okviru postupka akreditacije, tijekom kojeg se razmatraju pravila i postupci na temelju kojih se izdaju certifikati, pečati ili oznake (članak 43. stavak 2. točka (c)).

28. Postojanje mehanizma certificiranja i kriterija certificiranja neophodno je za akreditaciju certifikacijskog tijela na temelju članka 43. Velik učinak na ono čime se certifikacijsko tijelo bavi proizlazi iz opsega i vrste kriterija certificiranja, koji utječu na postupke certificiranja i obrnuto. Za određene kriterije mogu se, primjerice, zahtijevati određene metode evaluacije, kao što su inspekcije na terenu i preispitivanje kodeksa. Ti su postupci obvezni za akreditiranje te su dodatno objašnjeni u smjernicama o akreditiranju.

29. Od certifikacijskog se tijela na temelju Opće uredbe o zaštiti podataka zahtijeva da nadzornim tijelima dostavlja informacije, osobito o pojedinačnim certificiranjima, koje su potrebne za praćenje primjene mehanizma certificiranja (članak 42. stavak 7., članak 43. stavak 5., članak 58. stavak 2. točka (h)).

4 ODOBRAVANJE KRITERIJA CERTIFICIRANJA

30. Kriteriji certificiranja integralni su dio svakog mehanizma certificiranja. Stoga se u Općoj uredbi o zaštiti podataka zahtijeva da kriterije za mehanizam certificiranja odobri nadležno nadzorno tijelo (članak 42. stavak 5. i članak 43. stavak 2. točka (b)) dok, u slučaju Europskog pečata za zaštitu podataka, kriterije certificiranja odobrava Europski odbor za zaštitu podataka (članak 42. stavak 5. i članak 70. stavak 1. točka (o)). Oba postupka za odobravanje kriterija certificiranja objašnjena su u nastavku.

31. Europski odbor za zaštitu podataka priznaje sljedeće svrhe u koje se odobravaju kriteriji certificiranja:

    - kako bi se ispravno odražavali zahtjevi i načela u pogledu zaštite pojedinaca u vezi s obradom osobnih podataka koji su utvrđeni u Uredbi (EU) 2016/679 i
    - kako bi se pridonijelo dosljednoj primjeni Opće uredbe o zaštiti podataka.

32. Odobrenje se daje na temelju zahtjeva iz Opće uredbe o zaštiti podataka prema kojemu se mehanizam certificiranja, koji voditeljima obrade i izvršiteljima obrade omogućuje dokazivanje sukladnosti s Općom uredbom o zaštiti podataka, u potpunosti odražava u kriterijima certificiranja.

4.1 Odobravanje kriterija koje provodi nadležno nadzorno tijelo

33. Kriterije certificiranja mora odobriti nadležno nadzorno tijelo prije ili tijekom postupka akreditacije certifikacijskog tijela. Odobrenje je potrebno i u slučaju ažuriranih ili dodatnih programa ili skupova kriterija istog certifikacijskog tijela na temelju norme ISO 17065, prije primjene izmijenjenih mehanizama certificiranja (članak 42. stavak 5. i članak 43. stavak 2. točka (b)). Nadzorna tijela sa svim zahtjevima za odobrenje kriterija certificiranja postupaju na pravedan i nediskriminirajući način, u skladu s javno dostupnim postupkom u kojem se određuju opći uvjeti koji se trebaju ispuniti i opis postupka odobravanja.

34. Certifikacijsko tijelo može izdavati certifikate samo u određenoj državi članici u skladu s kriterijima koje je odobrilo nadzorno tijelo u toj državi članici. Drugim riječima, ako

certifikacijsko tijelo namjerava nuditi certificiranje i ako dobije akreditaciju, kriterije certificiranja mora odobriti nadležno nadzorno tijelo. Za programe certificiranja na europskoj razini vidjeti odjeljak u nastavku.

4.2 Odobravanje kriterija za Europski pečat za zaštitu podataka koje provodi Europski odbor za zaštitu podataka

35. Certifikacijsko tijelo može izdavati i certifikate za Europski pečat za zaštitu podataka u skladu s kriterijima koje je odobrio Europski odbor za zaštitu podataka. Iz kriterija certificiranja koje je odobrio Odbor u skladu s člankom 63. može proizaći Europski pečat za zaštitu podataka (članak 42. stavak 5.). S obzirom na postojeće konvencije o certificiranju i akreditiranju, Odbor potvrđuje da je poželjno izbjeći fragmentiranje tržišta certifikata za zaštitu podataka. Odbor napominje da se u članku 42. stavku 1. propisuje da države članice, nadzorna tijela, Odbor i Komisija potiču uspostavu mehanizama certificiranja, osobito na razini Unije.

4.2.1 Zahtjev za odobrenje

36. Zahtjev za odobrenje kriterija, koji u skladu s člankom 42. stavkom 5. i člankom 70. stavkom 1. točkom (o) odobrava Odbor, mora se podnijeti preko nadležnog nadzornog tijela i u njemu treba navesti namjeru vlasnika programa, kandidata za akreditaciju ili akreditiranog certifikacijskog tijela da nudi kriterije iz mehanizma certificiranja koji je namijenjen voditeljima i izvršiteljima obrade u svim državama članicama. Nadležno nadzorno tijelo dostavit će Odboru nacrt odluke ako smatra da bi Odbor mogao odobriti te kriterije.

37. Izbor mjesta podnošenja zahtjeva za odobrenje kriterija temeljit će se na lokaciji sjedišta vlasnika programa certificiranja ili certifikacijskih tijela.

38. Ako zahtjev podnosi certifikacijsko tijelo, ono će obično biti u postupku podnošenja zahtjeva za akreditaciju ili će već imati akreditaciju koju je izdalo nadležno nadzorno tijelo ili nacionalno akreditacijsko tijelo iz njegove države članice. Ako je certifikacijsko tijelo već akreditirano za mehanizam certificiranja na temelju Opće uredbe o zaštiti podataka, to može pojednostavniti postupak odobravanja.

4.2.2 Kriteriji za Europski pečat za zaštitu podataka

39. Europski odbor za zaštitu podataka koordinirat će postupak ocjenjivanja i odobriti kriterije za Europski pečat za zaštitu podataka kako se zahtijeva. Pri ocjenjivanju se vodi računa o pitanjima kao što su opseg kriterija i mogućnost da oni služe kao zajednička certifikacija. Ako Odbor odobri te kriterije, očekuje se da nadzorno tijelo koje je nadležno za sjedište tog certifikacijskog tijela u EU-u postupa povodom pritužbi o samom mehanizmu te da obavijesti ostala nadzorna tijela. To nadzorno tijelo ujedno je nadležno i za poduzimanje mjera protiv tog certifikacijskog tijela. Ovisno o slučaju, nadležno nadzorno tijelo obavijestit će ostala nadzorna tijela i Europski odbor za zaštitu podataka.

40. Kriteriji certificiranja koji se odnose na zajedničko certificiranje podliježu zahtjevima iz cijelog EU-a pa bi trebali imati poseban mehanizam kako bi se mogli nositi s tim zahtjevima. Europski mehanizmi certificiranja moraju biti namijenjeni za primjenu u svim državama članicama. Mehanizam za Europski pečat za zaštitu podataka, koji se temelji na članku 42. stavku 5., te njegovi kriteriji moraju se, prema potrebi, moći prilagoditi nacionalnim propisima koji su specifični za određeni sektor, npr. za obradu podataka u školama, te moraju predviđati primjenu na razini cijelog EU-a.

41. Primjer: međunarodna škola koja nudi školovanje ispitanicima u Uniji smještena je u državi članici „A". Škola želi svoj postupak za prijavu preko interneta certificirati s pomoću programa certificiranja na razini cijelog EU-a kako bi dobila Europski pečat za zaštitu podataka. Ta škola namjerava podnijeti zahtjev za certificiranje postupaka obrade koje nudi certifikacijsko tijelo s poslovnim nastanom u državi članici „B" na temelju Europskog pečata za zaštitu podataka. Kriterijima za taj pečat koji su osmišljeni i dokumentirani u okviru relevantnog mehanizma moraju se moći uzeti u obzir propisi za škole koji se primjenjuju u državi članici „A". Tim kriterijima trebalo bi se zahtijevati i da se u okviru postupka te škole za prijavu preko interneta pružaju informacije i vodi računa o primjenjivim zahtjevima za zaštitu podataka u toj državi članici, koji se mogu razlikovati od onih u drugim državama članicama. Primjer su za to skupovi osobnih podataka koje treba dostaviti za potrebe prijave, npr. ocjene iz vrtića ili rezultati testiranja, različiti rokovi čuvanja podataka, prikupljanje ili obrada financijskih ili biometrijskih podataka, ograničenja u pogledu daljnje obrade.

    - Kriteriji visoke razine za odobrenje mehanizma Europskog pečata za zaštitu podataka uključuju:
        - kriterije koje je odobrio Odbor,
        - primjenu u različitim jurisdikcijama pri čemu se, prema potrebi, poštuju odgovarajući nacionalni pravni zahtjevi i propisi koji su specifični za određeni sektor,
        -
    - usklađene kriterije koji se mogu prilagoditi kako bi odražavali nacionalne zahtjeve,
        - opis mehanizma certificiranja u kojemu se određuju:
        - sporazumi o certificiranju, kojima se priznaju paneuropski zahtjevi,
        - postupci za osiguravanje i pružanje rješenja za nacionalne različitosti i osiguravanje da Pečat pomaže u dokazivanju sukladnosti s Općom uredbom o zaštiti podataka i
        - jezik izvješća koja su namijenjena svim nadzornim tijelima na koje se određeni slučaj odnosi.

42. U Prilogu se nalaze i savjeti o kriterijima za Europski pečat za zaštitu podataka.

4.2.3 Uloga akreditiranja

43. Kako je navedeno u odjeljku 4.2.1., kad se utvrdi da su kriteriji prikladni za zajedničku certifikaciju te ih je Odbor kao takve odobrio u skladu s člankom 42. stavkom 5., tada se certifikacijska tijela mogu akreditirati za provođenje certifikacije na temelju tih kriterija na razini Unije.

44. Programi koji su namijenjeni da ih se nudi samo u određenim državama članicama neće biti kandidati za pečate EU-a. Akreditacija za područje primjene Europskog pečata za zaštitu podataka zahtijevat će akreditiranje u državi članici u kojoj je sjedište certifikacijskog tijela koje namjerava upravljati tim programom, tj. koje je odgovorno za izdavanje certifikata i upravljanje aktivnostima certificiranja svojih subjekata i društava kćeri u drugim državama članicama. Ako drugi poslovni nastani ili uredi autonomno upravljaju certificiranjem i autonomno izvršavaju certificiranje, za svaki od tih poslovnih nastana ili ureda bit će potrebna posebna akreditacija u državi članici u kojoj se nalaze. Drugim riječima, akreditacija je potrebna samo u državi članici u kojoj se nalazi sjedište certifikacijskog tijela samo ako to sjedište jedino izdaje certifikate. Za razliku od toga, ako drugi poslovni nastani certifikacijskog tijela isto izdaju certifikate, potrebno je akreditirati i te poslovne nastane.

45. Stoga, ako certifikacijsko tijelo nije akreditirano za certificiranje na temelju Europskog pečata za zaštitu podataka, ne mogu se koristiti kriteriji koje je odobrio Odbor i ne može se nuditi Pečat.

5 IZRADA KRITERIJA CERTIFICIRANJA

46. Općom uredbom o zaštiti podataka uspostavljen je okvir za izradu kriterija certificiranja. Dok su temeljni zahtjevi za postupak certificiranja utvrđeni u člancima 42. i 43. uz istodobno propisivanje bitnih kriterija postupaka certificiranja, temelj za kriterije certificiranja mora se izvesti iz načela i pravila Opće uredbe o zaštiti podataka i mora pomoći u pružanju jamstva da su oni ispunjeni.

47. Pri izradi kriterija certificiranja naglasak bi trebalo staviti na provjerljivost, važnost i primjerenost kriterija certificiranja za dokazivanje sukladnosti s Uredbom. Kriteriji certificiranja trebali bi se formulirati tako da budu jasni i razumljivi te da je moguća njihova praktična primjena.

48. Pri izradi kriterija certificiranja, prema potrebi se, među ostalim, uzimaju u obzir sljedeći aspekti sukladnosti kojima se podupire ocjenjivanje postupka obrade:

    - zakonitost obrade u skladu s člankom 6.,
    - načela obrade podataka u skladu s člankom 5.,
    - prava ispitanika u skladu s člancima od 12. do 23.,
    - obveza izvješćivanja o povredi podataka u skladu s člankom 33.,
    - obveza tehničke i integrirane zaštite podataka, u skladu s člankom 25.,
    - je li provedena procjena učinka na zaštitu podataka, u skladu s člankom 35. stavkom 7. točkom (d), ako je primjenjivo i

- jesu li uspostavljene tehničke i organizacijske mjere u skladu s člankom 32.

49. Mjera u kojoj se ta razmatranja odražavaju u kriterijima može se razlikovati ovisno o opsegu certificiranja, koje može uključivati vrste postupaka obrade i područje (npr. zdravstveni sektor) certificiranja.

5.1 Što se može certificirati na temelju Opće uredbe o zaštiti podataka?

50. Europski odbor za zaštitu podataka smatra da se Općom uredbom o zaštiti podataka predviđa široko područje primjene u pogledu onoga što se može certificirati na temelju te uredbe sve dok je naglasak stavljen na pomaganje u dokazivanju da su postupci obrade koje provode voditelji i izvršitelji obrade u skladu s tom uredbom (članak 42. stavak 1.).

51. Pri ocjenjivanju postupka obrade, u obzir se, ako je primjenjivo, moraju uzeti sljedeće tri ključne sastavnice:

    1. osobni podaci (glavno područje primjene Opće uredbe o zaštiti podataka);
    2. tehnički sustavi – infrastruktura, kao što su računalna oprema i računalni programi koji se koriste za obradu osobnih podataka i
    3. procesi i postupci koji se odnose na postupke obrade.

52. Za svaku se sastavnicu koja se koristi u postupcima obrade mora provesti ocjenjivanje na temelju utvrđenih kriterija. Na to mogu utjecati najmanje četiri različita značajna čimbenika: 1. organizacijska i pravna struktura voditelja ili izvršitelja obrade; 2. odjel, okruženje i osobe uključene u postupke obrade; 3. tehnički opis elemenata koje treba ocijeniti i konačno 4. informatička infrastruktura koja podržava postupak obrade, uključujući operativne sustave, virtualne sustave, baze podataka, sustave za autentifikaciju i autorizaciju, usmjerivače i vatrozide, sustave za pohranu podataka, komunikacijsku infrastrukturu ili pristup internetu te s njima povezane tehničke mjere.

53. Sve tri ključne sastavnice relevantne su za osmišljavanje postupaka i kriterija certificiranja. Mjera u kojoj se one uzimaju u obzir može se razlikovati ovisno o predmetu certificiranja. Primjerice, u nekim se slučajevima neke sastavnice mogu zanemariti ako se smatra da nisu relevantne za predmet certificiranja.

54. Kako bi se dodatno odredilo što se može certificirati na temelju Opće uredbe o zaštiti podataka, u Uredbi se nalaze dodatne smjernice. Iz članka 42. stavka 7. proizlazi da se certifikati na temelju te uredbe izdaju samo voditeljima i izvršiteljima obrade, što, primjerice, isključuje mogućnost certificiranja službenika za zaštitu podataka. U članku 43. stavku 1. točki (b) upućuje se na normu ISO 17065 kojom se uređuje akreditacija certifikacijskih tijela koja ocjenjuju sukladnost proizvoda, usluga i procesa. Iz postupka ili skupa postupaka obrade može proizaći proizvod ili usluga prema terminologiji iz norme ISO 17065 te oni mogu biti predmetom certificiranja. Primjerice, obrada podataka o zaposlenicima za potrebe isplate plaća ili upravljanja dopustima skup je postupaka u smislu Opće uredbe o zaštiti podataka te iz njega može proizaći proizvod ili usluga prema terminologiji iz norme ISO.

55. Na temelju tih razmatranja, Europski odbor za zaštitu podataka smatra da je područje primjene certificiranja na temelju Uredbe usmjereno na postupke ili skupove postupaka obrade. Oni se mogu sastojati od postupaka upravljanja u smislu organizacijskih mjera, što ih čini integralnim dijelom postupka obrade (npr. postupak upravljanja koji je uspostavljen za potrebe postupanja povodom pritužbi u okviru obrade podataka o zaposlenicima za potrebe isplate plaća).

56. Kako bi se ocijenila sukladnost postupka obrade s kriterijima certificiranja, mora se navesti slučaj njegove primjene. Primjerice, sukladnost primjene tehničke infrastrukture koja se koristi u postupku obrade ovisi o kategorijama podataka za čiju je obradu osmišljena. Organizacijske mjere ovise o kategorijama i količini podataka te o tehničkoj infrastrukturi koja se koristi za obradu, uzimajući u obzir prirodu, opseg, sadržaj i svrhe obrade te rizike za prava i slobode ispitanika.

57. Nadalje, mora se imati na umu da se informatičke aplikacije mogu znatno razlikovati čak i ako služe istim svrhama obrade. Stoga se to mora uzeti u obzir pri utvrđivanju opsega mehanizama certificiranja i pri izradi kriterija certificiranja, tj. opseg certificiranja i kriterija ne bi trebao biti toliko uzak da se time isključe informatičke aplikacije koje su drugačije osmišljene.

5.2 Određivanje predmeta certificiranja

58. Opseg mehanizma certificiranja treba razlikovati od predmeta certificiranja – koji se naziva i predmetom evaluacije – u pojedinačnim projektima certificiranja u okviru mehanizma certificiranja. Opseg mehanizma certificiranja može se definirati općenito ili u odnosu na određenu vrstu ili određeno područje postupaka obrade pa se stoga već time mogu utvrditi predmeti certificiranja koji su obuhvaćeni opsegom mehanizma certificiranja (npr. sigurna pohrana i zaštita osobnih podataka koji se nalaze u digitalnom sefu). U svakom slučaju, pouzdano, smisleno ocjenjivanje sukladnosti može se provesti samo ako se precizno opiše pojedinačni predmet projekta certificiranja. Moraju se jasno opisati postupci obrade koji su uključeni u predmet certificiranja, a zatim i ključne sastavnice, tj. koji će se podaci, procesi i tehnička infrastruktura ocjenjivati, a koji se neće ocjenjivati. Pritom se uvijek moraju uzeti u obzir sučelja s drugim procesima te i njih treba opisati. Jasno, ono što nije poznato ne može biti dio ocjenjivanja pa se stoga ne može ni certificirati. U svakom slučaju, pojedinačni predmet certificiranja mora biti smislen s obzirom na poruku ili tvrdnju koja je iznesena u certifikatu te se njome ne bi trebalo zavaravati korisnika, klijenta ili potrošača.

59. [Primjer 1.]

    Banka svojim klijentima nudi internetske stranice za potrebe internetskog bankarstva. U okviru te usluge mogu se provoditi prijenosi sredstava, kupovati dionice, pokretati trajni nalozi i upravljati računom. Banka na temelju mehanizma certificiranja zaštite podataka s općim opsegom koji se temelji na generičkim kriterijima želi certificirati sljedeće:

    a) sigurnu prijavu

Sigurna prijava postupak je obrade koji je razumljiv krajnjem korisniku i koji je relevantan iz perspektive zaštite podataka jer ima važnu ulogu u jamčenju sigurnosti osobnih podataka koji se pritom koriste. Stoga je taj postupak obrade neophodan za sigurnu prijavu te stoga može biti smislen predmet evaluacije ako se na certifikatu jasno navodi da je certificiran samo postupak obrade za potrebe prijave.

b) *web*-sučelje

Iako *web*-sučelje može biti relevantno iz perspektive zaštite podataka, ono nije razumljivo krajnjem korisniku pa stoga ne može biti smislen predmet evaluacije. Osim toga, korisniku nije jasno koje su usluge na internetskim stranicama, a time i postupci obrade, obuhvaćene tim certifikatom.

c) internetsko bankarstvo

Web-sučelje zajedno s pozadinskim sustavom postupci su obrade koji se pružaju u okviru usluge internetskog bankarstva i koji mogu biti smisleni korisniku. U tom se kontekstu oba ta postupka moraju uključiti u predmet evaluacije, dok se postupci obrade koji nisu izravno povezani s pružanjem usluge internetskog bankarstva, kao što su postupci obrade za potrebe sprečavanja pranja novca, mogu isključiti iz predmeta evaluacije.

Međutim, usluge internetskog bankarstva koje banka nudi putem svojih internetskih stranica mogu uključivati i druge usluge za koje su pak potrebni posebni postupci obrade. U tom kontekstu, druge usluge mogu uključivati, primjerice, ponudu proizvoda osiguranja. Budući da ta dodatna usluga nije izravno povezana sa svrhom pružanja usluga internetskog bankarstva, može se isključiti iz predmeta evaluacije. Ako se ta dodatna usluga (osiguranje) isključi iz predmeta evaluacije, sučelja za tu uslugu koja su integrirana u internetske stranice dio su predmeta evaluacije pa se stoga moraju opisati kako bi se te usluge jasno razlikovalo. Takav je opis neophodan za utvrđivanje i evaluaciju mogućeg protoka podataka između tih dviju usluga.

60. [Primjer 2.]

Banka svojim klijentima nudi uslugu kojom im omogućuje da objedine informacije koje se odnose na različite račune i kreditne kartice iz više banaka (objedinjavanje računa). Ta banka želi certificirati svoju uslugu na temelju Opće uredbe o zaštiti podataka. Nadležno nadzorno tijelo odobrilo je konkretan skup kriterija certificiranja koji su usmjereni na tu vrstu aktivnosti. Opsegom mehanizma certificiranja obuhvaćeni su samo sljedeći aspekti sukladnosti:

- autentifikacija korisnika i
- prihvatljivi načini za dobivanje podataka iz drugih banaka/usluga koje treba objediniti.

Budući da je predmet evaluacije sam po sebi definiran opsegom tog mehanizma certificiranja, nije moguće na smislen način suziti predmet evaluacije na temelju predloženog opsega i certificirati samo određene značajke ili samo jednu aktivnost obrade. U tom scenariju, predmet evaluacije mora biti jednak odgovarajućem opsegu.

5.3 Metode evaluacije i metodologija ocjenjivanja

61. Za ocjenjivanje sukladnosti radi pomaganja u dokazivanju sukladnosti postupaka obrade potrebno je utvrditi i odrediti metode za evaluaciju i metodologiju ocjenjivanja. Važno je jesu li informacije za ocjenjivanje prikupljene samo iz dokumentacije (što samo po sebi ne bi bilo dovoljno) ili su aktivno prikupljene na terenu i izravnim ili neizravnim pristupom. Način prikupljanja informacija utječe na značaj certificiranja pa bi ga stoga trebalo utvrditi i opisati.

    Postupci za izdavanje i periodično preispitivanje certifikata trebali bi uključivati specifikacije za utvrđivanje primjerene razine evaluacije (dubine i granularnosti) kako bi se ispunili kriteriji certificiranja te bi trebali uključivati:

    - informacije o primijenjenim metodama ocjenjivanja i specifikacije tih metoda te prikupljene nalaze, npr. tijekom revizija na terenu ili iz dokumentacije,
    - metode evaluacije kod kojih se naglasak stavlja na postupke obrade (podaci, sustavi, procesi) i svrhu obrade,
    - utvrđivanje kategorija podataka, potreba za zaštitom te informacije o uključenosti izvršitelja obrade ili trećih strana,
    - utvrđivanje uloga i postojanje mehanizma za kontrolu pristupa utvrđenog oko uloga i odgovornosti.

62. Dubina evaluacije utječe na značaj i vrijednost certificiranja. Smanjenjem dubine evaluacije iz pragmatičnih razloga ili radi smanjenja troškova, smanjit će se značaj certificiranja zaštite podataka. S druge strane, odlukama o granularnosti evaluacije mogu se premašiti financijske sposobnosti podnositelja zahtjeva, a često i sposobnost evaluatora i revizora. Za potrebe dokazivanja sukladnosti neće uvijek biti presudno postići vrlo detaljnu razinu analize korištenih informatičkih sustava kako bi to dokazivanje i dalje bilo smisleno.

5.4 Dokumentiranje ocjenjivanja

63. Dokumentacija o certificiranju trebala bi biti temeljita i sveobuhvatna. Nepostojanje dokumentacije znači da se ne može provesti ispravno ocjenjivanje. Bitna je funkcija dokumentacije o certificiranju ta što se njome osigurava transparentnost u postupku evaluacije na temelju mehanizma certificiranja. U dokumentaciji se nalaze odgovori na pitanja o zahtjevima koji su utvrđeni pravom. U okviru mehanizama certificiranja trebala bi se propisati standardizirana metodologija za dokumentiranje. Nakon toga evaluacijom će se omogućiti usporedba dokumentacije o certificiranju sa stvarnim stanjem na terenu i u odnosu na kriterije certificiranja.

64. Sveobuhvatna dokumentacija o tome što je certificirano i o primijenjenoj metodologiji služi u svrhu transparentnosti. U skladu s člankom 43. stavkom 2. točkom (c), mehanizmima certificiranja trebali bi se uspostaviti postupci koji omogućuju preispitivanje certifikata. Kako bi se nadzornom tijelu omogućilo da ocijeni može li se, i u kojoj mjeri, certificiranje priznati u službenim istragama, detaljna dokumentacija vjerojatno je najprikladnije sredstvo za

prenošenje informacija o tome. Stoga bi u dokumentaciji izrađenoj tijekom evaluacije naglasak trebao biti na trima glavnim aspektima:

- dosljednosti i usklađenosti primijenjenih metoda evaluacije,
- metodama evaluacije koje su usmjerene na dokazivanje sukladnosti predmeta certificiranja s kriterijima certificiranja, a time i s Uredbom i
- činjenici da je rezultate evaluacije potvrdilo neovisno i nepristrano certifikacijsko tijelo.

5.5 Dokumentiranje rezultata

65. U uvodnoj izjavi 100. navode se informacije o ciljevima koji se nastoje ostvariti uvođenjem certificiranja.

„Kako bi se povećala transparentnost i usklađenost s ovom Uredbom, trebalo bi se poticati uvođenje mehanizama certificiranja te pečata i oznaka za zaštitu podataka, što bi ispitanicima omogućilo brzu procjenu razine zaštite podataka za relevantne proizvode i usluge."

66. Dokumentiranje i prenošenje rezultata imaju važnu ulogu u povećanju transparentnosti. Certifikacijska tijela koja upotrebljavaju mehanizme certificiranja, pečate ili oznake usmjerene na ispitanike (u njihovim ulogama potrošača ili klijenata) trebala bi pružati lako dostupne, razumljive i smislene informacije o certificiranim postupcima obrade. Te bi javne informacije trebale uključivati barem sljedeće:

    - opis predmeta evaluacije,
    - upućivanje na odobrene kriterije koji su primijenjeni na određeni predmet evaluacije,
    - metodologiju za evaluaciju kriterija (evaluacija na terenu, dokumentacija itd.) i
    - informacije o trajanju valjanosti certifikata i
    - trebale bi omogućiti usporedivost rezultata nadzornim tijelima i javnosti.

6 SMJERNICE ZA UTVRĐIVANJE KRITERIJA CERTIFICIRANJA

67. Kriteriji certificiranja integralni su dio mehanizma certificiranja. Postupak certificiranja uključuje zahtjeve o načinu ocjenjivanja koje se provodi u pojedinačnim projektima certificiranja za određeni predmet evaluacije i zahtjeve o tome tko i u kojoj mjeri provodi to ocjenjivanje te koja se razina granularnosti ocjenjivanja zahtijeva. U okviru kriterija certificiranja nalaze se nominalni zahtjevi u odnosu na koje se ocjenjuje stvarni postupak obrade koji je utvrđen u predmetu evaluacije. U ovim se Smjernicama za utvrđivanje kriterija certificiranja daju općeniti savjeti s pomoću kojih će se olakšati ocjenjivanje kriterija certificiranja za potrebe dobivanja odobrenja.

- Pri odobravanju ili utvrđivanju kriterija certificiranja trebalo bi u obzir uzeti sljedeća opća razmatranja o kriterijima certificiranja:
- kriteriji certificiranja trebali bi biti ujednačeni i provjerljivi,
- trebala bi se moći provesti revizija kriterija certificiranja radi olakšavanja evaluacije postupaka obrade na temelju Opće uredbe o zaštiti podataka, navođenjem posebice ciljeva i provedbenih smjernica za postizanje tih ciljeva,
- kriteriji certificiranja trebali bi biti relevantni za ciljnu publiku (npr. među poduzećima (B2B) te između poduzeća i klijenata (B2C)),
- u okviru kriterija certificiranja trebalo bi se voditi računa o drugim normama te bi oni, prema potrebi, trebali biti interoperabilni s drugim normama (kao što su norme ISO ili norme na nacionalnoj razini) i
- kriteriji certificiranja trebali bi biti fleksibilni i prilagodljivi kako bi se mogli primijeniti na različite vrste i veličine organizacija, uključujući mikro, mala i srednja poduzeća u skladu s člankom 42. stavkom 1. i pristup koji se temelji na riziku u skladu s uvodnom izjavom 77.

68. Mala lokalna poduzeća, kao što su trgovine na malo, obično će provoditi postupke obrade koji su manje složeni nego u slučaju velikih multinacionalnih trgovina na malo. Iako su zahtjevi o zakonitosti postupaka obrade isti, potrebno je uzeti u obzir opseg obrade podataka i njezinu složenost. Iz toga proizlazi potreba za postojanjem mehanizama certificiranja čiji se kriteriji mogu prilagoditi u skladu s predmetnom aktivnošću obrade.

6.1 Postojeće norme

69. Certifikacijska tijela morat će razmotriti kako se u okviru određenih kriterija može voditi računa o postojećim relevantnim instrumentima, kao što su kodeksi ponašanja, tehničke norme ili nacionalne regulatorne i zakonske inicijative. U idealnom slučaju, kriteriji će biti interoperabilni s postojećim normama koje mogu pomoći voditelju ili izvršitelju obrade da ispuni svoje obveze na temelju Opće uredbe o zaštiti podataka. Međutim, dok je naglasak industrijskih normi često na sigurnosti organizacije i njezinoj zaštiti od prijetnji, Opća uredba o zaštiti podataka usmjerena je na zaštitu temeljnih prava pojedinaca. Ta različita perspektiva mora se uzeti u obzir pri osmišljavanju kriterija ili odobravanju kriterija ili mehanizama certificiranja koji se temelje na industrijskim normama.

6.2 Utvrđivanje kriterija

70. Kriteriji certificiranja moraju odgovarati certifikacijskoj izjavi (poruci ili tvrdnji) iz mehanizma ili programa certificiranja te biti u skladu s očekivanjima koja time nastaju. Moguće je da je nazivom mehanizma certificiranja već utvrđeno područje primjene te da će to imati posljedice na određivanje kriterija.

71. [Primjer 3.]

Područje primjene mehanizma koji se naziva „HealthPrivacyMark" (oznaka privatnosti u zdravstvu) trebalo bi biti ograničeno na zdravstveni sektor. Zbog naziva pečata može se zaključiti da su ispitani zahtjevi za zaštitu podataka u vezi sa zdravstvenim podacima. U skladu s time, kriteriji tog mehanizma moraju biti prikladni za ocjenjivanje zahtjeva za zaštitu podataka u tom sektoru.

72. [Primjer 4.]

    Za mehanizam koji se odnosi na certificiranje postupaka obrade koji uključuju sustave upravljanja u obradi podataka trebalo bi utvrditi kriterije koji omogućuju prepoznavanje i ocjenjivanje procesa upravljanja te njihovih popratnih tehničkih i organizacijskih mjera.

73. [Primjer 5.]

    U okviru kriterija za mehanizam koji se odnosi na računalstvo u oblaku potrebno je uzeti u obzir posebne tehničke zahtjeve koji su potrebni za korištenje uslugama koje se temelje na računalstvu u oblaku. Primjerice, ako se koriste poslužitelji izvan EU-a, u okviru tih kriterija moraju se uzeti u obzir uvjeti utvrđeni u poglavlju V. Opće uredbe o zaštiti podataka s obzirom na prijenose podataka trećim zemljama.

74. Kriteriji koji su osmišljeni kako bi bili prikladni za različite predmete evaluacije u različitim sektorima i/ili državama članicama trebali bi omogućiti primjenu u različitim scenarijima te omogućiti utvrđivanje odgovarajućih mjera koje su prikladne za male, srednje ili velike postupke obrade te odražavaju rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca u skladu s Općom uredbom o zaštiti podataka. Kao posljedica toga, postupci certificiranja (npr. za dokumentiranje, ispitivanje ili metodu i dubinu evaluacije) koji nadopunjuju te kriterije moraju odgovarati na te potrebe te omogućavati i imati pravila za, primjerice, primjenu relevantnih kriterija u pojedinačnim projektima certificiranja. Kriteriji moraju olakšavati ocjenjivanje toga jesu li osigurana dostatna jamstva za provedbu odgovarajućih tehničkih i organizacijskih mjera.

6.3 Vijek trajanja kriterija certificiranja

75. Iako kriteriji certificiranja moraju biti pouzdani tijekom duljeg vremena, oni ne bi trebali biti nepromjenjivi. Kriteriji podliježu reviziji, primjerice, u slučaju:

    - izmjene pravnog okvira,
    - tumačenja pojmova i odredbi u presudama Suda ili
    - promjena u tehničkim dostignućima.

Za Europski odbor za zaštitu podataka

Predsjednica

(Andrea Jelinek)

Doneseno

PRILOG 1.: ZADAĆE I OVLASTI NADZORNIH TIJELA U ODNOSU NA CERTIFICIRANJE U SKLADU S OPĆOM UREDBOM O ZAŠTITI PODATAKA

	Odredbe	Zahtjevi
Zadaće	Članak 43. stavak 6.	Zahtijeva se da nadzorno tijelo objavljuje kriterije iz članka 42. stavka 5. u lako dostupnom obliku i da ih prosljeđuje Odboru.
	Članak 57. stavak 1. točka (n)	Zahtijeva se da nadzorno tijelo odobrava kriterije certificiranja u skladu s člankom 42. stavkom 5.
	Članak 57. stavak 1. točka (o)	Propisuje se da nadzorno tijelo, prema potrebi (tj. ako izdaje certifikat), provodi periodično preispitivanje izdanih certifikata u skladu s člankom 42. stavkom 7.
	Članak 64. stavak 1. točka (c)	Zahtijeva se da nadzorno tijelo obavijesti Odbor o nacrtu odluke ako ona ima za cilj odobriti kriterije certificiranja iz članka 42. stavka 5.
Ovlasti	Članak 58. stavak 1. točka (c)	Propisuje se da nadzorno tijelo ima ovlast provoditi preispitivanje certifikata u skladu s člankom 42. stavkom 7.
	Članak 58. stavak 2. točka (h)	Propisuje se da nadzorno tijelo ima ovlast povući certifikat, certifikacijskom tijelu narediti da povuče certifikat ili certifikacijskom tijelu narediti da ne izda certifikat.
	Članak 58. stavak 3. točka (e)	Propisuje se da nadzorno tijelo ima ovlast akreditirati certifikacijska tijela.
	Članak 58. stavak 3. točka (f)	Propisuje se da nadzorno tijelo ima ovlast izdati certifikate i odobriti kriterije certificiranja.
	Članak 58. stavak 3. točka (e)	Propisuje se da nadzorno tijelo ima ovlast akreditirati certifikacijska tijela.
	Članak 58. stavak 3. točka (f)	Propisuje se da nadzorno tijelo ima ovlast izdati certifikate i odobriti kriterije certificiranja.

PRILOG 2.

1 UVOD

U Prilogu 2. daju se smjernice za preispitivanje i procjenu kriterija certificiranja u skladu s člankom 42. stavkom 5. U nastavku se utvrđuju teme koje će nadzorna tijela za zaštitu podataka i Europski odbor za zaštitu podataka razmotriti i primijeniti u svrhu odobrenja kriterija certificiranja za mehanizam certificiranja. Certifikacijska tijela i vlasnici programa koji žele izraditi i podnijeti kriterije na odobravanje trebali bi proučiti pitanja navedena u nastavku. Taj popis nije konačan, ali u njemu je naveden minimalan broj tema koje treba uzeti u obzir. Sva pitanja neće biti primjenjiva, no potrebno ih je uzeti u obzir pri izradi kriterija, a možda će biti potrebno i obrazložiti zašto kriteriji ne obuhvaćaju određene aspekte. Neka se pitanja ponavljaju, no kontekst je različit. Ove je smjernice potrebno uzeti u obzir u skladu s pravnim zahtjevima Opće uredbe o zaštiti podataka i, ako je primjenjivo, nacionalnog zakonodavstva.

2 OPSEG MEHANIZMA CERTIFICIRANJA I PREDMET EVALUACIJE

a. Je li opseg mehanizma certificiranja (za koji će se koristiti kriteriji zaštite podataka) jasno opisan?

b. Je li opseg mehanizma certificiranja relevantan ciljnoj publici i je li nedvosmislen?

- *Primjer: pečat pouzdanosti poduzeća ukazuje na to da je u cijelom poduzeću provedena revizija aktivnosti obrade, čak i ako samo određeni postupci obrade, npr. postupak plaćanja internetom, podliježu certificiranju. Opseg je stoga dvosmislen.*

c. Odražava li opseg mehanizma certificiranja sve relevantne aspekte postupaka obrade?

- *Primjer: oznaka privatnosti u zdravstvu mora uključivati sve podatke dobivene evaluacijom koji se odnose na zdravlje kako bi se ispunili zahtjevi iz članka 9.*

d. Dopušta li opseg mehanizma certificiranja smisleno certificiranje zaštite podataka uzimajući u obzir prirodu, sadržaj i rizik povezanih postupaka obrade?

- *Primjer: ako je opseg mehanizma certificiranja usredotočen samo na određene aspekte postupaka obrade, kao što je prikupljanje podataka, a ne na daljnju obradu, kao što je obrada u svrhu izrade oglašivačkih profila ili upravljanja pravima ispitanika, to ispitanicima nije korisno.*

e. Obuhvaća li opseg mehanizma certificiranja obradu osobnih podataka u relevantnoj zemlji primjene ili prekograničnu obradu i/ili prijenos?

f. Je li u kriterijima certificiranja dostatno opisano kako bi predmet evaluacije trebao biti definiran?

- *Primjer: pečat privatnosti s općim opsegom koji zahtijeva samo specifikaciju obrade podložne certificiranju ne bi pružio dovoljno jasne smjernice o tome kako utvrditi i opisati predmet evaluacije.*
- *Primjer: (poseban) opseg, pečat privatnosti za sigurnu pohranu osobnih podataka u digitalnom sefu trebao bi detaljno opisati zahtjeve za ispunjavanje kriterija tog opsega,*

npr. definirati digitalni sef, zahtjeve sustava te obvezne tehničke i organizacijske mjere. U tom slučaju opseg može jasno definirati predmet evaluacije.

(1) Zahtijevaju li kriteriji da predmet evaluacije obuhvaća utvrđivanje svih relevantnih postupaka obrade, prikaz protoka podataka i određivanje područja primjene predmeta evaluacije?

- *Primjer: opseg mehanizma certificiranja omogućava certificiranje postupaka obrade koje provode voditelji obrade u skladu s Općom uredbom o zaštiti podataka bez dodatnog preciziranja područja primjene (opći opseg). Kriteriji kojima se koristi mehanizam zahtijevaju da voditelj obrade koji podnosi zahtjev odredi ciljni postupak obrade u smislu vrsta podataka te korištenih sustava i postupaka.*

(2) Je li kriterijima propisano da podnositelj zahtjeva mora jasno navesti gdje započinje i završava obrada koja podliježe evaluaciji? Zahtijevaju li kriteriji da predmet evaluacije obuhvaća sučelja u koje međuovisni postupci obrade nisu uključeni kao dio predmeta evaluacije? Je li to obrazloženo na zadovoljavajući način?

- *Primjer: predmet evaluacije koji dovoljno detaljno opisuje postupak obrade internetske usluge, kao što su registracija korisnika, pružanje usluge, fakturiranje, bilježenje IP adresa te sučelja za korisnike i treće strane, ali ne udomljavanje poslužitelja (osim sporazuma o obradi te tehničkim i organizacijskim mjerama).*

g. Jamče li kriteriji da su (pojedinačni) predmeti evaluacije razumljivi ciljnoj publici, uključujući prema potrebi ispitanike?

3 OPĆI ZAHTJEVI

a. Jesu li svi relevantni pojmovi upotrebljeni u katalogu kriterija (tj. potpuni skup kriterija certificiranja) utvrđeni, objašnjeni i opisani?

b. Jesu li utvrđeni svi normativni izvori?

c. Definiraju li se u kriterijima odgovornosti, postupci i obrada u području zaštite podataka obuhvaćeni opsegom mehanizma certificiranja?

4 POSTUPAK OBRADE, ČLANAK 42. STAVAK 1.

Kad je riječ o opsegu mehanizma certificiranja (općem ili posebnom), jesu li sve relevantne sastavnice postupaka obrade (podaci, sustavi i postupci) obuhvaćene kriterijima?

a. Zahtijevaju li kriteriji utvrđivanje valjanih pravnih osnova za obradu u pogledu predmeta evaluacije?

b. Kad je riječ o predmetu evaluacije, navode li se u kriterijima sve faze obrade i čitav životni vijek podataka, uključujući brisanje i/ili anonimizaciju?

c. Kad je riječ o predmetu evaluacije, zahtijevaju li kriteriji prenosivost podataka?

d. Kad je riječ o predmetu evaluacije, omogućavaju li kriteriji utvrđivanje i uzimanje u obzir posebnih vrsta postupaka obrade, npr. automatiziranog donošenja odluka, izrade profila?

e. Kad je riječ o predmetu evaluacije, omogućavaju li kriteriji utvrđivanje posebnih kategorija podataka?

f. Omogućavaju li i zahtijevaju li kriteriji procjenu rizika pojedinačnih postupaka obrade te potreba za zaštitom prava i sloboda ispitanika?

g. Omogućavaju li i zahtijevaju li kriteriji da se rizici za prava i slobode pojedinaca na odgovarajući način uzmu u obzir?

…

5 ZAKONITOST OBRADE

a. Zahtijevaju li kriteriji da se, kad je riječ o svrsi obrade i potrebi za obradom, provjeri zakonitost pojedinačnih postupaka obrade?

b. Je li u kriterijima propisano da je potrebno provjeriti zahtjeve pravne osnove pojedinačnih postupaka obrade?

6 NAČELA, ČLANAK 5.

a. Jesu li kriterijima na odgovarajući način obuhvaćena sva načela zaštite podataka iz članka 5.?

b. Je li, u skladu s kriterijima, potrebno dokazati smanjenje količine podataka za pojedinačni predmet evaluacije?

…

7 OPĆE OBVEZE VODITELJA I IZVRŠITELJA OBRADE

a. Je li, u skladu s kriterijima, potrebno dostaviti dokaz o ugovorima sklopljenima među voditeljima i izvršiteljima obrade?

b. Podliježu li ti ugovori evaluaciji?

c. Jesu li u kriterijima u obzir uzete obveze voditelja obrade iz Poglavlja IV.?

d. Je li, u skladu s kriterijima, potrebno dostaviti dokaz o preispitivanju i ažuriranju tehničkih i organizacijskih mjera koje je proveo voditelj obrade u skladu s člankom 24. stavkom 1.?

e. Je li kriterijima propisano da je potrebno provjeriti je li organizacija procijenila da bi se, u skladu s člankom 24., trebao imenovati službenik za zaštitu podataka? Ispunjava li službenik za zaštitu podataka zahtjeve iz članaka od 37. do 39., ako je to relevantno?

f. Je li kriterijima propisano da je potrebno provjeriti evidenciju aktivnosti obrade u skladu s člankom 30. stavkom 5. i na odgovarajući način uzeti u obzir zahtjeve iz članka 30.?

8 PRAVA ISPITANIKA

a. Je li kriterijima na odgovarajući način obuhvaćeno pravo ispitanika na informacije i zahtijevaju li uspostavu odgovarajućih mjera?

b. Je li kriterijima propisano da ispitanici imaju odgovarajući ili čak veći pristup svojim podacima te kontrolu nad njima, uključujući prenosivost podataka?

c. Zahtijevaju li kriteriji uspostavu mjera kojima se omogućava intervencija u postupak obrade kako bi se zajamčila prava ispitanika i dopustili ispravci, brisanje ili ograničenja?

…

9 RIZICI ZA PRAVA I SLOBODE POJEDINACA

a. Omogućavaju li i zahtijevaju li kriteriji procjenu rizika za prava i slobode pojedinaca?

b. Navodi li se u kriterijima priznata metodologija procjene rizika ili zahtijeva li se u njima primjena takve metodologije? Je li ta metodologija prema potrebi razmjerna?

c. Omogućavaju li i zahtijevaju li kriteriji procjenu utjecaja predviđenih postupaka obrade na prava i slobode pojedinaca?

d. Zahtijevaju li kriteriji prethodno savjetovanje u vezi s preostalim rizicima koji se nisu mogli ublažiti, na temelju rezultata procjene učinka na zaštitu podataka?

10 TEHNIČKE I ORGANIZACIJSKE MJERE KOJIMA SE JAMČI ZAŠTITA

a. Zahtijevaju li kriteriji primjenu tehničkih i organizacijskih mjera kojima se osigurava povjerljivost postupaka obrade?

b. Zahtijevaju li kriteriji primjenu tehničkih i organizacijskih mjera kojima se osigurava cjelovitost postupaka obrade?

c. Zahtijevaju li kriteriji primjenu tehničkih i organizacijskih mjera kojima se osigurava dostupnost postupaka obrade?

d. Zahtijevaju li kriteriji primjenu mjera kojima se osigurava transparentnost postupaka obrade kad je riječ o sljedećem:

e. odgovornosti?

f. pravima ispitanika?

g. procjeni pojedinačnih postupaka obrade, npr. u smislu algoritamske transparentnosti?

h. Zahtijevaju li kriteriji primjenu tehničkih i organizacijskih mjera kojima se jamče prava ispitanika, npr. mogućnost pružanja informacija ili prenosivost podataka?

i. Zahtijevaju li kriteriji primjenu tehničkih i organizacijskih mjera kojima se omogućava intervencija u postupak obrade kako bi se zajamčila prava ispitanika i dopustili ispravci, brisanje ili ograničenja?

j. Zahtijevaju li kriteriji primjenu mjera kojima se omogućava intervencija u postupak obrade kako bi se uklonile slabosti u sustavu ili postupku?

k. Zahtijevaju li kriteriji primjenu tehničkih i organizacijskih mjera radi osiguravanja smanjenja količine podataka, npr. brisanjem poveznica na osobne podatke ili odvajanjem podataka od ispitanika, anonimizacijom i pseudonimizacijom ili izoliranjem podatkovnih sustava?

l. Zahtijevaju li kriteriji primjenu tehničkih mjera kojima se uspostavlja zadana zaštita podataka?

m. Zahtijevaju li kriteriji primjenu tehničkih i organizacijskih mjera kojima se uspostavlja integrirana zaštita podataka, npr. sustav upravljanja zaštitom podataka namijenjen prikazivanju, kontroli i provedbi zahtjeva za zaštitu podataka i informiranju o njima?

n. Zahtijevaju li kriteriji uspostavu tehničkih i organizacijskih mjera za provedbu odgovarajućeg periodičnog osposobljavanja i obrazovanja osoblja koje ima trajan ili redovan pristup osobnim podacima?

o. Zahtijevaju li kriteriji preispitivanje mjera?

p. Zahtijevaju li kriteriji provođenje samoprocjene / unutarnje revizije?

q. Zahtijevaju li kriteriji mjere kojima se osigurava da se dužnosti obavješćivanja o povredi osobnih podataka obavljaju u propisanom roku i opsegu?

r. Zahtijevaju li kriteriji uspostavu i provjeru postupaka upravljanja incidentima?

s. Zahtijevaju li kriteriji praćenje novih pitanja povezanih s privatnošću i tehnologijom te prema potrebi ažuriranje sustava?

…

11 DRUGE POSEBNE ZNAČAJKE POGODNE ZA ZAŠTITU PODATAKA

a. Zahtijevaju li kriteriji provedbu tehnika za unapređenje zaštite podataka? To bi moglo uključivati kriterije koji zahtijevaju poboljšanu zaštitu podataka uklanjanjem ili smanjenjem osobnih podataka i/ili rizika povezanog sa zaštitom podataka.

- *Primjer: jedna takva tehnika za unapređenje zaštite podataka mogli bi biti kriteriji koji zahtijevaju poboljšano brisanje poveznica na osobne podatke primjenom upravljanja identitetom usmjerenog na korisnika, kao što je dokazivanje identiteta na temelju atributa, umjesto upravljanja identitetom usmjerenog na organizaciju.*

b. Zahtijevaju li kriteriji provedbu poboljšane kontrole ispitanika radi olakšavanja samoodređenja i izbora?

…

12 KRITERIJI KOJIMA SE DOKAZUJE POSTOJANJE ODGOVARAJUĆIH ZAŠTITNIH MJERA PRI PRIJENOSU OSOBNIH PODATAKA

O tim će kriterijima više riječi biti u budućim smjernicama o članku 42. stavku 2.

13 DODATNI KRITERIJI ZA EUROPSKI PEČAT ZA ZAŠTITU PODATAKA

a. Jesu li kriteriji namijenjeni svim državama članicama?

b. Mogu li se u kriterijima uzeti u obzir zakonodavstvo ili scenariji država članica u području zaštite podataka?

c. Zahtijevaju li kriteriji evaluaciju pojedinačnih predmeta evaluacije u pogledu sektorskog zakonodavstva država članica o zaštiti podataka?

d. Zahtijevaju li kriteriji da voditelj ili izvršitelj obrade ispitanicima i zainteresiranim stranama dostavi informacije o sljedećem na jezicima država članica:

e. obradi / predmetu evaluacije?

f. dokumentaciji povezanoj s obradom / predmetom evaluacije?

g. rezultatima evaluacije?

…

14 CJELOVITA EVALUACIJA KRITERIJA

a. Obuhvaćaju li kriteriji cijeli opseg mehanizma certificiranja (tj. jesu li kriteriji sveobuhvatni) kako bi se dostatno zajamčila pouzdanost certificiranja?

- *Primjer: ako je opseg mehanizma certificiranja usredotočen na obradu zdravstvenih podataka, potrebno je zajamčiti visoku razinu zaštite podataka definiranjem kriterija kojima se osigurava, na primjer, temeljito ocjenjivanje i primjena načela integrirane i zadane privatnosti.*

b. Jesu li kriteriji razmjerni veličini postupka obrade obuhvaćenog opsegom mehanizma certificiranja, osjetljivosti informacija i riziku koji predstavlja obrada?

c. Smatrate li da će kriteriji poboljšati usklađenost voditelja i izvršitelja obrade s propisima o zaštiti podataka?

d. Hoće li ispitanici imati koristi kad je riječ o njihovu pravu na informacije te hoće li im, među ostalim, biti objašnjeni željeni rezultati?