UDHËZIM
Nr. 8, datë 20.11.2025

PËR KRITERET SHTESË PËR AKREDITIMIN E ORGANIZMAVE CERTIFIKUES

Në mbështetje të pikës 1, të nenit 38, të pikës 1, të nenit 85 dhe pikës 2, të nenit 97, të ligjit nr. 124/2024, "Për mbrojtjen e të dhënave personale", Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale

UDHËZON:

KREU I
RREGULLA TË PËRGJITHSHME

Neni 1
Objekti

1. Objekti i këtij udhëzimi është përcaktimi i kritereve shtesë për akreditimin e organizmave që do të kryejnë certifikimin, në përputhje me parashikimet e neneve 37 dhe 38, të ligjit nr. 124/2024, "Për mbrojtjen e të dhënave personale".
2. Kriteret shtesë plotësojnë kuadrin ligjor në fuqi dhe të gjitha së bashku përbëjnë mekanizmin certifikues.
3. Të gjitha kriteret dhe parashikimet e standardit ndërkombëtar ISO 17065 (vlerësimi i konformitetit – kriteret për organizmat e certifikimit të produkteve, proceseve dhe shërbimeve) janë të zbatueshme për efekt të akreditimit si organizëm certifikues.
4. Parashikimet e këtij udhëzimi nuk ndryshojnë apo prekin parashikimet e ligjeve të posaçme, rregulloreve apo akteve të tjera nënligjore të miratuara nga Drejtoria e Përgjithshme e Akreditimit apo çdo organizëm kombëtar kompetent për akreditimin, që janë të zbatueshme krahas kritereve të përcaktuara në këtë udhëzim.

Neni 2
Përkufizime

Termat e përdorur në këtë udhëzim kanë të njëjtin kuptim si ato të parashikuara në ligjin nr. 124/2024, "Për mbrojtjen e të dhënave personale", si dhe ISO 17065 (vlerësimi i konformitetit – kriteret për organizmat e certifikimit të produkteve, proceseve dhe shërbimeve). Shtohen në këtë udhëzim edhe përkufizimet e mëposhtme:

a) "Akreditim" është dëshmia/certifikata e lëshuar nga organizmi kombëtar i akreditimit për organizmin certifikues, që përmbush kërkesat e përcaktuara në standardet e harmonizuara bazuar në procedurën dhe kriteret ligjore të parashikuara në ligjin nr. 116/2014, "Për akreditimin e organeve të vlerësimit të konformitetit në Republikën e Shqipërisë", si dhe kriteret shtesë të përcaktuara bazuar në nenin 38, të ligjit nr. 124/2024, "Për mbrojtjen e të dhënave personale", si dhe në këtë udhëzim;

b) "Organizëm certifikues" është çdo person juridik që kryen veprimtari të vlerësimit të konformitetit sipas akreditimit nga Drejtoria e Përgjithshme e Akreditimit, në përputhje me parashikimet e ligjit nr. 116/2014, "Për akreditimin e organeve të vlerësimit të konformitetit në Republikën e Shqipërisë", ligjit nr. 124/2024, "Për mbrojtjen e të dhënave personale", si dhe të këtij udhëzimi;

c) “Drejtoria e Përgjithshme e Akreditimit” është organizmi kombëtar që kryen akreditimin e organeve të certifikimit dhe lëshon dëshminë/certifikatën përkatëse;

ç) “Mekanizëm certifikues” është tërësia e kritereve dhe kompetencave strukturore, funksionale dhe operacionale të nevojshme për kryerjen e aktiviteteve certifikuese që siguron koherencë, qëndrueshmëri dhe paanshmëri;

d) “Skemë certifikimi” nënkupton tërësinë e rregullave dhe procedurave të brendshme, hartuar dhe zbatuar nga organizmi i certifikimit që përfshin mënyrën e verifikimit të përputhshmërisë me kriteret e certifikimit dhe metodologjinë e vlerësimit për certifikimin e veprimit(eve) të përpunimit;

e) “Klient” nënkupton çdo kontrollues ose përpunues të të dhënave personale, që kërkon nga organizmi certifikues, certifikimin e veprimit(eve) përpunuese të të dhënave personale sipas parashikimeve të ligjit nr. 124/2024, “Për mbrojtjen e të dhënave personale” dhe udhëzimit të Komisionerit nr. 9, datë 20.11.2025, “Për kriteret e përgjithshme për certifikimin dhe për dhënien e vulave dhe të shenjave të mbrojtjes së të dhënave personale” (në vijim udhëzimi nr. 9);

ë) “Komisioneri” nënkupton Komisionerin për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale.

KREU II
PROCEDURA E AKREDITIMIT

Neni 3
Parimet e akreditimit

1. Subjekti që synon të akreditohet si organizëm certifikues vërteton se ushtron veprimtarinë certifikuese në përputhje me këto parime:

a) paanësi dhe pavarësi, që nënkupton ushtrimin e veprimtarisë në mënyrë të pavarur, të lirë nga ndikimet e papërshtatshme, si dhe garantimin e vendimmarrjes në mënyrë të paanshme në të gjitha veprimtaritë e certifikimit;

b) konfidencialitet, që nënkupton garancinë për marrjen e masave që parandalojnë aksesin e paautorizuar në informacionin e marrë në kuadër të veprimtarisë certifikuese, përveç kur parashikohet ndryshe në ligj;

c) llogaridhënie, që nënkupton transparencë në vendimmarrjen, lidhur me certifikimin dhe në proceset certifikuese, me qëllim demonstrimin e përputhshmërisë me parashikimet ligjore;

ç) përgjegjësi, që nënkupton marrjen përsipër të përgjegjësisë për veprimtarinë e certifikimit, duke përfshirë përgjegjësinë ligjore që mund të lindë në kuadër të kryerjes së veprimtarisë certifikuese;

d) strukturë organizative të qartë dhe të dokumentuar që siguron funksionim efektiv të veprimtarisë certifikuese dhe përputhshmëri me standardet që zbatohen për këtë natyrë veprimtarie;

e) burime të nevojshme financiare dhe teknike, si dhe trajnim të vazhdueshëm të burimeve njerëzore për të kryer veprimtaritë certifikuese në përputhje me udhëzimin e Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale nr. 9, datë 20.11.2025, “Për kriteret e përgjithshme për certifikimin dhe për dhënien e vulave dhe të shenjave të mbrojtjes së të dhënave personale”.

2. Zbatueshmëria e këtyre parimeve është objekt i monitorimit nga Komisioneri në përputhje me parashikimet e ligjit nr. 124/2024, “Për mbrojtjen e të dhënave personale” dhe këtij udhëzimi.

Neni 4

Akreditimi

1. Subjekti që synon të akreditohet si organizëm certifikues kryen procedurën e akreditimit pranë Drejtorisë së Përgjithshme të Akreditimit, në përputhje me parashikimet e ligjit nr. 116/2014, "Për akreditimin e organeve të vlerësimit të konformitetit në Republikën e Shqipërisë".

2. Akreditimi lëshohet për një afat maksimal prej 5 (pesë) vjetësh dhe mund të rinovohet me të njëjtat kushte si akreditimi fillestar.

Neni 5

Lista e dokumenteve për akreditim

1. Subjekti që synon akreditimin paraqet dokumentet e mëposhtme që vërtetojnë përmbushjen e kritereve ligjore të parashikuara në nenin 38, pika 2, të ligjit nr. 124/2024, "Për mbrojtjen e të dhënave personale" dhe ato shtesë të përcaktuara në këtë udhëzim:

a) dokumente ose akte të autoriteteve vendase apo të huaja që vërtetojnë nivelin e duhur të njohurive, në lidhje me veprimtarinë e certifikimit, të vulave ose shenjave, si dhe zbatimin e mbrojtjes së të dhënave për veprimin përpunues, objekt certifikimi;

b) dokumente ose akte të brendshme të subjektit që vërtetojnë krijimin e Komitetit për Garantimin e Pavarësisë, miratuar nga organet e brendshme kompetente sipas statutit apo aktit të themelimit, që provojnë pavarësi dhe angazhim në ushtrimin e përgjegjësive dhe detyrave në mënyrë të tillë që nuk shkakton konflikt interesi sipas parashikimeve të këtij udhëzimi;

c) dokumente ose akte që demonstrojnë një skemë certifikimi, që konsiston në dokumentimin e kritereve, procedurave ose protokolleve, që do të zbatohen për vlerësimin e veprimit(eve) të përpunimit të të dhënave personale, rishikimin periodik, pezullimin dhe shfuqizimin e certifikimit, vulave dhe shenjave të mbrojtjes së të dhënave personale;

ç) dokumente ose akte të brendshme të subjektit që pasqyrojnë angazhim për të respektuar kriteret e certifikimit të përcaktuara në udhëzimin nr. 9 dhe mekanizmin e certifikimit, të miratuar nga organet përkatëse sipas statutit apo aktit të themelimit;

d) dokumente ose akte të brendshme të subjektit që përcaktojë procedura dhe struktura përgjegjëse për shqyrtimin e ankesave për shkeljen e procedurës së certifikimit ose mënyrën sesi është zbatuar, ose po zbatohet certifikimi nga kontrolluesi ose përpunuesi, si dhe për t'i bërë këto procedura dhe struktura transparente për subjektet e të dhënave dhe publikun;

dh) model marrëveshjeje për certifikim që nënshkruhet midis organizimit certifikues dhe klientëve;

e) dokumente ose akte të brendshme që tregojnë angazhimin e subjektit që synon akreditim për ruajtjen e konfidencialitetit;

ë) dokumente ose akte që parashikojnë përputhshmërinë, lidhur me kërkesat për aksesin në informacion sipas nenit 11 të këtij udhëzimi;

f) dokumente ose akte që vërtetojnë përputhshmërinë me kriterin e përgjegjësisë, sipas nenit 12 të këtij udhëzimi;

g) dokumente ose akte që vërtetojnë përputhshmërinë me kriterin strukturor, sipas nenit 13 të këtij udhëzimi;

gj) dokumente ose akte që vërtetojnë përputhshmërinë në lidhje me burimet, sipas nenit 14 të këtij udhëzimi;

h) dokumente ose akte të autoriteteve vendase apo të huaja që vërtetojnë përshtatshmërinë teknike, aftësinë, certifikimin apo trajnimin e stafit;

i) dokumente ose akte të brendshme që tregojnë mënyrën e trajtimit dhe parandalimit të situatave të konfliktit të interesit;

j) dokumente ose akte të brendshme që përcaktojnë procedurën që do të ndiqet në rast shkeljeje të procedurës së certifikimit ose shkeljeve gjatë zbatimit të certifikimit nga ana kontrolluesit ose përpunuesit.

2. Parashikimet e pikës 1 të këtij neni nuk cenojnë të drejtën e Drejtorisë së Përgjithshme të Akreditimit për të kërkuar paraqitjen e dokumenteve të tjera, në përputhje me parashikimet e ligjit nr. 116/2014, "Për akreditimin e organeve të vlerësimit të konformitetit në Republikën e Shqipërisë" dhe akteve nënligjore të miratuara në zbatim të tij.

KREU III
KRITERET E AKREDITIMIT

Neni 6
Detyrimet ligjore të organizimit certifikues

1. Pavarësisht përmbushjes së kritereve të parashikuara në pikën 4.1.1 të ISO 17065, organizmi certifikues, gjatë ushtrimit të veprimtarisë certifikuese zbaton procedura të përditësuara, në lidhje me përgjegjësitë ligjore sipas parashikimeve të këtij udhëzimi.

2. Organizmi i certifikimit zbaton procedura dhe masa për përpunimin e të dhënave personale të klientëve si pjesë e procesit të certifikimit, në përputhje me parashikimet e ligjit nr. 124/2024, "Për mbrojtjen e të dhënave personale". Të dhënat për këto masa dhe procedura i vihen në dispozicion Komisionerit për të verifikuar kontrollin dhe menaxhimin e të dhënave të klientit.

3. Organizmi i certifikimit njofton Drejtorinë e Përgjithshme të Akreditimit për çdo ndryshim thelbësor të rrethanave faktike apo ligjore që lidhen me certifikimin, menjëherë dhe në çdo rast jo më vonë se 15 ditë pas evidentimit të rrethanës. Rrethana thelbësore janë ato rrethana që ndikojnë në aftësinë e organizmit certifikues për të dhënë certifikime të besueshme dhe të arsyetuara, duke përfshirë por pa u kufizuar vetëm tek llogaridhënia, paanësia, kapaciteti financiar, konfidencialiteti, transparenca, kompetenca dhe trajtimi i menjëhershëm i ankesave.

4. Organizmi i certifikimit konfirmon që nuk ekzistojnë procedura ligjore që mund të rezultojnë në mospërputhshmëri me kriteret e akreditimit sipas nenit 38, të ligjit nr. 124/2024, "Për mbrojtjen e të dhënave personale" dhe këtij udhëzimi.

Neni 7
Marrëveshja e certifikimit

1. Përveç përmbushjes së kritereve të parashikuara në pikën 4.1.2 të ISO 17065, marrëveshja e certifikimit e nënshkruar përkatësisht nga përfaqësuesit ligjorë të organizmit certifikues dhe klientit përfshin dhe përmban dakordësinë e palëve, në lidhje me këto aspekte:

a) përputhshmërinë me kriteret e certifikimit dhe zbatimin e çdo përditësimi që komunikohet nga organizmi certifikues;

b) dhënien e aksesit në informacion, dokumentacion, regjistra, pajisje, vendndodhje, personel ose informacion për kontraktorët apo nënkontraktorët e klientit në mënyrë që organizmi certifikues të kryejë procedurën e certifikimit, në përputhje me ligjin nr. 124/2024, "Për mbrojtjen e të dhënave personale" dhe parashikimet e udhëzimit nr. 9;

c) përmbylljen/përfundimin brenda afateve të procedurës së certifikimit të parashikuar në skemën përkatëse të certifikimit;

ç) njoftimin e organizmit certifikues për ndryshime thelbësore në statusin ligjor, veprimet e përpunimit të të dhënave personale, përputhshmërinë me kriteret e certifikimit ose informacionin mbi dokumentin formal të certifikimit. Ndryshime thelbësore të produktit, proceseve dhe shërbimeve janë ato që përbëjnë ndryshime në objektin e certifikimit, pasi

nënkuptojnë shtesa ose ndryshime thelbësore të objektit të certifikimit apo llojit të produktit, objektit të përpunimit dhe mënyrës së dhënies së shërbimeve;

d) bashkëpunimin për veprimtaritë monitoruese, auditimin periodik dhe masat korrigjuese që kërkohen nga organizmi certifikues. Mospërmbushja e këtij detyrimi passjell pezullimin apo shfuqizimin e certifikimit për subjektin që i nënshtrohet certifikimit, në përputhje me parashikimet e udhëzimit të Komisionerit nr. 9, datë 20.11.2025, "Për kriteret e përgjithshme për certifikimin dhe për dhënien e vulave dhe të shenjave të mbrojtjes së të dhënave";

e) raportimin e menjëhershëm të çdo shkeljeje ligjore apo rregullatore që mund të passjellë mospërputhje me kriteret e certifikimit.

2. Marrëveshja e certifikimit përmban, gjithashtu, parashikime në lidhje me:

a) përgjegjësinë për klientin që certifikimi nuk i përjashton ata nga detyrimet ligjore sipas legjislacionit për mbrojtjen e të dhënave personale;

b) metodat e vlerësimit, ankesat dhe procedurat përkatëse, si dhe detyrimet ndaj klientit, në lidhje me këto procese që janë të përcaktuara nga organizmi i certifikimit, në përputhje me pikën 4.1.2.2 të ISO 17065 dhe parashikimet e këtij udhëzimi;

c) rregullat për vlefshmërinë, rinovimin, pezullimin dhe shfuqizimin e certifikimit, duke përfshirë rivlerësimin periodik në përputhje me pikën 4.1.2.2 të ISO 17065 dhe parashikimet e këtij udhëzimi;

d) pasojat e përfundimit të afatit, pezullimit, shfuqizimit apo moslëshimit të certifikatës, si dhe veprimet për të mbajtur ose rinovuar certifikimin.

Neni 8

Përdorimi i certifikatës, vulës dhe shenjës

1. Përveç përmbushjes së kritereve të parashikuara në pikën 4.1.3 të ISO 17065, organizmi i certifikimit, nëpërmjet krijimit/hartimit të një mekanizmi të brendshëm, ruan kontrollin mbi përdorimin dhe ekspozimin e certifikatës, vulës dhe shenjës, si dhe çdo aspekti tjetër të certifikimit duke siguruar që:

a) mekanizmi i certifikimit është qartësisht i identifikueshëm. Komunikimet përshkruajnë në mënyrë transparente objektin e veprimit(eve) përpunues/e që përfshihen në certifikim;

b) objekti i certifikimit është i përcaktuar qartë dhe shmang çdo keqinterpretim, në lidhje me veprimin(et) përpunues/e të vlerësuara në kuadër të procesit të certifikimit;

c) rregullat për përdorimin e vulës certifikuese zbatohen vetëm për klientët e certifikuar.

2. Çdo përdorim i pasaktë, çorientues apo që mund të keqinterpretohet i certifikatës, vulës ose shenjës, ose çdo aspekti tjetër të certifikimit, adresohet nëpërmjet instrumenteve korrigjuese të zbatueshme, që duhet të përfshijnë të paktën sa më poshtë:

a) kërkesën ndaj klientit për shmangien e praktikës së pasaktë apo që mund të shpjerë në keqinterpretim;

b) garantimin që klienti përditëson informacionin publik nëpërmjet mjeteve të komunikimit të ngjashme me ato që janë zbatuar më parë;

c) njoftimin e organizmit të certifikimit pa vonesë, në lidhje me mospërputhshmërinë dhe masat korrigjuese të ndërmarra.

3. Masa të tjera shtesë që vlerësohen nga organizmi i certifikimit mund të përfshijnë pezullimin ose shfuqizimin e certifikimit, publikimin e cenimit dhe nëse konsiderohet e nevojshme ndërmarrjen e procedurave ligjore.

Neni 9

Paanësia dhe pavarësia

1. Përveç përmbushjes së kritereve të parashikuara në pikën 4.2 të ISO 17065, organizmi i certifikimit garanton paanësi dhe pavarësi në ushtrimin e veprimtarisë certifikuese nëpërmjet krijimit, organizimit dhe funksionimit të një komiteti të posaçëm, me pjesëmarrje të balancuar të përfaqësuesve të grupeve të interesit, duke siguruar që asnjë interes të mos mbizotërojë. Komiteti zhvillon takime periodike, të paktën një herë në vit, për të vlerësuar rreziqet lidhur me pavarësinë dhe efektivitetin e masave të zbatuara nga organizmi i certifikimit. Organizmi i certifikimit paraqet dokumente ose akte që vërtetojnë pavarësinë, veçanërisht sa i takon financimit duke përfshirë, por pa u kufizuar vetëm në:

a) statutin dhe aktin e themelimit;

b) rregullat dhe procedurat e brendshme që lidhen me përbërjen, emërimin, shpërblimin dhe kohëzgjatjen e mandatit të anëtarëve të organizmit që kanë kompetenca vendimmarrëse mbi certifikimin;

c) dokumente që pasqyrojnë marrëdhëniet tregtare, financiare, kontraktuale ose të një natyre tjetër midis organizmit të certifikimit dhe klientëve, duke përfshirë pasqyrat financiare vjetore dhe evidentimin e burimeve të financimit.

2. Organizmi i certifikimit sigurohet që të mos mbajë marrëdhënie të çfarëdo lloji me klientin që është në proces vlerësimi. Veçanërisht, organizmi i certifikimit identifikon rreziqet e paanësisë dhe pavarësisë në mënyrë të rregullt dhe merr masa efektive për të mënjanuar rreziqet që rezultojnë nga veprime të palëve të treta, duke përfshirë individë, subjekte tregtare ose organe publike. Rreziku për paanësi dhe pavarësi përfshin kërcënimet që vijnë nga marrëdhënie financiare, tregtare, kontraktuale ose individuale.

3. Organizmi i certifikimit sigurohet për çdo klient që:

a) personeli i përfshirë në proces vlerësimi, shqyrtimi apo vendimmarrje të mos ketë marrëdhënie me klientin përtej veprimtarisë, në kuadër të procesit certifikues dhe nuk kryen veprime të tjera që mund të cenojnë paanësinë;

b) klienti nuk ka marrëdhënie familjare apo të një natyre tjetër që mund të përbëjë rrezik për paanësinë e organizmit të certifikimit;

c) nuk ekziston asnjë marrëdhënie financiare, përtej veprimtarisë në kuadër të procesit të certifikimit, midis organizmit të certifikimit dhe klientit. Organizmi i certifikimit dokumenton dhe menaxhon rrezikun për paanësinë.

4. Organizimi i brendshëm garanton që funksionet, detyrat dhe strukturat organizative të mos lenë vend për dyshime mbi konflikt interesi. Organizmi i certifikimit krijon dhe siguron zbatimin e një mekanizmi të brendshëm që garanton identifikimin, parandalimin dhe menaxhimin efektiv të konfliktit të interesit. Të gjithë punonjësit deklarojnë çdo konflikt aktual, të mundshëm apo të perceptuar të interesit sipas procedurave të brendshme të miratuara nga organi përkatës i organizmit të certifikimit. Konfliktet mund të lindin, por pa u kufizuar vetëm, në situatat e mëposhtme:

a) organizmi i certifikimit ka marrëdhënie financiare me klientin, që ushtron ndikim në të ardhurat ose influencë financiare;

b) organizmi i certifikimit ose punonjës të tij kanë kuota ose aksione në shoqërinë që jep shërbime konsulence, lidhur me produktet, proceset apo shërbimet që do të certifikohen;

c) organizmi i certifikimit nuk angazhohet në shërbime konsulence ose aktivitete të tjera që cenojnë paanësinë dhe pavarësinë, duke përfshirë por pa u kufizuar, veprimtarinë si nëpunës i mbrojtjes së të dhënave personale ose shërbime konsulence në lidhje me përputhshmërinë me legjislacionin për mbrojtjen e të dhënave personale.

5. Niveli drejtues dhe personeli përgjegjës i organizmit të certifikimit që angazhohet në vlerësimin e përputhshmërisë nuk duhet:

a) të ketë marrë pjesë në projektimin, prodhimin, shpërndarjen, instalimin apo blerjen e produktit, procesit ose shërbimit që i nënshtrohet vlerësimit;

b) të jetë zotërues, përdorues ose mirëmbajtës i produktit, procesit ose shërbimit në fjalë;

c) të veprojë si person i autorizuar i subjekteve që janë përfshirë në rolet e përmendura në pikën 5/“b” të këtij neni.

6. Organizmi i certifikimit zbaton procedura dhe mekanizma të brendshëm për identifikimin e vazhdueshëm dhe menaxhimin e rrezikut për paanësi dhe pavarësi, dhe sigurohet që i gjithë personeli të ruajnë pavarësinë dhe paanësinë në të gjitha aktivitetet certifikuese.

7. Përveç kritereve të parashikuara në pikën 4.4 të ISO 17065, organizmi i certifikimit zbaton procedura certifikimit të drejta dhe jo diskriminuese, dhe siguron akses të barabartë në këto procedura certifikimi pavarësisht përmasave të klientit, përkatësisë, origjinës së produktit dhe siguron zbatueshmërinë e procedurës në mënyrë të barabartë tek të gjithë klientët.

Neni 10
Konfidencialiteti

1. Përveç kritereve të parashikuara në pikën 4.5 të ISO 17065, organizmi i certifikimit është përgjegjës për administrimin e informacionit të mbledhur, krijuar ose përdorur në kuadër të veprimtarisë së certifikimit. Organizmi i certifikimit i garanton klientëve aktualë ose të ardhshëm që personeli i tij, veçanërisht ai i angazhuar në proces vlerësimi dhe vendimmarrjeje, ruan konfidencialitetin e informacionit nëpërmjet zbatimit të marrëveshjeve të konfidencialitetit, vetëdeklarimeve ose dokumenteve të tjera me natyrë detyruese. Detyrimi përfshin të gjithë informacionin, pavarësisht natyrës sensitive, tregtare, pronësore, sekretin tregtar, procesin(et) tregtare, dokumentimin teknik dhe të dhënat personale, pa cenuar detyrimin e organizmit të certifikimit për të vepruar në përputhje me kuadrin ligjor për transparencë ose përmbushje të detyrimeve ligjore.

2. Detyrimi sipas pikës 1 të këtij neni nuk pengon organizmin e certifikimit të publikojë kriteret e certifikimit, metodologjinë dhe rezultatet e natyrës jokonfidenciale.

Neni 11
Llogaridhënia dhe aksesi në informacion

1. Përveç kritereve të parashikuara në pikën 4.6 të ISO 17065, organizmi i certifikimit publikon dhe mundëson akses për publikun, në lidhje me:

a) të gjitha versionet (në fuqi dhe të shfuqizuara) e kritereve të certifikimit, duke specifikuar periudhën e vlefshmërisë përkatëse;

b) procedurat e përditësuara të certifikimit duke përfshirë edhe atë për ankim;

c) informacion rreth procedurës së certifikimit që zbatohet në praktikë, duke përfshirë informacion për të dhënat e subjektit që preket nga përpunimi i të dhënave sipas objektit të certifikimit, si dhe mënyrën për të paraqitur dhe trajtuar ankesën;

ç) regjistër publik të vulave dhe shenjave të regjistruara.

Neni 12
Përgjegjësia

1. Përveç kritereve të parashikuara në pikën 4.3 të ISO 17065, organizmi i certifikimit krijon dhe zbaton masa të përshtatshme, të tilla si sigurimi profesional ose rezerva financiare, për të mbuluar çdo përgjegjësi që rrjedh nga veprimtaritë certifikuese. Organizmi i certifikimit zbaton masa të përshtatshme për të siguruar mbulim tërësor të juridiksionit dhe përmbushja e këtij detyrimi është objekt verifikimi nga Drejtoria e Përgjithshme e Akreditimit.

2. Organizmi i certifikimit vërteton përmbushjen e detyrimit që lidhet me përgjegjësinë nëpërmjet dokumenteve/akteve ose vërtetimeve (polica sigurimi), si më poshtë:

a) sigurim profesional për mbulim të përgjegjësive që rrjedhin nga veprimtaritë e certifikimit;

b) nuk është në procedurë likuidimi ose falimentimi sipas legjislacionit në fuqi;

c) ka shlyer të gjitha detyrimet për kontributet shëndetësore dhe shoqërore sipas legjislacionit në fuqi;

ç) nuk është në procedurë ekzekutimi të detyrimeve tatimore;

d) përfaqësuesi ligjor nuk është dënuar me vendim të formës së prerë për vepra penale që lidhen me veprimtarinë e organizmit të certifikimit.

3. Organizmi i certifikimit kryen një vlerësim rreziku në lidhje me veprimtarinë certifikuese dhe zbaton masa të përshtatshme për të mënjanuar rreziqet e identifikuara, si dhe vendos në dispozicion të Drejtorisë së Përgjithshme të Akreditimit dhe Komisionerit dokumentacionin përkatës, nëse kërkohet. Rreziqet që lidhen me veprimtaritë e certifikimit mund të përfshijnë, por pa u kufizuar vetëm në sa më poshtë:

a) përcaktimin objektivave të auditit;

b) mënyrat e mbledhjes së të dhënave gjatë procesit të auditit;

c) rrezikun ekzistues dhe të perceptuar për paanshmërinë;

d) çështje që lidhen me përgjegjësinë dhe detyrimet ligjore, duke përfshirë përputhshmërinë me legjislacionin për mbrojtjen e të dhënave personale;

e) karakteristikat organizative dhe operative të klientit të audituar;

f) efektin e mundshëm të auditit te klienti dhe veprimtaritë që ushtron;

g) aspektet e shëndetit dhe sigurisë për ekipin auditues;

h) deklarata të pasakta ose çorientuese të klientit;

i) përdorimi dhe mbrojtja e markave tregtare.

4. Masat e përshtatshme për të mënjanuar rrezikun e identifikuar mund të përfshijnë, ndër të tjera, edhe kontraktimin e policave të sigurimit që mbulojnë pretendime të mundshme, duke krijuar zëra buxhetorë të mjaftueshëm ose masa të ngjashme. Organizmi i certifikimit kryen vlerësime periodike të rrezikut, të paktën një herë në vit, për të identifikuar rreziqet që mund të vijnë ose ato që kanë ndryshuar, në lidhje me veprimtarinë dhe personelin.

Neni 13

Kriteret strukturore

1. Kriteret e parashikuara në pikën 5.1 të ISO/IEC 17065 zbatohen në lidhje me organizimin strukturor dhe nivelin e lartë drejtues.

2. Kriteret e parashikuara në pikën 5.2 të ISO/IEC 17065 zbatohen për mekanizmat që garantojnë paanësinë.

Neni 14

Burimet

1. Përveç kritereve të parashikuara në pikën 6.1 të ISO 17065, organizmi i certifikimit krijon, zbaton dhe mban procedura drejtimi që vërtetojnë se personeli gëzon aftësitë, njohuritë dhe ekspertizën e nevojshme për të kryer veprimtaritë e certifikimit. Informacioni mbi personelin përpunohet në mënyrë të ligjshme, të drejtë dhe transparente, në përputhje me legjislacionin për mbrojtjen e të dhënave personale. Organizmi i certifikimit siguron që personeli të ketë në përbërje individë me njohuri teknike dhe ligjore të nevojshme për procesin e certifikimit, përfshirë fushën e mbrojtjes së të dhënave personale, rregullat që zbatohen për mbrojtjen e të dhënave të klientëve, masat teknike dhe organizative për mbrojtjen e të dhënave personale, si dhe vlerësimin dhe auditimin e veprimeve të përpunimit të të dhënave.

2. Organizmi i certifikimit siguron dhe paraqet dokumentacionin e nevojshëm që vërteton njohuritë teknike të personelit, duke përfshirë:

a) diplomë në shkenca kompjuterike, sistemet e informacionit ose sigurisë kibernetike apo në fusha të ngjashme;

b) të paktën 5 vjet eksperiencë profesionale në mbrojtjen e të dhënave personale;

c) të paktën 2 ditë trajnim, në lidhje me menaxhimin e sigurisë së sistemit të informacionit, duke përfshirë rregullat, standardet, metodat, praktikat e mira dhe menaxhimin e rrezikut.

3. Organizmi i certifikimit siguron dhe paraqet dokumentacionin e nevojshëm që vërteton njohuritë ligjore të personelit, duke përfshirë:

a) diplomë në nivelin master ose kualifikim ekuivalent;

b) të paktën 5 vjet eksperiencë profesionale në fushën e mbrojtjes së të dhënave personale.

4. Organizmi i certifikimit siguron forcim të vazhdueshëm të kapaciteteve të personelit nëpërmjet programeve të trajnimit profesional që përfshijnë standardet teknike, kriteret rregullatore dhe detyrimet, lidhur me mbrojtjen e të dhënave personale. Trajnimi dhe përditësimi i njohurive/aftësive kryhet çdo vit dhe dokumentohet në mënyrë formale.

5. Organizmi i certifikimit siguron personel me njohuritë teknike dhe aftësitë/eksperiencën, si më poshtë:

a) për vlerësuesit, të paktën 2 vjet eksperiencë profesionale në fushën e të dhënave personale, përfshirë analizimin dhe zbatimin e masave teknike dhe organizative për mbrojtjen e të dhënave personale, testime për sigurinë, vlerësime teknike ose certifikime;

b) për drejtuesit ose vendimmarrësit, të paktën 2 vjet eksperiencë profesionale në identifikimin, përcaktimin, monitorimin dhe këshillimin për masa të mbrojtjes së të dhënave personale.

6. Organizmi i certifikimit siguron personel me njohuritë ligjore dhe aftësitë/eksperiencën, si më poshtë:

a) për vlerësuesit, të paktën 2 vjet eksperiencë profesionale në fushën e mbrojtjes së të dhënave personale, përfshirë analizimin ose zbatimin e përputhshmërisë së veprimeve të përpunimit të të dhënave personale, auditeve, ose rishikimit të kontratave;

b) për drejtuesit ose vendimmarrësit, të paktën 2 vjet eksperiencë profesionale në monitorim të përputhshmërisë ose këshillim në fushë e mbrojtjes së të dhënave personale.

7. Përveç kritereve të parashikuara në pikën 6.2 të ISO 170656, në lidhje me pavarësinë nga interesat tregtarë apo interesa të tjerë me klientin, personeli i angazhuar në procesin e certifikimit vepron në përputhje me rregullat e miratuara nga organizmi i certifikimit.

8. Organizmi i certifikimit përdor informacionin për personelin për të identifikuar dhe mënjanuar rreziqet lidhur me paanësinë që rrjedhin nga veprimtaritë ose lidhjet institucionale. Të gjithë konfliktet e mundshme të interesit verifikohen dhe mënjanohen për të siguruar që personeli ruan pavarësinë nga interesat tregtarë ose interesa të tjerë me klientin.

9. Në rast se veprimtaritë e certifikimit kryhen nga subjekte të nënkontraktuara, organizmi i certifikimit siguron që subjekti i nënkontraktuar dhe personeli i tij përmbushin kriteret e zbatueshme në lidhje me veprimtaritë e vlerësimit.

10. Në përputhje me pikat 6.2.24 dhe 7.6.1 të ISO 17065, organizmi i certifikimit mban përgjegjësi të plotë dhe përgjigjet për të gjitha aktivitetet e nënkontraktuara dhe siguron që subjekti i nënkontraktuar dhe personeli i tij të plotësojë të gjitha kriteret e zbatueshme, duke përfshirë parashikimet e ligjit nr. 124/2024, “Për mbrojtjen e të dhënave personale” dhe mbetet përgjegjës mbi vendimmarrjet që lidhen me certifikimin.

KREU IV
ZBATIMI I PROCESIT TË CERTIFIKIMIT

Neni 15

Zbatimi i ISO 17065

Kriteret e pikës 7.1 të ISO 17065 zbatohen në kuadër të procesit të certifikimit. Veprimi(et) e përpunimit të të dhënave personale vlerësohen sipas kritereve ligjore të parashikuara në ligjin nr. 124/2024, "Për mbrojtjen e të dhënave personale" dhe këtë udhëzim.

Neni 16
Paraqitja e kërkesës nga klienti

1. Klienti paraqet pranë organizmit të certifikimit kërkesën me shkrim për vlerësim dhe certifikim. Kërkesa specifikon bashkëpunimin që mund të ekzistojë midis klientit dhe palëve të treta për kontrollin ose angazhimin e përpunuesve të të dhënave që do të jenë objekt i certifikimit. Në rast se klienti vepron si bashkëkontrollues ose bashkëpërpunues, kërkesa specifikon përgjegjësitë e klientit, detyrat dhe dokumentacionin kontraktual dhe ligjor mbi të cilat mbështetet bashkëpunimi.

2. Përveç kritereve të parashikuara në pikën 7.2 të ISO 17065, klienti i paraqet organizmit të certifikimit informacionin, si më poshtë, në lidhje me vlerësimin:

a) përshkrim të detajuar të objektit të vlerësimit, duke përfshirë aspekte që lidhen me ndërfaqen me sisteme të jashtme ose subjekte të tjera, protokollet e zbatuara dhe garancitë për sigurinë e komunikimit të të dhënave;

b) listë të transferimeve ndërkombëtare të të dhënave, duke përfshirë kuadrin ligjor të marrësit të të dhënave dhe garancitë që janë zbatuar për mbrojtjen e tyre;

c) listë të përpunuesve të të dhënave ose nënpërpunuesve, duke përfshirë përgjegjësitë, veprimtaritë e përpunimit të të dhënave, kontratat kryesore ose model mbi të cilat bazohet marrëdhënia me klientin;

ç) listën e bashkëkontrolluesve, duke përfshirë përgjegjësitë dhe detyrat, si dhe parimet dhe instrumentet ligjore mbi të cilat bazohet marrëdhënia me klientin;

d) karakteristikat e përgjithshme të veprimeve të përpunimit të të dhënave që do të jenë objekt i certifikimit, duke përfshirë vendndodhjen fizike ku përpunohen të dhënat, kategorinë e të dhënave, si dhe detyrimet ligjore të zbatueshme;

dh) informacion mbi certifikimet ose rezultate të tjera të vlerësimeve që janë kryer më parë, në rast se ka pasur të tilla, dhe nëse natyra e këtyre vlerësimeve, si dhe objekti i tyre mund të konsiderohet në kuadër të procesit të certifikimit;

e) informacion në lidhje me hetime, sanksione të vendosura rishtazi ose masa korrigjuese të vendosura nga Komisioneri ose autoritete të tjera kompetente, në lidhje me përpunimin e të dhënave personale në kuadër të objektit të certifikimit;

ë) në rast se përpunimi i të dhënave personale mund të përbëjë rrezik të lartë për të drejtat dhe liritë e individit, të tilla si përpunimi i të dhënave sensitive ose përdorimi i teknologjive të avancuara ose procese vendimmarrëse automatike, klienti kryen dhe paraqet një vlerësim ndikimi në mbrojtjen e të dhënave në përputhje me nenin 31, të ligjit nr. 124/2024, "Për mbrojtjen e të dhënave personale".

Neni 17
Shqyrtimi i kërkesës për certifikim

1. Organizmi i certifikimit shqyrton kërkesën në përputhje me pikën 7.3 të ISO 17065 dhe parashikimet e pikës 2 të këtij neni.

2. Përveç përmbushjes së kritereve të parashikuara në pikën 7.3.1, organizmi i certifikimit vlerëson dokumentacionin e paraqitur dhe sigurohet që:

a) klienti të jetë kandidat i përshtatshëm për vlerësimin përkundrejt kritereve të certifikimit duke pasur parasysh rregullat e përcaktuara në mekanizmin e certifikimit, si dhe verifikon që klienti dhe veprimet e përpunimit të të dhënave janë brenda fushës së certifikimit, përgjegjësitë e klientit sipas kuadrit ligjor për mbrojtjen e të dhënave personale dhe llojet e veprimeve të përpunimit të të dhënave për të cilat janë miratuar kritere certifikimi;

b) ka metoda të përshtatshme vlerësimi për klientin, duke pasur parasysh rregullat e përcaktuara në skemën e certifikimit, kuadrin ligjor për mbrojtjen e të dhënave personale dhe çdo hetim në proces, sanksione të vendosura rishtazi ose masa korrigjuese të vendosura nga Komisioneri. Metodat e vlerësimit zbatohen në klientë të ngjashëm për të prodhuar rezultate të krahasueshme;

c) ka njohuritë e nevojshme teknike dhe ligjore në mbrojtjen e të dhënave personale për të kryer veprimtaritë e certifikimit, veçanërisht në rast se nuk ka pasur eksperiencë të mëparshme në kryerjen e vlerësimeve me objekt të njëjtë ose të ngjashëm.

3. Në rast se skema e certifikimit përcakton rregulla për llogaritjen e kohëzgjatjes së veprimtarisë së certifikimit, organizmi i certifikimit zbaton një procedurë për të llogaritur kohëzgjatjen e vlerësimit, duke pasur parasysh:

a) shkallën e veprimeve të përpunimit të të dhënave që do të jenë objekt certifikimi;

b) natyrën e të dhënave të përpunuara;

c) rreziqet për subjektet e të dhënave;

ç) kompleksitetin e teknologjive të përdorura;

d) angazhimin e përpunuesve të të dhënave;

e) numrin e vendeve ose strukturave në të cilat kryhet përpunimi i të dhënave të klientit.

4. Organizmi i certifikimit llogarit kohëzgjatjen e auditimit, në përputhje me skemën e certifikimit dhe përcakton nëse është e mjaftueshme për të përmbyllur vlerësimin ose nëse nevojitet kohë shtesë. Kohëzgjatja e auditit vendoset në marrëveshjen midis organizmit të certifikimit dhe klientit.

5. Organizmi i certifikimit siguron që marrëveshja e certifikimit të përmbajë metodologjinë e detyrueshme të vlerësimit të klientit dhe që vlerësimi të përfshijë në mënyrë të arsyeshme kompetencat teknike dhe ligjore në fushën e mbrojtjes së të dhënave personale. Posedimi i këtyre kompetencave vlerësohet i përmbushur kur personeli i angazhuar në procesin e certifikimit përmbush kriteret teknike dhe ligjore të parashikuara në nenin 14 të këtij udhëzimi, duke përfshirë dokumentimin, lidhur me formimin dhe eksperiencën profesionale, si dhe ndjekjen e trajnimeve të vazhdueshme.

6. Organizmi i certifikimit ruan regjistrat që vërtetojnë kompetencat dhe verifikon përmbushjen e kritereve për të gjithë personelin, duke përfshirë, sipas rastit, edhe ato për vlerësuesit e nënkontraktuar.

Neni 18

Plani i vlerësimit

Përveç kritereve të parashikuara në pikën 7.4 të ISO 17065, organizmi i certifikimit harton dhe zbaton një plan vlerësimi që parashikon zbatimin e metodologjisë së vlerësimit të parashikuar në marrëveshje. Metodologjia mund të përfshijë vlerësime në terren, dokumentare, kryerjen e auditeve, intervistave ose zbatimin e instrumenteve të tjera të përshtatshme për të mbledhur gjetje që vërtetojnë plotësimin e kritereve të vlerësimit. Plani i vlerësimit përmban një vlerësim rreziku dhe vlerësimin e ndikimit në mbrojtjen e të dhënave për veprime përpunimi me rrezik të lartë për liritë dhe të drejtat themelore të individëve.

Neni 19

Metodologjia e vlerësimit

1. Devijimi nga metodologjia e vlerësimit dokumentohet duke parashtruar arsyet, vlerësimin e rrezikut dhe efektet e gjetjeve që janë me vlerë për certifikimin.

2. Organizmi i certifikimit siguron që metodologjia e vlerësimit të jetë e përshtatshme për të vlerësuar përmbushjen e kritereve të certifikimit, e standardizuar dhe e zbatueshme. Metodologjia e vlerësimit përfshin respektimin e kritereve ligjore të certifikimit të përmendura në këtë udhëzim. Organizmi i certifikimit siguron dokumentimin dhe ruajtjen e metodologjisë së zbatuar dhe rezultateve përkatëse. Metodologjia e vlerësimit përshtatet për tipologjinë, kompleksitetin dhe nivelin e rrezikut të veprimeve të përpunimit për të siguruar që përpunimi me rrezik të lartë të vlerësohet në mënyrë të plotë.

3. Detyrat lidhur me vlerësimin mund t'i caktohen personelit të brendshëm ose ekspertëve të jashtëm të miratuar nga organizmi i certifikimit, me kusht që ekipi i angazhuar në vlerësim të përmbushë kriteret për njohuritë ligjore dhe teknike të përmendura në nenin 14 të këtij udhëzimi. Organizmi i certifikimit siguron që klienti të plotësojë kriteret e mekanizmit të certifikimit, në rast se i bëhet referencë rezultateve të mëparshme të certifikimit. Raportet e mëparshme të vlerësimit janë të aksesueshme dhe gjetjet e tjera dokumentohen.

4. Në përputhje me kriteret e pikës 7.5 të ISO 17065, organizmi i certifikimit vlerëson të gjithë informacionin dhe rezultatet e vlerësimit. Procesi i vlerësimit siguron përputhshmëri midis objektit të certifikimit dhe objektit të vlerësimit, dhe që metodologjia e vlerësimit është zbatuar në mënyrë koherente përkundrejt gjetjeve të dokumentuara.

Neni 20

Informimi i klientit

1. Përveç kritereve të parashikuara në pikën 7.4.6 të ISO 17065, organizmi i certifikimit përcakton procedurat për informimin e klientit, në lidhje me rezultatet e vlerësimit, duke përfshirë mospërputhshmëritë dhe duke specifikuar llojin, formën dhe afatin kohor në përputhje me skemën e certifikimit.

2. Përveç kritereve të parashikuara në pikën 7.4.9 të ISO 17065, gjetjet e vlerësimit dokumentohen për çdo kriter vlerësimi në përputhje me skemën e certifikimit. Dokumentet e mbledhura gjatë vlerësimit evidentohen në mënyrë të qartë në mënyrë që të krijohet lidhja me kriterin përkatës të certifikimit dhe gjetjet përkatëse. Klienti ftohet të propozojë masa korrigjuese dhe parandaluese që i bashkëngjiten planit të veprimit dhe që verifikohen përpara marrjes së vendimit të certifikimit. Raporti i vlerësimit përmban:

a) një përshkrim të klientit;

b) planin e vlerësimit;

c) referenca për dokumentet e shqyrtuara;

ç) referencat në veprimet e përpunimit që janë vlerësuar;

d) funksionet e personave të intervistuar, vendndodhjen e gjetjeve, përshkrim të mospërputhshmërisë duke përfshirë shkallën dhe përmasën;

dh) organizmi i certifikimit përcakton, zbaton dhe mban një metodologji formale vlerësimi që specifikon qasjen, kriteret, afatet kohore dhe rregullat e vendimmarrjes që përcaktojnë përmbushjen e çdo kriteri të certifikimit. Metodologjia zbatohet në mënyrë koherente për klientin dhe dokumentohet në planin dhe raportet e vlerësimit.

Neni 21

Aksesi në raportet e vlerësimit

1. Raportet e vlerësimit dhe anekset përkatëse janë plotësisht të aksesueshme me kërkesë nga Komisioneri dhe ruhen për një periudhë kohore 6-vjeçare.

2. Komisioneri mund të marrë pjesë si vëzhgues gjatë kryerjes së procedurës së vlerësimit.

KREU V
VENDIMI PËR CERTIFIKIMIN, MONITORIMIN DHE RINOVIMIN E CERTIFIKIMIT

Neni 22
Vendimi për certifikimin

1. Përveç kritereve të parashikuara në pikën 7.6 të ISO 17065, organizmi i certifikimit përcakton dhe zbaton procedura që sigurojnë pavarësinë dhe llogaridhënien, në lidhje me vendimin për certifikim. Procedurat vendimmarrëse përfshijnë analizën e rrezikut dhe sigurojnë që vendimi të mbështetet në dokumente dhe prova.

2. Personi(at) apo ekipi përgjegjës për vendimin e certifikimit nuk duhet të kenë marrë pjesë në mënyrë të drejtpërdrejtë apo të tërthortë në aktivitetet vlerësuese ose këshilluese për të njëjtin klient dhe duhet të nënshkruajnë deklaratën e konfliktit të interesit. Kur është e nevojshme, me qëllim ruajtjen e pavarësisë, zbatohet rotacion i personelit.

3. Organizmi i certifikimit dokumenton dhe ruan të gjitha vendimet për certifikim, duke përfshirë arsyetimin, dokumentacionin provues dhe identifikimin e personave vendimmarrës, si dhe krijon mekanizëm të brendshëm për vlerësim dhe shqyrtim të ankesave.

Neni 23
Dokumenti që vërteton certifikimin

1. Përveç kritereve të parashikuara në pikën 7.7 të ISO 17065, organizmi i certifikimit i dorëzon klientit një dokument formal (certifikatë) nëpërmjet të cilës identifikohet:

a) emri i plotë dhe versioni i kritereve të certifikimit që janë përdorur për vlerësimin;

b) objekti i certifikimit, duke përfshirë një parashtrim (formulim) të qartë dhe të kuptueshëm të objektit të certifikimit, përshkrimin e llojit të të dhënave personale, veprimet përpunuese të përfshira dhe një listë me vendndodhjet ku kryhen këto veprime përpunimi;

c) klienti, përfshirë numrin unik të identifikimit të subjektit (NUIS).

2. Periudha e vlefshmërisë së certifikimit nuk mund të tejkalojë 3 vite. Monitorimi periodik i certifikimit kryhet dhe dokumentohet në përputhje me nenin 25 të këtij udhëzimi.

3. Në rast ndryshimesh ligjore ose rregullatore që ndikojnë në përputhshmërinë e klientit, organizmi i certifikimit siguron, brenda një afati të arsyeshëm, përditësimin e certifikatës dhe dokumenteve të tjera.

Neni 24
Detyrimi për publikimin e raportit të vlerësimit

1. Përveç kritereve të parashikuara në pikën 7.8 të ISO 17065, organizmi i certifikimit ruan informacionin e klientit të certifikuar, duke mundësuar akses nëpërmjet faqes zyrtare të internetit në një përmbledhje (ekstrakt) të këtij informacioni. Përmbledhja (ekstrakti) i raportit të vlerësimit përmban të dhënat e mëposhtme:

a) objektin e certifikimit, duke përfshirë një parashtrim të qartë dhe të kuptueshëm të objektit të certifikimit dhe çdo veprimi përpunimi të të dhënave personale që përfshihen në certifikim;

b) kriteret përkatëse të certifikimit, duke përfshirë versionin, statusin dhe referencat e zbatueshme tek standardet e njohura ose rregullat e tjera referuese;

c) metodat e vlerësimit dhe testet e kryera;

ç) rezultatet, duke përfshirë mospërputhshmërinë, kufizimet e vlerësimit dhe rreziqet e identifikuara të paadresuara.

2. Përmbledhja (ekstrakti) vlerësohet dhe përditësohet të paktën një herë në vit ose kur ka ndryshime thelbësore në objekt, kritere, metodologjinë e vlerësimit, rreziqet e paadresuara, duke siguruar që informacioni të mbetet i saktë, i plotë dhe i përditësuar.

Neni 25

Detyrimi për zbatimin e masave të monitorimit

1. Organizmi i certifikimit zbaton masa monitoruese gjatë të gjithë vlefshmërisë së certifikimit për të verifikuar përputhshmërinë e vazhdueshme me kriteret e certifikimit, duke siguruar që objekti, periodiciteti dhe intensiteti i monitorimit të jetë në proporcion me rreziqet e vlerësuara për subjektet e të dhënave dhe mundësinë e mospërputhjeve.

2. Veprimtaritë e monitorimit planifikohen dhe zhvillohen bazuar në vlerësimin e rrezikut, rreziqet që lidhen me klientin dhe veprimet e përpunimit të certifikuara. Përveç kritereve të parashikuara në pikën 7.9 të ISO 17065, monitorimi përfshin vlerësimin e aspekteve të mëposhtme:

a) ndryshimin e veprimeve të përpunimit të të dhënave që nga momenti i vlerësimit të fundit;

b) zbatimin e kritereve të vlerësimit që janë shtyrë më parë;

c) masat korrigjuese nga audite të mëparshme; dhe

ç) kriteret e përzgjedhura bazuar në rrezikun e evidentuar për mospërputhshmëri.

3. Procedura e monitorimit është transparente, efektive, e verifikueshme dhe nga pikëpamja operative, e zbatueshme dhe e përshtatshme për skemën e certifikimit. Procedurat e monitorimit janë të pavarura nga ndikime operative apo tregtare që mund të cenojnë paanshmërinë. Këto procedura përfshijnë:

a) përcaktimin e përgjegjësive, strukturës dhe burimeve të caktuara për monitorim;

b) aktivitete periodike monitorimi që mund të përfshijnë inspektim, audit ose vlerësime të ngjashme;

c) mekanizmin për të vlerësuar nëse kriteret për mbajtjen e certifikimit vijojnë të konsiderohen të plotësuara;

ç) vlerësime shtesë që vijnë nga ankesat, mospërputhshmëria që është evidentuar publikisht ose udhëzime nga Drejtoria e Përgjithshme e Akreditimit apo nga Komisioneri.

4. Organizmi i certifikimit, për efekt transparence, publikon regjistrin e përditësuar, lidhur me statusin e certifikimit (vlefshmërinë, pezullimin apo shfuqizimin).

5. Të gjitha aktivitetet e monitorimit, vlerësimit të rrezikut, masave korrigjuese dhe vendimet përkatëse dokumentohen për të siguruar gjurmueshmëri, llogaridhënie dhe transparencë në përputhje me ligjin nr. 124/2024, “Për mbrojtjen e të dhënave personale” dhe aktet nënligjore përkatëse.

Neni 26

Ndryshime që ndikojnë në certifikim

1. Përveç kritereve të parashikuara në pikën 7.10 të ISO 17065, organizmi i certifikimit konsideron si ndryshime që ndikojnë në certifikim:

a) çdo ndryshim në legjislacionin për mbrojtjen e të dhënave personale përkundrejt objektit të mekanizmit të certifikimit;

b) vendimet e Komisionerit, në lidhje me objektin e mekanizimit të certifikimit;

c) vendime të gjykatës që lidhen me mbrojtjen e të dhënave personale për çështje të paraqitura për shqyrtim në raport me objektin e certifikimit;

ç) zhvillime të reja teknologjike që përdoren për veprimet e përpunimit të të dhënave;

d) rreziqe të reja për mbrojtjen e të dhënave personale duke përfshirë identifikimin dhe vlerësimin e rreziqeve të reja ose që po evoluojnë nga inovacioni në teknologji, ndryshime në praktikat e përpunimit të të dhënave ose zhvillime të tjera që mund të ndikojnë në efektivitetin e procesit të certifikimit dhe zbatimin e masave teknike, dhe organizative për të zvogëluar këto rreziqe.

2. Ndryshimet mund të menaxhohen nëpërmjet procedurave të posaçme, duke përfshirë periudha tranzitore, rivlerësime të klientit, dhe nëse konsiderohet e përshtatshme edhe masa për shfuqizimin e certifikimit në rast se përpunimi nuk përmbush kriteret e përditësuara.

Neni 27

Përfundimi, pezullimi dhe shfuqizimi i certifikimit

1. Përveç kritereve të parashikuara në pikën 7.11 të ISO 17065, organizmi i certifikimit harton dhe zbaton procedura për të njoftuar menjëherë me shkrim klientin, Drejtorinë e Përgjithshme të Akreditimit dhe Komisionerin për çdo vendim certifikimi, që lidhet me vlefshmërinë, reduktimin e objektit, pezullimin ose shfuqizimin e tij, duke përfshirë vendimet që merren si pasojë e ankesave:

a) në rast përfundimi me kërkesë nga klienti, organizmi i certifikimit informon Drejtorinë e Përgjithshme të Akreditimit dhe Komisionerin, brenda 30 ditëve kalendarike nga dita e marrjes së kërkesës, për përfundimin e certifikimit;

b) në rast të vendosjes ose heqjes së pezullimit, shfuqizimit ose reduktimit të objektit, organizmi i certifikimit informon pa vonesë Drejtorinë e Përgjithshme të Akreditimit dhe Komisionerin.

2. Organizmi i certifikimit përcakton procedurat për trajtimin e mospërputhshmërisë së klientit sipas rregullave të përcaktuara në skemën e certifikimit, që përfshin të paktën aspektet e mëposhtme:

a) përcakton nëse masat korrigjuese të propozuara nga klienti janë të përshtatshme për të adresuar problemin, përpara se të merret vendimi mbi certifikimin. Për të gjithë mospërputhshmëritë, organizmi i certifikimit vlerëson nëse plani i veprimit është i përshtatshëm për të siguruar përputhshmëri me veprimet e përpunimit të të dhënave, përpara se të merret vendimi mbi certifikimin. Në rast se një plan veprimi nuk është i përshtatshëm për të siguruar përputhshmëri, organizmi i certifikimit pezullon vendimin për certifikim derisa të paraqiten prova për zbatimin e masave korrigjuese;

b) përcakton vonesat në zbatimin e masave korrigjuese (plan veprimi) nga 30 deri në 60 ditë duke pasur parasysh shkallën dhe natyrën e mospërputhshmërisë;

c) në rast se certifikimi është i kushtëzuar nga zbatimi i planit të veprimit, organizmi i certifikimit verifikon masat korrigjuese që janë zbatuar dhe ndërmerr veprimet e nevojshme në rast se mospërputhshmëria me kriteret nuk është adresuar sipas planit të veprimit.

3. Organizmi i certifikimit zbaton aktet me karakter detyrues të Drejtorisë së Përgjithshme të Akreditimit dhe Komisionerit, duke përfshirë revokimin, pezullimin dhe refuzimin e certifikimit në rast se konstatohet që kriteret nuk përmbushen.

4. Në rast se vendoset refuzim, pezullim ose shfuqizim i certifikimit, klienti informohet për të drejtën për t'u ankuar, lidhur me vendimin, mjetet në dispozicion, si dhe afatet përkatëse.

Neni 28

Dokumentimi

1. Përveç kritereve të parashikuara në pikën 7.12 të ISO 17065, organizmi i certifikimit mban dokumentacionin në mënyrë të plotë, të kuptueshme, të përditësuar dhe të verifikueshme.

2. Dokumentacioni duhet të përfshijë të paktën sa më poshtë:

a) dokumente që lidhen me certifikimin(et) që është/janë dhënë ose vendimet për refuzim;

b) dokumente që lidhen me procedurat në shqyrtim për certifikim.

3. Dokumentacioni është i aksesueshëm për një periudhë 6-vjeçare. Në rast mosmarrëveshjeje midis organizmit të certifikimit dhe klientit ose në rast ankese, afati i ruajtjes së dokumentacionit për efekt të zgjidhjes së mosmarrëveshjes, përcaktohet nga rregullat e zbatueshme të mosmarrëveshjes.

Neni 29
Ankimi

1. Organizmi i certifikimit garanton mekanizma ankimi për çdo subjekt të të dhënave ose organizatë aktive në mbrojtjen e të dhënave personale, të autorizuar nga një subjekt të dhënash, në lidhje me veprimtaritë e certifikimit, pa paragjykuar të drejtën e subjekteve të të dhënave për të paraqitur ankim pranë Komisionerit ose padi në gjykatë.

2. Përveç kritereve të parashikuara në pikën 7.13 të ISO 17065, organizmi i certifikimit zbaton një procedurë të dokumentuar që përfshin marrjen, shqyrtimin dhe vendimmarrjen mbi ankimin, në lidhje me procesin e certifikimit, duke pasur parasysh rregullat e parashikuara në skemën e certifikimit. Procedura është e aksesueshme për publikun dhe për të gjitha subjektet e të dhënave, si dhe organet kompetente brenda objektit të certifikimit.

3. Procedura e trajtimit të ankimit siguron pjesëmarrje, paanësi dhe të drejtën për t'u dëgjuar. Ankuesi informohet mbi ecurinë dhe vendimmarrjen brenda një afati të arsyeshëm, por jo më vonë se 3 muaj nga data e paraqitjes së ankesës. Vlerësimi paraprak mbi ankesën dërgohet brenda një muaji nga data e paraqitjes së ankimit që parashtron përgjigjen paraprake dhe hapat që do të ndiqen në 2 (dy) muajt e ardhshëm. Në rast se nuk mund arrihet në një vendimmarrje formale brenda afatit 3-(tre-)-mujor, organizmi i certifikimit informon ankuesin mbi përfundimin e procesit dhe arsyet pse nuk ka qenë e mundur arritja e një përfundimi brenda këtij afati.

4. Procedura e ankimit duhet të paktën të përfshijë sa më poshtë vijon:

a) subjektet që legjitimohen të paraqesin ankim;

b) subjektin përgjegjës për të mbledhur dhe verifikuar informacionin e nevojshëm për ecurinë e ankimit deri në vendimmarrje;

c) subjektin përgjegjës për vendimmarrjen dhe zgjidhjen e ankimit;

ç) fazat e ndryshme për informimin e ankuesit, në lidhje me ecurinë, rezultatin dhe përmbylljen e ankimit, duke përfshirë afatet kohore përkatëse;

d) mënyrën se si kryhet verifikimi;

dh) procedurën që mund të ndërmerret për të zgjidhur ankimin, duke përfshirë konsultimet me aktorët e përfshirë;

e) palëve që iu dërgohet konfirmimi i njoftimit, brenda 1 (një) muaji nga marrja, që mund të zgjatet nëse është e nevojshme dhe në mënyrë të arsyetuar edhe 1 (një) muaj;

ë) afatet kohore për të cilat pala duhet të jetë në dijeni;

f) procedurat e tjera në rast se çështja (ankimi) mbetet e/i pazgjidhur apo papërfunduar.

5. Organizmi i certifikimit siguron që trajtimi i ankesës të jetë i ndryshëm nga ai i vlerësimit, shqyrtimit dhe vendimmarrjes mbi certifikimin, me qëllim mënjanimin e konfliktit të interesit.

6. Organizmi i certifikimit krijon dhe përditëson regjistrin e ankesave që duhet të përfshijë:

a) ecurinë e çdo ankese (depozituar, në hetim ose përfunduar);

b) datat e veprimeve të ndërmarra (regjistrim ankimi, marrje dijeni, përditësim mbi ecurinë, vendimmarrjen etj.).

7. Regjistri është i aksesueshëm për inspektime nga Drejtoria e Përgjithshme e Akreditimit, si dhe Komisioneri.

KREU VI
KRITERET PËR SISTEMIN E MENAXHIMIT

Neni 30
Kriteret e përgjithshme të sistemit të menaxhimit

1. Përveç kritereve të parashikuara në pikën 8 të ISO 17065, organizmi i certifikimit zhvillon dhe mirëmban një sistem menaxhimi që përmbush kriteret e përcaktuara në këtë udhëzim për të gjithë veprimtaritë e certifikimit dhe brenda objektit të akreditimit. Sistemi përfshin dokumentimin, vlerësimin dhe monitorimin e pavarur të kritereve shtesë për të siguruar përputhshmëri, transparencë dhe gjurmueshmëri.

2. Sistemi i menaxhimit bazohet në një metodologji për zbatimin dhe kontrollin e kritereve, në përputhje me ligjin nr. 124/2024, "Për mbrojtjen e të dhënave personale" dhe këtë udhëzim, duke përfshirë monitorimin e vazhdueshëm për të siguruar përputhshmëri. Sistemi harmonizohet me parimet e përgjithshme të menaxhimit të ISO 17065, dokumentimin dhe kontrollin, raportet e auditeve të brendshme, vlerësimet e organeve drejtuese, si dhe masat korrigjuese dhe parandaluese.

3. Veçanërisht, sistemi i menaxhimit siguron:

a) informacion mbi certifikimin, duke përfshirë mekanizmin e certifikimit ose skemën e zbatuar, periudhën e vlefshmërisë, si dhe kushtet përkatëse që janë të aksesueshme për publikun në mënyrë të përhershme dhe të vazhdueshme. Informacioni përditësohet rregullisht, në lidhje me ndryshime të skemës së certifikimit ose vendimmarrje të tjera përkatëse;

b) përmbushjen e kritereve të neneve 11 dhe 24 të këtij udhëzimi;

c) se zbatimi i parimeve të menaxhimit është transparent dhe vërtetohet gjatë procesit të akreditimit ose me kërkesë të Drejtorisë së Përgjithshme të Akreditimit ose Komisionerit;

ç) se sistemi i menaxhimit është në përputhje me këto kritere:

i. pikën 8.2 të ISO 17065, në lidhje me dokumentimin e sistemit të menaxhimit, duke përfshirë procesin e hartimit, përditësimin dhe ruajtjen e dokumenteve sipas ndryshimeve ligjore dhe standardeve. Dokumentacioni është i aksesueshëm për të gjitha palët e interesuara, për sa kohë ruhet konfidencialiteti dhe integriteti i të dhënave;

ii. pikën 8.3 dhe 8.4 të ISO 17065, lidhur me kontrollin e dokumenteve për të siguruar që i gjithë dokumentacioni të jetë i arkivuar në përputhje me elementet e sigurisë dhe i përditësuar. Ndryshimet në dokumentacion monitorohen dhe auditohen për të siguruar saktësi dhe përputhshmëri të të dhënave;

iii. pikën 8.5 të ISO 17065, në lidhje me vlerësimin e nivelit drejtues, duke përfshirë analizën e rezultateve të auditit të brendshëm dhe vlerësimit të jashtëm. Vlerësimi kryhet rregullisht dhe është pjesë e procesit të përmirësimit të vazhdueshëm të sistemit të menaxhimit;

iv. pikën 8.6 të ISO 17065, në lidhje me auditin e brendshëm. Auditi kryhet në mënyrë të dokumentuar dhe përfshin të gjitha aspektet e sistemit të menaxhimit, duke përfshirë cilësinë, përputhshmërinë rregullatore dhe sigurinë e të dhënave. Auditorët janë të pavarur nga departamentet që auditojnë dhe kanë kryer trajnimet përkatëse. Rezultatet e auditit dokumentohen dhe përfshijnë rekomandime specifike për përmirësim dhe plan veprimi të detajuar për zbatimin e tyre;

v. pikën 8.7 të ISO 17065, në lidhje me masat korrigjuese të ndërmarra për të adresuar mospërputhshmëritë e evidentuara. Masat korrigjuese përfshijnë një analizë dhe janë objekt i vlerësimit nga auditi i brendshëm. Ato monitorohen dhe zbatohen brenda një periudhe kohore të caktuar. Organizmi i certifikimit raporton mbi progresin e zbatimit të këtyre masave dhe siguron që efektet të jenë matshme dhe vlerësueshme;

vi. pikën 8.8. të ISO 17065, në lidhje me masat parandaluese për të identifikuar dhe ulur rrezikun që mund të shkaktojë mospërputhshmëri në të ardhmen. Veprimet ndërmerren bazuar

në analizë rreziku dhe përfshijnë masa që ulin mundësinë që rreziku të materializohet. Masat parandaluese dokumentohen dhe rishikohen në mënyrë periodike për të siguruar që ato efektivisht parandalojnë mospërputhshmëritë.

Neni 31
Procedurat e përditësimit të metodave të vlerësimit

1. Organizmi i certifikimit harton procedura për përditësimin e metodologjisë së vlerësimit që zbatohen kur ka ndryshime në kuadrin ligjor, situatën tërësore dhe në zbatimin e kostove të masave teknike, dhe organizative dhe rreziqe domethënëse. Përditësimi përfshin analizë të rrezikut dhe vlerësim mbi ndikimin e këtyre ndryshimeve në procesin e vlerësimit dhe efektivitetit të tij.

2. Organizmi i certifikimit harton procedura për të siguruar trajnim të personelit për të përditësuar kapacitetet/aftësitë, duke pasur parasysh ndryshimet e përmendura në pikën 1 të këtij neni.

3. Organizmi i certifikimit harton procedura në rast reduktimi, pezullimi ose shfuqizimi të akreditimit, duke përfshirë kriteret për këto raste dhe njoftimin e klientit. Njoftimi i klientëve kryhet brenda një afati prej 30 (tridhjetë) ditësh dhe klienti ka mundësinë e ankimit brenda 30 (tridhjetë) ditëve nga data e njoftimit.

KREU VII
MONITORIMI NGA KOMISIONERI

Neni 32
Monitorimi dhe mbikëqyrja e organizmave të certifikimit nga Komisioneri

1. Komisioneri monitoron dhe mbikëqyr nëse organizmat e certifikimit përmbushin kriteret e parashikuara në ligjin nr. 124/2024, "Për mbrojtjen e të dhënave personale" dhe këtë udhëzim, pavarësisht dhe pa cenuar kompetencat mbikëqyrëse që ushtron Drejtoria e Përgjithshme e Akreditimit, sipas parashikimeve të ligjit nr. 116/2014, "Për akreditimin e organeve të vlerësimit të konformitetit në Republikën e Shqipërisë".

2. Komisioneri, në kuadër të monitorimit dhe mbikëqyrjes, mund të kërkojë nga organizmi i certifikimit:

a) dokumente ose akte të ndryshme, duke përfshirë procedurat e brendshme që zbatohen prej tij në funksion të përmbushjes së kritereve ligjore dhe atyre shtesë sipas këtij udhëzimi;

b) dokumentacionin ose informacionin e nevojshëm për të verifikuar përputhshmërinë me ligjin nr. 124/2024, "Për mbrojtjen e të dhënave personale", duke vendosur afate për paraqitjen/depozitimin e tyre;

c) kryerjen e inspektimeve në terren, auditeve, si dhe vlerësimeve teknike të tjera të ngjashme. Për këtë qëllim, Komisioneri njofton organizmin e certifikimit të paktën 7 ditë përpara inspektimit, auditit ose vlerësimit.

3. Organizmi i certifikimit bashkëpunon me Komisionerin dhe vendos në dispozicion, në mënyrë të plotë dhe brenda afatit të caktuar, çdo informacion/dokument të kërkuar, si dhe kryen çdo veprim tjetër të nevojshëm për të lehtësuar monitorimin dhe mbikëqyrjen.

4. Komisioneri, me qëllim lehtësimin e monitorimit, vlerësimit të përputhshmërisë dhe të rrezikut që lidhet me certifikimin, kërkon nga organizmi i certifikimit raportim me shkrim mbi certifikimin e lëshuar sipas nenit 37, të ligjit nr. 124/2024, "Për mbrojtjen e të dhënave personale", duke përfshirë objektin e certifikimit, numrin e tyre dhe periudhën e vlefshmërisë.

5. Në kuadër të bashkëpunimit institucional, Komisioneri mund të kërkojë nga Drejtoria e Përgjithshme e Akreditimit kopje të raportit të mbikëqyrjes mbi vlerësimin e konformitetit të hartuar në kuadër të zbatimit të ligjit nr. 116/2014, "Për akreditimin e organeve të vlerësimit të konformitetit në Republikën e Shqipërisë", si dhe çdo informacion tjetër mbi organizmat e certifikimit të akredituar sipas këtij udhëzimi, objektin dhe statusin përkatës të akreditimit (vlefshmërinë, pezullimin ose shfuqizimin) ose të dhëna të tjera të nevojshme për zbatimin efektiv të kompetencave monitoruese dhe mbikëqyrëse sipas ligjit nr. 124/2024, "Për mbrojtjen e të dhënave personale".

Neni 33
Sanksionet

1. Në rast se Komisioneri konstaton mospërputhshmëri në ushtrimin e veprimtarisë nga organizmi i certifikimit në raport me ligjin nr. 124/2024, "Për mbrojtjen e të dhënave personale", ushtron sipas rastit kompetencat hetimore, korrigjuese ose sanksionuese të parashikuara në ligjin nr. 124/2024, "Për mbrojtjen e të dhënave personale".
2. Komisioneri, mund t'i propozojë Drejtorisë së Përgjithshme të Akreditimit, shfuqizimin e akreditimit të organizmit të certifikimit, nëse konstaton se nuk janë plotësuar ose nuk plotësohen më kushtet dhe kriteret për akreditim ose nëse veprimet e organizmit të certifikimit shkelin ligjin nr. 124/2024, "Për mbrojtjen e të dhënave personale".

Neni 34
Dispozita kalimtare dhe të fundit

1. Organizmat e certifikimit që janë akredituar përpara hyrjes në fuqi të këtij udhëzimi, sipas udhëzimit të Komisionerit nr. 48, datë 14.9.2018, "Për certifikimin e sistemeve të menaxhimit të sigurisë së informacionit, të dhënave personale dhe mbrojtjes së tyre", vazhdojnë të kryejnë veprimtarinë certifikuese deri në përfundim të afatit të akreditimit.
2. Udhëzimi nr. 47, datë 14.9.2018, "Për përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga subjektet përpunuese të mëdha" dhe udhëzimi nr. 48, datë 14.9.2018, "Për certifikimin e sistemeve të menaxhimit të sigurisë së informacionit, të dhënave personale dhe mbrojtjes së tyre", shfuqizohen.

Ky udhëzim hyn në fuqi pas botimit në Fletoren Zyrtare.

KOMISIONERI PËR TË DREJTËN E INFORMIMIT
DHE MBROJTJEN E TË DHËNAVE PERSONALE
Besnik Dervishi