Smernice

Smernice 4/2018 o akreditaciji teles za certificiranje na podlagi člena 43 Splošne uredbe o varstvu podatkov (2016/679)

Različica 3.0

4. junij 2019

Dosedanje različice

Različica 3.0	4. junij 2019	Vključitev Priloge 1 (različica 2.0 Priloge 1, sprejeta 4. junija 2019 po javnem posvetovanju)
Različica 2.0	4. december 2018	Sprejetje smernic po javnem posvetovanju – istega dne je bila sprejeta Priloga 1 (različica 1.0) za javno posvetovanje
Različica 1.0	6. februar 2018	Sprejetje smernic s strani delovne skupine iz člena 29 (različica za javno posvetovanje). To različico je EOVP potrdil 25. maja 2018

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

ob upoštevanju rezultatov javnega posvetovanja o smernicah, ki je potekalo februarja 2018, in o Prilogi, ki je potekalo med 14. decembrom 2018 in 1. februarjem 2019, v skladu s členom 70(4) Splošne uredbe o varstvu podatkov

SPREJEL NASLEDNJE SMERNICE:

1 UVOD

Splošna uredba o varstvu podatkov (Uredba (EU) 2016/679 – v nadaljevanju SUVP), ki se je začela uporabljati 25. maja 2018, je posodobljen okvir za skladnost varstva podatkov v Evropi, ki temelji na odgovornosti in temeljnih pravicah. Osrednjega pomena zanj so različni ukrepi za skladnost z določbami SUVP, ki vključujejo obvezne zahteve v posebnih okoliščinah (tudi imenovanje pooblaščenih oseb za varstvo podatkov in izdelavo ocene učinkov varstva podatkov) in prostovoljne ukrepe, kot so kodeksi ravnanja in mehanizmi certificiranja.

Člen 43(1) SUVP določa, da morajo države članice za vzpostavitev mehanizmov certificiranja ter pečatov in označb za varstvo podatkov zahtevati, da telesa za certificiranje, ki izdajajo certifikate v skladu s členom 42(1), akreditirati pristojni nadzorni organ in/ali nacionalni akreditacijski organ. Če akreditiranje izvaja nacionalni akreditacijski organ v skladu z ISO/IEC 17065/2012, je treba izpolniti tudi dodatne zahteve, ki jih določi pristojni nadzorni organ.

S smiselnimi mehanizmi certificiranja se lahko okrepita skladnost s SUVP in preglednost za posameznike, na katere se nanašajo osebni podatki, ter v odnosih med podjetji, na primer med upravljavci in obdelovalci. Upravljavci in obdelovalci podatkov bodo imeli koristi od neodvisne potrditve, ki jo izvede tretja oseba za namene dokazovanja skladnosti njihovih dejanj obdelave.[1]

Evropski odbor za varstvo podatkov (v nadaljevanju EOVP) ugotavlja, da je treba nujno zagotoviti smernice o akreditaciji. Še posebej je vrednost in namen akreditacije, da se z njo zagotovi uradna izjava o pristojnosti teles za certificiranje, na podlagi katere se ustvari zaupanje v mehanizem certificiranja.

Namen smernic je zagotoviti navodila za razlago in izvajanje določb člena 43 SUVP. Predvsem je njihov namen pomagati državam članicam, nadzornim organom in nacionalnim akreditacijskim organom pri vzpostavitvi doslednega in harmoniziranega izhodišča za akreditacijo teles za certificiranje, ki izdajajo certifikate v skladu s SUVP.

[1] V uvodni izjavi 100 SUVP je navedeno, da se lahko z uvedbo mehanizmov certificiranja povečata preglednost in skladnost s to uredbo ter posameznikom, na katere se nanašajo osebni podatki, omogoči, da hitro ocenijo raven varstva podatkov zadevnih proizvodov in storitev.

2 PODROČJE UPORABE SMERNIC

Te smernice:

- določajo namen akreditacije v smislu SUVP;
- pojasnjujejo možnosti, ki so na voljo za akreditacijo teles za certificiranje v skladu s členom 43(1), in opredeljujejo ključna vprašanja, ki jih je treba obravnavati;
- zagotavljajo okvir za vzpostavitev dodatnih zahtev za akreditacijo, kadar akreditacijo izvaja nacionalni akreditacijski organ, in
- zagotavljajo okvir za vzpostavitev zahtev za akreditacijo, kadar akreditacijo izvaja nadzorni organ.

Smernice niso postopkovnikakreditacije teles za certificiranje v skladu s SUVP. Ne razvijajo novega tehničnega standarda za akreditacijo teles za certificiranje za namene SUVP.

Te smernice so namenjene:

- državam članicam, ki morajo zagotoviti, da telesa za certificiranje akreditira nadzorni organ in/ali nacionalni akreditacijski organ;
- nacionalnim akreditacijskim organom, ki akreditirajo telesa za certificiranje v skladu s členom 43(1)(b);
- pristojnemu nadzornemu organu, ki opredeli „dodatne zahteve“ poleg zahtev iz ISO/IEC 17065/2012[2], kadar akreditacijo izvaja nacionalni akreditacijski organ v skladu s členom 43(1)(b);
- EOVP pri pripravi mnenja o zahtevah za akreditacijo pristojnega nadzornega organa in njihovi odobritvi v skladu s členi 43(3), 70(1)(p) in 64(1)(c);
- pristojnemu nadzornemu organu pri opredelitvi zahtev za akreditacijo, če akreditacijo izvaja nadzorni organ v skladu s členom 43(1)(a);

- drugim deležnikom, kot so prihodnja telesa za certificiranje ali lastniki certifikacijske sheme, ki določajo merila in postopke za certificiranje[3].

Opredelitev pojmov

Naslednje opredelitve pojmov so namenjene širjenju enotnega razumevanju temeljnih elementov akreditacijskega postopka. Upoštevati jih je treba kot oporne točke in niso neizpodbojne. Opredelitve

[2] Mednarodna organizacija za standardizacijo: Ugotavljanje skladnosti – zahteve za organe, ki certificirajo proizvode, procese in storitve.

[3] Lastnik sheme je določljiva organizacija, ki je vzpostavila merila in zahteve za certificiranje, na podlagi katerih se ugotavlja skladnost. Za akreditacijo je odgovorna organizacija, ki izvaja ocenjevanje (člen 43(4)) na podlagi zahtev shem za certificiranje in izdaja certifikate (tj. telo za certificiranje, imenovano tudi organ za ugotavljanje skladnosti). Organizacija, ki izvaja ocenjevanja, bi lahko bila organizacija, ki je razvila shemo in je njena lastnica, lahko pa bi bile sprejete ureditve, v skladu s katerimi je ena organizacija lastnica sheme, druga (ali več drugih) pa izvaja ocenjevanje.

pojmov temeljijo na zakonodajnih okvirih in standardih, zlasti na ustreznih določbah SUVP in ISO/IEC 17065/2012.

Opredelitve pojmov v teh smernicah so:

„*akreditacija*“ teles za certificiranje – glej oddelek 3 o razlagi akreditacije za namene člena 43 SUVP;

„*dodatne zahteve*“ pomenijo zahteve, ki jih opredeli pristojni nadzorni organ in na podlagi katerih se izvede akreditacija[4];

„*certificiranje*“ pomeni ocenjevanje in nepristransko potrjevanje, ki ga opravi tretja oseba[5], da je bilo dokazano izpolnjevanje meril za certificiranje;

„*telo za certificiranje*“ pomeni organ za ugotavljanje skladnosti[6] s strani tretje osebe[7], ki upravlja mehanizme certificiranja[8];

„*shema certificiranja*“ pomeni sistem certificiranja, povezan z določenimi proizvodi, procesi in storitvami, za katere veljajo iste določene zahteve, posebna pravila in postopki;[9]

„*merila*“ ali merila za certificiranje pomenijo merila, na podlagi katerih se izvaja certificiranje (ugotavljanje skladnosti);[10]

„*nacionalni akreditacijski organ*“ pomeni edini verodostojni organ v državi članici, imenovan v skladu z Uredbo (ES) št. 765/2008 Evropskega parlamenta in Sveta, ki podeljuje akreditacijo v skladu s pooblastili, ki mu jih dodeli država[11].

3 RAZLAGA „AKREDITACIJE“ ZA NAMENE ČLENA 43 SUVP

Pojem „akreditacija“ v SUVP ni opredeljen. V členu 2(10) Uredbe (ES) št. 765/2008, ki določa splošne zahteve za akreditacijo, je akreditacija opredeljena kot

„potrditev nacionalnega akreditacijskega organa, da organ za ugotavljanje skladnosti izpolnjuje zahteve, določene s harmoniziranimi standardi, in, kjer je ustrezno, vse dodatne zahteve, vključno s tistimi, ki so določene v zadevnih sektorskih shemah, za opravljanje posebne dejavnosti ugotavljanja skladnosti“.

V skladu z ISO/IEC 17011

[4] Člen 43(1), (3) in (6).
[5] Opozoriti je treba, da se v skladu z ISO 17000 certificiranje, ki ga opravi tretja oseba, uporablja za vse predmete ugotavljanja skladnosti (5.5), razen za same organe za ugotavljanje skladnosti, za katere se uporablja akreditacija (5.6).
[6] Dejavnost ugotavljanja skladnosti s strani tretje osebe izvaja organizacija, ki je neodvisna od osebe ali organizacije, ki zagotovi predmet, in od interesov uporabnikov glede tega predmeta, prim. ISO 17000, 2.4.
[7] Glej ISO 17000, 2.5: „organ, ki izvaja storitve ugotavljanja skladnosti“; ISO 17011: „organ, ki izvaja storitve ugotavljanja skladnosti in je lahko predmet akreditacije“; ISO 17065, 3.12.
[8] Člen 42(1) in (5) Splošne uredbe o varstvu podatkov.
[9] Glej 3.9 v povezavi s Prilogo B k ISO 17065.

[10] Glej člen 42(5).
[11] Glej člen 2(11) Uredbe 765/2008/ES.

se akreditacija nanaša na potrditev tretje osebe v zvezi z organom za ugotavljanje skladnosti, ki pomeni uradno dokazilo njegove pristojnosti za izvajanje ustreznih nalog za ugotavljanje skladnosti.

Člen 43(1) določa:

„Brez poseganja v naloge in pooblastila pristojnega nadzornega organa iz členov 57 in 58 certifikat izdajo in podaljšajo telesa za certificiranje, ki imajo ustrezno raven strokovnega znanja v zvezi z varstvom podatkov, in sicer po tem, ko obvestijo nadzorni organ, da se mu po potrebi dovoli izvajanje pooblastil v skladu s točko (h) člena 58(2). Države članice zagotovijo, da so ta telesa za certificiranje akreditirana s strani enega ali obeh od naslednjih:

(a) nadzornega organa, ki je pristojen na podlagi člena 55 ali 56;
(b) nacionalnega akreditacijskega organa, imenovanega v skladu z Uredbo (ES) št. 765/2008 Evropskega parlamenta in Sveta v skladu z EN-ISO/IEC 17065/2012 in dodatnimi zahtevami, ki jih določi nadzorni organ, ki je pristojen na podlagi člena 55 ali 56.“

Zahteve za akreditacijo v zvezi s SUVP so oblikovane na podlagi

- ISO/IEC 17065/2012 in „dodatnih zahtev“, ki jih določi nadzorni organ, pristojen na podlagi člena 43(1)(b), kadar akreditacijo izvaja nacionalni akreditacijski organ, in nadzorni organ, kadar akreditacijo izvaja sam.

V obeh primerih morajo konsolidirane zahteve zajemati zahteve, ki so navedene v členu 43(2).

EOVP priznava, da je namen akreditacije zagotoviti uradno izjavo o pristojnostih organa, da izvede certificiranje (dejavnosti za ugotavljanje skladnosti)[12]. Akreditacija v smislu SUVP pomeni naslednje:

potrditev[13] nacionalnega akreditacijskega organa in/ali nadzornega organa, da je telo za certificiranje[14] usposobljeno za certificiranje v skladu s členoma 42 in 43 SUVP, ob upoštevanju ISO/IEC 17065/2012 in dodatnih zahtev, ki jih določi nadzorni organ in/ali odbor.

4 AKREDITACIJA V SKLADU S ČLENOM 43(1) SUVP

Člen 43(1) določa, da je možnosti za akreditacijo teles za certificiranje več. V skladu s SUVP nadzorni organi in države članice določijo postopek akreditacije teles za certificiranje. V tem oddelku so opredeljene možnosti akreditacije iz člena 43.

4.1 Vloga držav članic

Člen 43(1) določa, da morajo države članice *zagotoviti* akreditacijo teles za certificiranje, posameznim državam članicam pa dovoljuje, da določijo, kdo je odgovoren za ocenjevanje, na podlagi katerega je izvedena akreditacija. Na podlagi člena 43(1) so na voljo tri možnosti; akreditacijo izvajajo:

(1) samo nadzorni organ na podlagi svojih zahtev,

[12] Prim. uvodno izjavo 15 Uredbe 765/2008/ES.
[13] Prim. člen 2(10) Uredbe (ES) 765/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o določitvi zahtev za akreditacijo in nadzor trga v zvezi s trženjem proizvodov.
[14] Prim. z opredelitvijo pojma „akreditacija“ v skladu z ISO 17011.

(2) samo nacionalni akreditacijski organ, imenovan v skladu z Uredbo (ES) 765/2008 v skladu z ISO/IEC 17065/2012 in dodatnimi zahtevami, ki jih določi pristojni nadzorni organ, ali
(3) nadzorni organ in nacionalni akreditacijski organ (v skladu z vsemi zahtevami, navedenimi v zgornji točki 2).

Posamezne države članice morajo odločiti, ali bo dejavnosti akreditacije izvajal nacionalni akreditacijski organ ali nadzorni organ ali jih bosta izvajala oba skupaj, v vsakem primeru pa morajo zagotoviti ustrezne vire[15].

4.2 Medsebojno delovanje z Uredbo (ES) 765/2008

EOVP pojasnjuje, da člen 2(11) Uredbe (ES) št. 765/2008 opredeljuje nacionalni akreditacijski organ kot „*edini verodostojni* organ v državi članici, ki izvaja akreditacijo s pooblastilom te države“.

Člen 2(11) bi se lahko štel za neskladnega s členom 43(1) SUVP, ki dovoljuje, da akreditacijo izvede organ, ki ni nacionalni akreditacijski organ države članice. EOVP meni, da je bil namen zakonodaje EU odstopanje od splošnega načela, da lahko akreditacijo izvaja izključno nacionalni akreditacijski organ, in je nadzornim organom podelila enake pristojnosti glede akreditacije teles za certificiranje. Zato je člen 43(1) *lex specialis* v razmerju do člena 2(11) Uredbe 765/2008.

4.3 Vloga nacionalnega akreditacijskega organa

Člen 43(1) določa, da nacionalni akreditacijski organ akreditira telesa za certificiranje v skladu z ISO/IEC 17065/2012 in dodatnimi zahtevami, ki jih določi pristojni nadzorni organ.

EOVP zaradi jasnosti izpostavlja, da posebno sklicevanje na točko (b) odstavka 1 člena 43(3) pomeni, da „te zahteve“ pomenijo „dodatne zahteve“, ki jih določi pristojni nadzorni organ v skladu s členom 43(1)(b), in zahteve iz člena 43(2).

Nacionalni akreditacijski organi v postopku akreditacije uporabljajo dodatne zahteve, ki jih opredelijo nadzorni organi.

Telo za certificiranje z veljavno akreditacijo na podlagi ISO/IEC 17065/2012 za sheme certificiranja, ki niso povezane s SUVP, bo moralo, če želi razširiti obseg svoje akreditacije, ki bi zajemal certifikate, izdane v skladu s SUVP, izpolniti dodatne zahteve, ki jih določi nadzorni organ, če akreditacijo izvaja nacionalni akreditacijski organ. Če akreditacijo za certificiranje v smislu SUVP zagotavlja samo pristojni nadzorni organ, bo moralo telo za certificiranje, ki zaprosi za akreditacijo, izpolnjevati zahteve, ki jih določi ustrezni nadzorni organ.

4.4 Vloga nadzornega organa

EOVP poudarja, da člen 57(1)(q) določa, da nadzorni organ opravi akreditacijo telesa za certificiranje v skladu s členom 43 kot „nalogo nadzornega organa“ v skladu s členom 57, člen 58(3)(e) pa določa, da ima nadzorni organ dovoljenje in svetovalno pristojnost za akreditacijo teles za certificiranje v skladu s členom 43. Besedilo člena 43(1) dopušča nekaj prožnosti, akreditacijsko funkcijo nadzornega organa pa bi bilo treba kot nalogo razumeti le, če je to primerno. Za pojasnitev te točke se lahko uporabi pravo države članice. Telo za certificiranje pa mora v postopku akreditacije s strani nacionalnega

[15] Glej člen 4(9) Uredbe (ES) št. 765/2008.

akreditacijskega organa v skladu s členom 43(2)(a) pristojnemu nadzornemu organu izkazati svojo neodvisnost in strokovno znanje v zvezi z vsebino mehanizma certificiranja, ki ga zagotavlja.[16]

Če država članica določi, da mora telesa za certificiranje akreditirati nadzorni organ, mora ta opredeliti zahteve za akreditacijo, ki med drugim vključujejo zahteve iz člena 43(2). V primerjavi z obveznostmi za akreditacijo teles za certificiranje s strani nacionalnih akreditacijskih organov člen 43 daje manj navodil o zahtevah za akreditacijo, kadar nadzorni organ sam izvaja akreditacijo. Kot prispevek k harmoniziranemu pristopu k akreditaciji bi morala biti merila zajo, ki jih uporablja nadzorni organ, urejena v ISO/IEC 17065 in bi jih bilo treba dopolniti z dodatnimi zahtevami, ki jih določi nadzorni organ v skladu s členom 43(1)(b). EOVPpoudarja, da določbe v členu 43(2)(a) do (e) odražajo in natančneje določajo zahteve iz ISO 17065, kar bo prispevalo k dosledni uporabi.

Če država članica določi, da morajo telesa za certificiranje akreditirati nacionalni akreditacijski organi, mora nadzorni organ opredeliti dodatne zahteve, ki dopolnjujejo obstoječe dogovore glede akreditacije iz Uredbe (ES) 765/2008 (pri čemer se členi 3 do 14 nanašajo na organizacijo in delovanje akreditacije organov za ugotavljanje skladnosti), in tehnična pravila, ki opisujejo metode ter postopke teles za certificiranje. Ob upoštevanju tega Uredba (ES) 765/2008 zagotavlja nadaljnje smernice: člen 2(10) opredeljuje akreditacijo in se sklicuje na „harmonizirane standarde“ in „vse dodatne zahteve, vključno s tistimi, ki so določene v zadevnih sektorskih shemah“. Iz tega sledi, da bi morale dodatne zahteve, ki jih določi nadzorni organ, vključevati posebne zahteve in se med drugim osredotočati na olajšanje ocenjevanja neodvisnosti in raven strokovnega znanja teles za certificiranje na področju varstva podatkov, na primer na njihovo zmožnost ocenjevanja in certificiranja dejanj obdelave osebnih podatkov s strani upravljavcev in obdelovalcev v skladu s členom 42(1). To vključuje pristojnost, ki je potrebna za sektorske sheme, upoštevajoč varstvo temeljnih pravic in svoboščin posameznikov ter zlasti varstvo osebnih podatkov.[17] Priloga k tem smernicam je lahko pristojnim nadzornim organom v pomoč pri opredelitvi „dodatnih zahtev“ v skladu s členom 43(1)(b) in členom 43(3).

Člen 43(6) določa, da „[n]adzorni organ zahteve iz odstavka 3 tega člena in merila iz člena 42(5) objavi v lahko dostopni obliki“. Zaradi zagotavljanja preglednosti se objavijo vsa merila in zahteve, ki jih odobri nadzorni organ. Za potrebe kakovosti in zaupanja v telesa za certificiranjejezaželeno, da so vse zahteve za akreditacijo dostopne javnosti.

4.5 Nadzorni organ v vlogi telesa za certificiranje

Člen 42(5) določa, da lahko nadzorni organ izda certifikate, vendar SUVP ne zahteva njegove akreditacije za izpolnjevanje zahteve iz Uredbe (ES) 765/2008. EOVP poudarja, da člen 43(1)(a) ter zlasti člen 58(2)(h) in člen 58(3)(a) in (e) do (f) pooblašča nadzorne organe za izvajanje akreditacije in certificiranja, obenem pa za svetovanje in po potrebi preklic certifikatov ali izdajo odredbe telesom za certificiranje, naj ne izdajo certifikatov.

Verjetno je v nekaterih okoliščinah ločitev vlog in nalog akreditacije ter certificiranja primerna ali potrebna, na primer če nadzorni organ in drugo telo za certificiranje soobstajata v državi članici ter oba izdajata enak sklop certifikatov. Nadzorni organi bi morali zato sprejeti zadostne organizacijske ukrepe,

[16] Dodatne zahteve, ki jih nadzorni organ določi v skladu s členom 43(1)(b), bi morale opredeliti zahteve glede neodvisnosti in strokovnega znanja. Glej tudi Prilogo 1 k smernicam.
[17] Člen 1(2) SUVP.

da bi ločili naloge v smislu SUVP ter utrdili in olajšali mehanizme za certificiranje, obenem pa sprejeli previdnostne ukrepe, da bi preprečili navzkrižje interesov, ki ga to lahko povzroči. Države članice in nadzorni organi bi morali pri oblikovanju nacionalnega prava in postopkov, ki se nanašajo na akreditacijo in certificiranje v skladu s SUVP, upoštevati tudi harmonizirano evropsko raven.

4.6 Zahteve za akreditacijo

Priloga k tem smernicam vsebuje napotke, kako opredeliti dodatne zahteve za akreditacijo. Navaja ustrezne določbe iz SUVP in predlaga zahteve, ki bi jih morali preučiti nadzorni organi in nacionalni akreditacijski organi, da bi zagotovili skladnost s SUVP.

Kot je že navedeno, kadar telesa za certificiranje akreditira nacionalni akreditacijski organ v skladu z Uredbo (ES) 765/2008, je ISO/IEC 17065/2012 ustrezni standard za akreditacijo, ki ga dopolnjujejo dodatne zahteve nadzornega organa. Člen 43(2) odraža splošne določbe ISO/IEC 17065/2012 v zvezi z varstvom temeljnih pravic v okviru SUVP. Okvir iz priloge uporablja člen 43(2) in ISO/IEC 17065/2012 kot podlago za opredelitev zahtev in dodatnih meril za ocenjevanje strokovnega znanja teles za certificiranje na področju varstva podatkov in njihove zmožnosti spoštovanja pravic in svoboščin posameznikov v zvezi z obdelavo osebnih podatkov, kot določa SUVP. EOVP poudarja, da je zlasti osredotočen na zagotavljanje ustrezne ravni strokovnega znanja teles za certificiranje v zvezi z varstvom podatkov v skladu s členom 43(1).

Dodatne zahteve za akreditacijo, ki jih določi nadzorni organ, bodo veljale za vsa telesa za certificiranje, ki zaprosijo za akreditacijo. Akreditacijski organ bo ocenil, ali je zadevno telo za certificiranje pristojno za izvajanje dejavnosti certificiranja v skladu z dodatnimi zahtevami in vsebino certificiranja. Navedeni bodo specifični sektorji ali področja certificiranja, za katera je akreditirano telo za certificiranje.

EOVP poudarja tudi, da je poleg izpolnjevanja zahtev iz ISO/IEC 17065/2012 potrebno posebno strokovno znanje na področju varstva podatkov, če drugi, zunanji organi, kot so laboratoriji ali revizorji, izvajajo dele ali sklope dejavnosti certificiranja v imenu akreditiranega telesa za certificiranje. V teh primerih akreditacija zunanjih organov v smislu same SUVP ni mogoča. Za zagotovitev ustreznosti teh organov za opravljanje dejavnosti v imenu akreditiranih teles za certificiranje, mora akreditirano telo za certificiranje zagotoviti, da ima zahtevano strokovno znanje na področju varstva podatkov, pri čemer mora to znanje dokazati zunanji organ za zadevno dejavnost, ki jo opravlja.

Okvir za opredelitev dodatnih zahtev za akreditacijo, kot je predstavljen v prilogi k tem smernicam, ni postopkovnik akreditacije, ki jo izvaja nacionalni akreditacijski organ ali nadzorni organ. Zagotavlja le smernice o strukturi in metodologiji, torej je orodje, ki nadzornim organom pomaga opredeliti dodatne zahteve za akreditacijo.

PRILOGA 1

V Prilogi 1 so navedene smernice za določitev „dodatnih“ zahtev za akreditacijo ob upoštevanju ISO/IEC 17065/2012 in v skladu s členom 43(1)(b) in členom 43(3) SUVP.

V tej prilogi so predlagane zahteve, ki jih pripravi nadzorni organ za varstvo podatkov in ki se uporabljajo pri akreditaciji telesa za certificiranje s strani nacionalnega akreditacijskega organa ali pristojnega nadzornega organa[18]. Te dodatne zahteve je treba pred odobritvijo iz člena 64(1)(c) sporočiti Evropskemu odboru za varstvo podatkov.

To prilogo bi bilo treba brati v povezavi z ISO/IEC 17065/2012. Uporabljene številke oddelkov ustrezajo tistim, ki se uporabljajo v ISO/IEC 17065/2012. Kadar akreditacijo izvajajo nadzorni organi v skladu s členom 43(1)(a), bi se uporaba tega pristopa štela za dobro prakso, če je to izvedljivo. To bi podprlo harmoniziracijo akreditacije na ravni EU.

Pristojni nadzorni organ lahko ne glede na naslednje usmeritve ali če ni usmeritev v zvezi s katerim koli elementom ISO/IEC 17065/2012, določi nadaljnje dodatne zahteve v zvezi s temi elementi, če je to v skladu z nacionalno zakonodajo.

0 UVOD

[Ta oddelek je namenjen morebitnim dogovorjenim pogojem sodelovanja med nacionalnim akreditacijskim organom in nadzornim organom za varstvo podatkov, npr. kdo je odgovoren za sprejemanje vlog ali kako organizirati potrditev odobrenih meril v okviru postopka akreditacije.]

1 PODROČJE UPORABE[19]

Področje uporabe ISO/IEC 17065/2012 se uporablja v skladu s SUVP. Dodatne informacije so navedene v smernicah o akreditaciji in certificiranju. Nacionalni akreditacijski organ in pristojni nadzorni organ bi morala pri oceni v postopku akreditacije upoštevati področje uporabe mehanizma certificiranja (na primer certificiranje dejavnosti obdelave v okviru storitev računalništva v oblaku), zlasti kar zadeva merila, strokovno znanje in metodologijo vrednotenja. Široko področje uporabe ISO/IEC 17065/2012, ki zajema proizvode, procese in storitve, ne bi smelo znižati ali nadomestiti zahtev SUVP, npr. mehanizem upravljanja ne more biti edini element mehanizma certificiranja, saj mora certificiranje vključevati obdelavo osebnih podatkov, tj. dejanja obdelave. V skladu s členom 42(1) se certificiranje na podlagi SUVP uporablja samo za dejanja obdelave s strani upravljavcev in obdelovalcev.

2 NORMATIVNA REFERENCA

SUVP ima prednost pred ISO/IEC 17065/2012. Če se dodatne zahteve ali mehanizem certificiranja sklicujejo na druge ISO standarde, jih je treba razlagati v skladu z zahtevami iz SUVP.

[18] Za informacije o postopku odobritve meril za certificiranje glej oddelek 4 smernic o certificiranju.
[19] Številčenje ustreza ISO/IEC 17065/2012.

3 IZRAZI IN OPREDELITVE POJMOV

V tej prilogi se uporabljajo izrazi in opredelitve pojmov iz smernic o akreditaciji (WP 261) in certificiranju (EOVP 1/2018), ki imajo prednost pred opredelitvami ISO.

4 SPLOŠNE ZAHTEVE ZA AKREDITACIJO

4.1 Pravne in pogodbene zadeve

4.1.1 Pravna odgovornost

Telo za certificiranje bi moralo biti sposobno nacionalnemu akreditacijskemu organu ali pristojnemu nadzornemu organu (kadar koli) dokazati, da so njegovi postopki posodobljeni in skladni s pravnimi odgovornostmi, določenimi v pogojih akreditacije, vključno z dodatnimi zahtevami glede uporabe Uredbe (EU) 2016/679. Opozoriti je treba, da je telo za certificiranje tudi samo upravljavec/obdelovalec podatkov, zato mora biti kot del postopka certificiranja sposobno dokazati, da so njegovi postopki in ukrepi, namenjeni posebej upravljanju osebnih podatkov organizacije, ki je njegova stranka, in ravnanju z njimi, skladni z Uredbo (EU) 2016/679.

Pristojni nadzorni organ lahko določi dodatne zahteve in postopke za preverjanje skladnosti teles za certificiranje s SUVP pred akreditacijo.

4.1.2 Sporazum o certificiranju

Minimalne zahteve za sporazum o certificiranju se dopolnijo z naslednjimi točkami:

Telo za certificiranje poleg zahtev iz ISO/IEC 17065/2012 dokaže, da njegovi sporazumi o certificiranju:

1. od vložnika zahtevajo, da vedno izpolnjuje splošne zahteve za certificiranje v smislu točke 4.1.2.2 (a) ISO/IEC 17065/2012 in merila, ki jih odobri pristojni nadzorni organ ali EOVP v skladu s členom 43(2)(b) in členom 42(5);
2. od vložnika zahtevajo, da pristojnemu nadzornemu organu omogoči popolno preglednost, kar zadeva postopek certificiranja, vključno s pogodbeno zaupnimi zadevami, povezanimi z izpolnjevanjem zahtev glede varstva podatkov, v skladu s členom 42(7) in členom 58(1)(c);
3. ne zmanjšujejo odgovornosti vložnika za izpolnjevanje zahtev Uredbe (EU) 2016/679 in ne posegajo v naloge in pooblastila nadzornega organa, ki je pristojen v skladu s členom 42(5);
4. od vložnika zahtevajo, da v skladu s členom 42(6) telesu za certificiranje zagotovi vse informacije in dostop do svojih dejavnosti obdelave, ki so potrebni za izvedbo postopka certificiranja;
5. od vložnika zahtevajo, da spoštuje veljavne roke in postopke. V sporazumu o certificiranju mora biti navedeno, da je treba spoštovati roke in postopke, določene na primer v programu certificiranja ali drugih predpisih, ter se jih držati;
6. ob upoštevanju točke 4.1.2.2 (c) št. 1 ISO/IEC 17065/2012 določajo pravila o veljavnosti, podaljšanju in preklicu v skladu s členoma 42(7) in 43(4), vključno s pravili, ki določajo ustrezne časovne razmike za ponovno vrednotenje ali pregled (pravilnost) v skladu s členom 42(7);
7. telesu za certificiranje dovoljujejo, da razkrije vse informacije, potrebne za dodelitev certifikata, v skladu s členoma 42(8) in 43(5);

8. vključujejo pravila o potrebnih previdnostnih ukrepih za preiskovanje pritožb v smislu točke 4.1.2.2 (c) št. 2, dodatno pa v smislu točke (j) vsebujejo tudi izrecne navedbe strukture in postopka za obravnavanje pritožb v skladu s členom 43(2)(d);
9. če ima preklic ali začasni odvzem akreditacije za telo za certificiranje posledice za stranko, bi morale biti poleg minimalnih zahtev iz točke 4.1.2.2 ISO/IEC 17065/2012 obravnavane tudi posledice za stranko;
10. od vložnika zahtevajo, da v primeru znatnih sprememb njegovega dejanskega ali pravnega položaja in sprememb njegovih proizvodov, procesov in storitev, ki jih zadeva certificiranje, o tem obvesti telo za certificiranje.

4.1.3 Uporaba pečatov in označb za varstvo podatkov

Certifikati, pečati in označbe se uporabljajo samo v skladu s členoma 42 in 43 ter smernicami o akreditaciji in certificiranju.

4.2 Upravljanje nepristranskosti

Akreditacijski organ zagotovi, da poleg zahteve iz točke 4.2. ISO/IEC 17065/2012:

1. telo za certificiranje izpolnjuje tudi dodatne zahteve pristojnega nadzornega organa (na podlagi člena 43(1)(b))
    a. v skladu s členom 43(2)(a) predloži ločene dokaze o svoji neodvisnosti. To velja zlasti za dokaze v zvezi s financiranjem telesa za certificiranje, kar zadeva zagotavljanje nepristranskosti;
    b. njegove naloge in dolžnosti ne povzročajo nasprotja interesov v skladu s členom 43(2)(e);
2. telo za certificiranje ni pomembno povezano s stranko, ki jo ocenjuje.

4.3 Odgovornost in financiranje

Akreditacijski organ poleg zahteve iz točke 4.3.1 ISO/IEC 17065/2012 redno zagotavlja, da ima telo za certificiranje vzpostavljene ustrezne ukrepe (npr. zavarovanje ali rezerve) za kritje svoje odgovornosti v geografskih regijah, v katerih deluje.

4.4 Nediskriminatorni pogoji

Nadzorni organ lahko določi dodatne zahteve, če so v skladu z nacionalno zakonodajo.

4.5 Zaupnost

Nadzorni organ lahko določi dodatne zahteve, če so v skladu z nacionalno zakonodajo.

4.6 Javno dostopne informacije

Akreditacijski organ poleg zahteve iz točke 4.6 ISO/IEC 17065/2012 od telesa za certificiranje zahteva vsaj to, da

1. se objavijo vse različice (sedanje in prejšnje) odobrenih meril, ki se uporabljajo v smislu člena 42(5), in so enostavno dostopne javnosti, kar velja tudi za vse postopke certificiranja, pri čemer se na splošno navede ustrezno obdobje veljavnosti;
2. se v skladu s členom 43(2)(d) objavijo informacije o postopkih za obravnavo pritožb in ugovorov.

5 STRUKTURNE ZAHTEVE, ČLEN 43(4) [„USTREZNO“ OCENJEVANJE]

5.1 Organizacijska struktura in najvišje vodstvo

Nadzorni organ lahko določi dodatne zahteve.

5.2 Mehanizmi za zagotavljanje nepristranskosti

Nadzorni organ lahko določi dodatne zahteve.

6 ZAHTEVE GLEDE VIROV

6.1 Osebje telesa za certificiranje

Akreditacijski organ poleg zahteve iz oddelka 6 ISO/IEC 17065/2012 za vsako telo za certificiranje zagotovi, da:

1. je njegovo osebje dokazalo ustrezno in stalno strokovno znanje (znanje in izkušnje) v zvezi z varstvom podatkov v skladu s členom 43(1);
2. je njegovo osebje neodvisno in ima stalno strokovno znanje v zvezi s predmetom certificiranja v skladu s členom 43(2)(a) in nima nasprotja interesov v skladu s členom 43(2)(e);
3. se njegovo osebje zaveže, da bo spoštovalo merila iz člena 42(5) v skladu s členom 43(2)(b);
4. ima njegovo osebje relevantno in ustrezno znanje in izkušnje na področju uporabe zakonodaje o varstvu podatkov;
5. ima njegovo osebje relevantno in ustrezno znanje in izkušnje na področju tehničnih in organizacijskih ukrepov za varstvo podatkov (kot je ustrezno);
6. lahko njegovo osebje dokaže izkušnje na področjih, navedenih zlasti v dodatnih zahtevah 6.1.1, 6.1.4 in 6.1.5.

Za osebje s tehničnim znanjem:

- osebje je pridobilo vsaj 6. raven evropskega ogrodja kvalifikacij[20] na ustreznem tehničnem strokovnem področju ali zaščiteni poklicni naziv (npr. dipl. inž.) v ustreznem reguliranem poklicu ali ima pomembne strokovne izkušnje.
- *Osebje, odgovorno za odločitve o certificiranju*, mora imeti pomembne strokovne izkušnje pri opredeljevanju in izvajanju ukrepov za varstvo podatkov.
- *Osebje, odgovorno za vrednotenje*, mora imeti strokovne izkušnje na področju tehničnega varstva podatkov ter znanje in izkušnje s primerljivimi postopki (npr. certificiranje/revizije) in biti registrirano v skladu z veljavnimi pravili.

Osebje dokaže, da s stalnim strokovnim razvojem ohranja posebno tehnično in revizijsko znanje.

Za osebje s pravnim znanjem:

- študij prava na univerzi, priznani s strani EU ali države, ki je trajal najmanj osem semestrov, in akademski magisterij prava (LL.M.) ali enakovreden naziv ali pomembne strokovne izkušnje.

[20] Glej spletno orodje za primerjavo kvalifikacij na naslednjem naslovu: https://ec.europa.eu/ploteus/en/compare?

- *Osebje, odgovorno za odločitve o certificiranju*, mora dokazati pomembne strokovne izkušnje na področju prava o varstvu podatkov in biti registrirano, kot se zahteva v državi članici.
- *Osebje, odgovorno za vrednotenje*, mora dokazati vsaj dve leti strokovnih izkušenj na področju prava o varstvu podatkov ter znanje in izkušnje s primerljivimi postopki (npr. certificiranje/revizije) in biti registrirano, če se to zahteva v državi članici.
    - Osebje dokaže, da s stalnim strokovnim razvojem ohranja posebno tehnično in revizijsko znanje.

6.2 Viri za vrednotenje

Nadzorni organ lahko določi dodatne zahteve, če so v skladu z nacionalno zakonodajo.

7 ZAHTEVE GLEDE POSTOPKOV, ČLEN 43(2)(C) IN (D)

7.1 Splošno

Akreditacijski organ mora poleg zahteve iz oddelka 7.1 ISO/IEC 17065/2012 zagotoviti, da:

1. telesa za certificiranje pri vložitvi vloge izpolnjujejo dodatne zahteve pristojnega nadzornega organa (na podlagi člena 43(1)(b)), da zaradi njihovih nalog in dolžnosti ne pride do nasprotja interesov v skladu s členom 43(2)(b);
2. obvesti ustrezne pristojne nadzorne organe, preden telo za certificiranje začne upravljati odobren evropski pečat za varstvo podatkov v novi državi članici iz satelitske pisarne.

7.2 Vloga

Poleg točke 7.2 ISO/IEC 17065/2012 je treba zahtevati, da:

1. se v vlogi podrobno opiše predmet certificiranja (cilj vrednotenja). To vključuje tudi vmesnike in prenose v druge sisteme in organizacije, protokole in druga zagotovila;
2. se v vlogi navede, ali se uporabljajo obdelovalci. Kadar je obdelovalec vložnik, se opišejo njegove odgovornosti in naloge, vloga pa vsebuje ustrezne pogodbe med upravljavcem in obdelovalcem.

7.3 Pregled vloge

Poleg točke 7.3 ISO/IEC 17065/2012 je treba zahtevati, da:

1. se v sporazumu o certificiranju določijo zavezujoče metode vrednotenja glede na cilj vrednotenja;
2. ocena iz točke 7.3 (e) glede tega, ali obstaja zadostno strokovno znanje, v ustreznem obsegu upošteva tehnično in pravno znanje na področju varstva podatkov.

7.4 Vrednotenje

Poleg točke 7.4 ISO/IEC 17065/2012 se v mehanizmih certificiranja opišejo zadostne metode vrednotenja za ocenjevanje skladnosti dejanj obdelave z merili za certificiranje, vključno z naslednjim, kadar je to primerno:

1. metodo za oceno potrebnosti in sorazmernosti dejanj obdelave glede na njihov namen in zadevne posameznike, na katere se nanašajo osebni podatki;
2. metodo za vrednotenje obsega, sestave in ocene vseh tveganj, ki jih upoštevata upravljavec in obdelovalec v zvezi s pravnimi posledicami na podlagi členov 30, 32, 35 in 36 SUVP ter v zvezi z opredelitvijo tehničnih in organizacijskih ukrepov na podlagi členov 24, 25 in 32 SUVP, kolikor ti členi veljajo za predmet certificiranja, in

3. metodo za oceno sredstev, vključno z jamstvi, zaščitnimi ukrepi in postopki za zagotovitev varstva osebnih podatkov v okviru obdelave, ki se pripiše predmetu certificiranja, in za dokazovanje, da so izpolnjene pravne zahteve, kakor so določene v merilih, ter
4. dokumentacijo o metodah in ugotovitvah.

Od telesa za certificiranje bi bilo treba zahtevati, da zagotovi, da so te metode vrednotenja standardizirane in se splošno uporabljajo. To pomeni, da se za primerljive cilje vrednotenja uporabljajo primerljive metode vrednotenja. Telo za certificiranje mora vsako odstopanje od tega postopka utemeljiti.

Poleg točke 7.4.2 ISO/IEC 17065/2012 bi bilo treba dovoliti, da vrednotenje izvajajo zunanji strokovnjaki, ki jih je priznalo telo za certificiranje.

Poleg točke 7.4.5 ISO/IEC 17065/2012 bi bilo treba zahtevati, da se lahko certificiranje za varstvo podatkov v skladu s členoma 42 in 43 SUVP, ki že zajema del predmeta certificiranja, vključi v trenutno certificiranje. Vendar to ne zadostuje za popolno nadomestitev (delnih) vrednotenj. Telo za certificiranje je dolžno preveriti izpolnjevanje meril. Za priznavanje se v vsakem primeru zahteva, da je na voljo popolno poročilo o vrednotenju ali informacije, ki omogočajo vrednotenje predhodnih dejavnosti certificiranja in njihovih rezultatov. Izjave o certificiranju ali podobna potrdila o certificiranju se ne bi smela šteti kot zadostna za nadomestitev poročila.

Poleg točke 7.4.6 ISO/IEC 17065/2012 bi bilo treba zahtevati, da telo za certificiranje v svojem mehanizmu certificiranja podrobno določi, kako se v okviru mehanizma certificiranja z obveščanjem, zahtevanim v točki 7.4.6, stranko (vložnika vloge za certificiranje) obvesti o neskladnostih. V zvezi s tem bi bilo treba opredeliti vsaj naravo in časovni okvir takega obveščanja.

Poleg točke 7.4.9 ISO/IEC 17065/2012 bi bilo treba zahtevati, da se dokumentacija v celoti da na voljo nadzornemu organu za varstvo podatkov na njegovo zahtevo.

7.5 Pregled

Poleg točke 7.5 ISO/IEC 17065/2012 se zahtevajo postopki za dodelitev, redni pregled in preklic zadevnih certifikatov v skladu s členom 43(2) in (3).

7.6 Odločitev o certificiranju

Poleg točke 7.6.1 ISO/IEC 17065/2012 bi bilo treba od telesa za certificiranje zahtevati, da v svojih postopkih podrobno opredeli, kako se zagotavljata njegova neodvisnost in odgovornost v zvezi s posameznimi odločitvami o certificiranju.

7.7 Dokumentacija o certificiranju

Poleg točke 7.7.1 (e) ISO/IEC 17065/2012 in v skladu s členom 42(7) SUVP bi bilo treba zahtevati, da obdobje veljavnosti certifikatov ni daljše od treh let.

Poleg točke 7.7.1 (e) ISO/IEC 17065/2012 bi bilo treba zahtevati, da se dokumentira tudi obdobje nameravanega spremljanja v smislu oddelka 7.9.

Poleg točke 7.7.1 (f) ISO/IEC 17065/2012 bi bilo treba od telesa za certificiranje zahtevati, da v dokumentaciji o certificiranju imenuje predmet certificiranja (z navedbo trenutne različice ali podobnih značilnosti, če je to ustrezno).

7.8 Register certificiranih proizvodov

Poleg točke 7.8 ISO/IEC 17065/2012 mora telo za certificiranje hraniti informacije o certificiranih proizvodih, procesih in storitvah, ki so na voljo tako interno kot tudi dostopni javnosti. Telo za

certificiranje zagotovi javno dostopen povzetek poročila o vrednotenju. Cilj tega povzetka je prispevati k preglednosti o tem, kateri predmeti so bili certificirani in kako so bili ocenjeni. V povzetku je pojasnjeno na primer naslednje:

(a) področje uporabe certificiranja in smiseln opis predmeta certificiranja (cilja vrednotenja);

(b) zadevna merila za certificiranje (vključno z različico ali statusom delovanja);

(c) metode vrednotenja in opravljeni testi ter

(d) rezultat(-i).

Poleg točke 7.8 ISO/IEC 17065/2012 in v skladu s členom 43(5) SUVP telo za certificiranje obvesti pristojne nadzorne organe o razlogih za dodelitev ali preklic zaprošenega certifikata.

7.9 Nadzor

Poleg točk 7.9.1, 7.9.2 in 7.9.3 ISO/IEC 17065/2012 in v skladu s členom 43(2)(c) SUVP bi bilo treba v obdobju spremljanja zahtevati obvezne redne ukrepe spremljanja za ohranitev certifikata.

7.10 Spremembe, ki vplivajo na certificiranje

Poleg točk 7.10.1 in 7.10.2 EN ISO/IEC 17065/2012 spremembe, ki vplivajo na certificiranje in ki bi jih moralo upoštevati telo za certificiranje, vključujejo: spremembe zakonodaje o varstvu podatkov, sprejetje delegiranih aktov Evropske komisije v skladu s členom 43(8) in (9), sklepe Evropskega odbora za varstvo podatkov in sodne odločbe v zvezi z varstvom podatkov. Postopki za spremembo, o katerih se je treba dogovoriti, lahko vključujejo naslednje: prehodna obdobja, postopek odobritve s strani pristojnega nadzornega organa, ponovno oceno zadevnega predmeta certificiranja in ustrezne ukrepe za preklic certifikata, če certificirano dejanje obdelave ni več v skladu s posodobljenimi merili.

7.11 Prekinitev, omejitev, začasen odvzem ali preklic certifikata

Poleg poglavja 7.11.1 ISO/IEC 17065/2012 bi bilo treba od telesa za certificiranje zahtevati, da takoj pisno obvesti pristojni nadzorni organ in nacionalni akreditacijski organ, če je to ustrezno, o sprejetih ukrepih ter o nadaljnji veljavnosti, omejitvah, začasnem odvzemu in preklicu certifikata.

V skladu s členom 58(2)(h) mora telo za certificiranje sprejeti odločitve in odredbe pristojnega nadzornega organa o preklicu ali neizdaji certifikata stranki (vložniku), če zahteve glede certificiranja niso ali niso več izpolnjene.

7.12 Evidence

Od telesa za certificiranje bi bilo treba zahtevati, da je vsa dokumentacija, ki jo hrani, popolna, razumljiva, posodobljena in pripravljena za revizijo.

7.13 Pritožbe in ugovori, člen 43(2)(d)

Poleg točke 7.13.1 ISO/IEC 17065/2012 je treba od telesa za certificiranje zahtevati, da določi:

(a) kdo lahko vloži pritožbo ali ugovor;

(b) kdo jih obdeluje pri telesu za certificiranje;

(c) katera preverjanja se v tem primeru opravijo ter

(d) možnosti za posvetovanje z zainteresiranimi stranmi.

Poleg točke 7.13.2 ISO/IEC 17065/2012 je treba od telesa za certificiranje zahtevati, da določi:

(a) kako je treba izdati tako potrditev in komu;

(b) časovne roke za potrditev ter

(c) katere postopke je treba začeti za tem.

Telo za certificiranje mora poleg točke 7.13.1 ISO/IEC 17065/2012 opredeliti, kako se zagotavlja ločevanje dejavnosti certificiranja ter obravnave ugovorov in pritožb.

8 ZAHTEVE ZA SISTEM UPRAVLJANJA

V skladu s poglavjem 8 ISO/IEC 17065/2012 je splošna zahteva za sistem upravljanja, da se izvajanje vseh zahtev iz prejšnjih poglavij v okviru področja uporabe mehanizma certificiranja s strani akreditiranega telesa za certificiranje neodvisno dokumentira, vrednoti, nadzoruje in spremlja.

Osnovno načelo upravljanja je opredeliti sistem, v katerem so cilji učinkovito in uspešno določeni, zlasti izvajanje storitev certificiranja s pomočjo primernih specifikacij. Za to sta potrebna preglednost in preverljivost v zvezi s tem, ali telo za certificiranje izvaja zahteve za akreditacijo in ali te zahteve ves čas izpolnjuje.

V ta namen mora sistem upravljanja določati metodologijo za doseganje in nadzorovanje teh zahtev v skladu s predpisi o varstvu podatkov ter za njihovo stalno preverjanje s strani samega akreditiranega telesa.

Ta načela upravljanja in dokumentiranje njihovega izvajanja morajo biti pregledna in jih mora akreditirano telo za certificiranje razkriti v skladu s postopkom akreditacije in členom 58 in nato na zahtevo nadzornega organa za varstvo podatkov kadar koli med preiskavo v obliki pregledov na področju varstva podatkov iz člena 58(1)(b) ali pregledom certifikatov, izdanih v skladu s členom 42(7), iz člena 58(1)(c).

Akreditirano telo za certificiranje mora zlasti stalno in nenehno javno objavljati, katera certificiranja so bila opravljena in na kateri podlagi (mehanizmi ali sheme certificiranja), kako dolgo so certifikati veljavni, na podlagi katerih okvirov in pod katerimi pogoji (uvodna izjava 100).

8.1 Splošne zahteve za sistem upravljanja

Pristojni nadzorni organ lahko določi in doda nadaljnje dodatne zahteve, če so v skladu z nacionalno zakonodajo.

8.2 Dokumentiranje sistema upravljanja

Pristojni nadzorni organ lahko določi in doda nadaljnje dodatne zahteve, če so v skladu z nacionalno zakonodajo.

8.3 Nadzor dokumentov

Pristojni nadzorni organ lahko določi in doda nadaljnje dodatne zahteve, če so v skladu z nacionalno zakonodajo.

8.4 Nadzor evidenc

Pristojni nadzorni organ lahko določi in doda nadaljnje dodatne zahteve, če so v skladu z nacionalno zakonodajo.

8.5 Pregled upravljanja

Pristojni nadzorni organ lahko določi in doda nadaljnje dodatne zahteve, če so v skladu z nacionalno zakonodajo.

8.6 Notranje revizije

Pristojni nadzorni organ lahko določi in doda nadaljnje dodatne zahteve, če so v skladu z nacionalno zakonodajo.

8.7 Popravni ukrepi

Pristojni nadzorni organ lahko določi in doda nadaljnje dodatne zahteve, če so v skladu z nacionalno zakonodajo.

8.8 Preprečevalni ukrepi

Pristojni nadzorni organ lahko določi in doda nadaljnje dodatne zahteve, če so v skladu z nacionalno zakonodajo.

9 NADALJNJE DODATNE ZAHTEVE[21]

9.1 Posodobitev metod vrednotenja

Telo za certificiranje določi postopke, ki usmerjajo posodabljanje metod vrednotenja vlog v okviru vrednotenja iz točke 7.4. Posodobitev mora potekati v kontekstu sprememb pravnega okvira, zadevnih tveganj, najsodobnejše tehnologije in stroškov izvajanja tehničnih in organizacijskih ukrepov.

9.2 Ohranjanje strokovnega znanja

Telesa za certificiranje vzpostavijo postopke za zagotovitev usposabljanja svojih zaposlenih za posodabljanje njihovih znanj in spretnosti ob upoštevanju razvoja iz točke 9.1.

9.3 Odgovornosti in pristojnosti

9.3.1 Komunikacija med telesom za certificiranje in njegovimi strankami

Vzpostavljeni so postopki za izvajanje ustreznih postopkov in struktur komuniciranja med telesom za certificiranje in njegovo stranko. Ti vključujejo:

1. vzdrževanje dokumentacije o nalogah in odgovornostih s strani akreditiranega telesa za certificiranje za namene:
    a. zahtev za informacije ali
    b. omogočanja stika v primeru pritožbe glede certificiranja;
2. postopek vložitve vloge za namene:
    a. informacij o statusu vloge;
    b. vrednotenj pristojnega nadzornega organa v zvezi s
        i. povratnimi informacijami;
        ii. odločitvami pristojnega nadzornega organa.

9.3.2 Dokumentiranje dejavnosti vrednotenja

Nadzorni organ lahko določi dodatne zahteve.

9.3.3 Upravljanje obravnave pritožb

Obravnava pritožb se vzpostavi kot sestavni del sistema upravljanja, v okviru katerega se zlasti izvajajo zahteve iz točk 4.1.2.2 (c), 4.1.2.2 (j), 4.6 (d) in 7.13 ISO/IEC 17065/2012.

[21] Pristojni nadzorni organ lahko določi in doda nadaljnje dodatne zahteve, če so v skladu z nacionalno zakonodajo.

Relevantne pritožbe in ugovore bi bilo treba posredovati pristojnemu nadzornemu organu.

9.3.4 Upravljanje preklica

Postopki za primer začasnega odvzema ali preklica akreditacije se vključijo v sistem upravljanja telesa za certificiranje, vključno z obveščanjem strank.