R E P U B L I K A E S H Q I P Ë R I S Ë
KOMISIONERI PËR TË DREJTËN E INFORMIMIT DHE MBROJTJEN E TË DHËNAVE PERSONALE

UDHËZIM

Nr. 09, 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 mbështetje të pikës 1, të nenit 37, 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. Ky Udhëzim parashikon kriteret e përgjithshme për certifikimin dhe dhënien e vulave dhe të shenjave të mbrojtjes së të dhënave personale.
2. Procesi i përpunimit të të dhënave personale kontrollohet dhe certifikohet nga organizmi i certifikimit vetëm nëse përmbush të gjitha parashikimet e mekanizmit të certifikimit të parashikuara në këtë udhëzim. Marrja e certifikimit në përputhje me parashikimet e nenit 37 të Ligjit dhe të këtij udhëzimi, konfirmon që procesi i përpunimit të të Dhënave personale kryhet në përputhje me mekanizmin e certifikimit të miratuar nga Komisioneri.

Neni 2
Përkufizime

1. Termat e përdorur në këtë udhëzim kanë të njëjtin kuptim si ato të parashikuara në Ligj, si dhe ISO 27701 (Siguria e të dhënave, siguria kibernetike dhe mbrojtja e të Dhënave personale — *Sistemet e Menaxhimit të të Dhënave Personale— Kritere dhe Udhëzime*).

Termat e tjerë të përdorur në këtë udhëzim kanë këto kuptime:

a) "Certifikim" është procesi i zhvilluar nga organizmi i certifikimit në përputhje me parashikimet e nenit 37 të Ligjit si dhe të këtij udhëzimi, me qëllim vlerësimin e konformitetit, në përfundim të të cilit klienti pajiset me vulën dhe shenjat për mbrojtjen e të dhënave personale, si dhe të gjitha aspektet e tjera që përfshijnë garantimin e përputhshmërisë dhe vlefshmërisë së certifikimit.

b) *"*Vula dhe shenja*"* është simboli që do të përdoret nga organizmi i certifikimit për të treguar që një veprim përpunimi ose veprimet e përpunimit janë vlerësuar dhe janë gjetur në konformitet me kërkesat specifike ligjore për mbrojtjen e të dhënave personale.

c) "Organizëm certifikimi" është personi juridik i akredituar nga Drejtoria e Përgjithshme e Akreditimit në përputhje me Ligjin nr. 116/2014, "Për akreditimin e organeve të vlerësimit të konformitetit në Republikën e Shqipërisë", Ligjin nr.124/2024 "Për mbrojtjen e të dhënave personale, si dhe Udhëzimin e Komisionerit nr. 8, datë 20.11.2025 "Për kriteret shtesë për akreditimin e organizmit certifikues".

ç) "Klient" është çdo person fizik apo juridik, publik ose privat, që bazuar në fushën e veprimtarisë ose në ushtrimin e kompetencave sipas ligjit, është kontrollues ose përpunues i të dhënave personale dhe për rrjedhojë i nënshtrohet vlerësimit të konformitetit dhe certifikimit me vula dhe shenja sipas parashikimeve të Ligjit dhe këtij udhëzimi.

d) "Audit" është procesi i kontrollit sistematik, i pavarur dhe i dokumentuar, nëpërmjet të cilit përftohen të dhëna audituese dhe vlerësuese që përcaktojnë në mënyrë objektive masën në të cilën janë përmbushur kritetet ligjore.

(dh) "Komisioneri" është Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale.

(e) "Ligji" është Ligji nr. 124/2024 "Për mbrojtjen e të dhënave personale"

KREU II
MARRËDHËNIET MIDIS KLIENTIT DHE ORGANIZMIT TË CERTIFIKIMIT

Neni 3
Kërkesa për certifikim

1. Klienti paraqet pranë organizmit të certifikimit kërkesën me shkrim për certifikim të një ose disa veprim(eve) të përpunimit të të dhënave personale.
2. Klienti vendos në dispozicion të organizmit të certifikimit të gjithë dokumentacionin dhe informacionin e nevojshëm për kryerjen e procedurës së certifikimit si dhe mundëson akses në veprimtaritë e përpunimit.

Neni 4
Përdorimi i vulës dhe shenjave të mbrojtes së të dhënave

1. Vulat dhe shenjat e mbrojtjes së të dhënave mund të përdoren vetëm nga ata kontrollues ose përpunues që kanë marrë certifikimin e duhur për proceset e përpunimit në përputhje me parashikimet e këtij udhëzimi.
2. Klienti, që është certifikuar në përputhje me parashikimet e këtij udhëzimi, publikon në faqen zyrtare, në një vend të dukshëm, rezultatin e certifikimit, duke specifikuar veprimin apo veprimet e përpunimit përkatës.

Neni 5
Publikimi i listës së subjekteve të certifikuara dhe raportimi pranë Komisionerit

1. Organizmi i certifikimit publikon në faqen zyrtare të internetit, në një hapësirë të dedikuar, listën e të gjithë klientëve që ka kryer certifikim sipas këtij udhëzimi.
2. Brenda 31 Dhjetorit të çdo viti kalendarik, organizmi i certifikimit dërgon informacion me shkrim pranë Komisionerit mbi klientët e certifikuar, duke specifikuar veprimin apo veprimet e përpunimit që janë certifikuar si dhe problematikat e ndeshura në procesin e certifikimit.
3. Në rast se organizmi i certifikimit pezullon ose shfuqizon certifikimin në përputhje me parashikimet e neneve 16 dhe 17 të këtij udhëzimi, ai përditëson listën e të gjithë subjekteve që ka kryer certifikim, të publikuar në faqen zyrtare të internetit.

Neni 6
Afati i certifikimit

Certifikimi që i lëshohet kontrolluesit ose përpunuesit është i vlefshëm për një periudhë jo më të gjatë se 3 (tre) vjet dhe mund të rinovohet sipas të njëjtave kritere të përcaktuara në këtë udhëzim.

KREU III
KRITERET LIGJORE PËR CERTIFIKIMIN DHE DHËNIEN E VULAVE DHE SHENJAVE

Neni 7
Kriteret e vlerësimit

1. Klienti që plotëson kriteret e mëposhtme, certifikohet sipas parashikimeve të këtij udhëzimi:
   a) rezulton se ka Sistem të Menaxhimit të Sigurisë së Informacionit (SMSI) (ISO/IEC 27001), që është funksional dhe ushtron kontrolle specifike lidhur me të dhënat

personale;

b) rezulton se vepron bazuar në parimet e parashikuara në nenin 9 të këtij udhëzimi;
c) rezulton se zbaton ndarje të roleve dhe përgjegjësive të kontrolluesit, përpunuesit dhe nën-përpunuesve për të identifikuar, menaxhuar dhe raportuar cenime ose shkelje në të dhënat personale;
ç) rezulton se ekzistojnë procese të brendshme që tregojnë organizim në mënyrë të atillë që të mundësojnë ushtrimin e të drejtave të subjekteve të të dhënave;
d) rezulton se ekzistojnë masa të sigurisë/mbrojtëse në rast se subjekti kryen transferim të të dhënave në shtete të treta ose organizata ndërkombëtare;
e) rezulton se ekzistojnë masa teknike dhe organizative që garantojnë nivel sigurie të përshtatshëm për rrezikun.

Neni 8
Sistemi i menaxhimit të të dhënave personale

1. Klienti ka detyrimin të krijojë, zbatojë, mirëmbajë dhe përmirësojë në mënyrë të vazhdueshme një Sistem Menaxhimi të të Dhënave Personale (*Privacy Information Management System "PIMS"*) në përputhje me parashikimet e ISO/IEC 27701.
2. Klienti përcakton dhe gjurmon Treguesit Kyç të Përformancës (*Key Performance Indicators "KPI"*) për të matur eficiencën e PIMS, kryen vlerësime nga niveli drejtues, të paktën një herë në vit, siguron përmirësim të vazhdueshëm, si dhe planifikon dhe kryen audit të brendshëm, të paktën një herë në vit për të vlerësuar përputhshmërinë dhe efektivitetin e PIMS.

Neni 9
Parimet mbi të cilat vepron klienti

1. Vlerësimi që kryen organizmi i certifikimit duhet të sigurojë që i gjithë përpunimi i të dhënave personale kryhet në mënyrë të ligjshme, të drejtë dhe transparente. Baza ligjore për çdo veprim përpunues duhet të identifikohet, dokumentohet/evidentohet dhe është objekt rishikimi në intervale kohore të përcaktuara ose kur ndryshon veprimi(et) e përpunimit, me qëllim sigurimin e përputhshmërisë së vazhdueshme dhe ekzistencës së nevojës.
2. Regjistrat (dosjet) e veprimit (eve) të përpunimit duhet të evidentojnë në mënyrë të qartë qëllimin e përpunimit dhe bazën ligjore ku është mbështetur ky përpunim.
3. Klienti duhet të respektojë parimet e mëposhtme:
   a) parimin e ligjshmërisë, drejtësisë dhe transparencës;
   b) parimin e përpunimit në përputhje me qëllimin;
   c) parimin e minimizimit të të dhënave;
   ç) parimin e saktësisë së të dhënave;
   d) parimin e kufizimit të ruajtjes në kohë;

e) parimin e integritetit dhe konfidencialitetit;
ë) parimin e përgjegjshmërisë.

4. Klienti kryen kontrolle të vazhdueshme për të monitoruar dhe verifikuar përputhshmërinë me këto parime. Klienti ka detyrimin të ruajë të dhëna që demonstrojnë përputhshmëri, duke përfshirë raportet e auditit, dosjet e verifikimit apo dokumente të tjera të ngjashme.

Neni 10
Ndarja e roleve dhe përgjegjësive të klientit

1. Roli dhe përgjegjësitë e kontrolluesit, përpunuesit dhe nënpërpunuesve përcaktohen dhe dokumentohen në mënyrë të qartë.
2. Marrëveshja(et) për përpunimin e të dhënave personale përmbajnë dispozita mbi përgjegjësitë, rregullat që zbatohen midis palëve si dhe përgjegjshërinë. Vlerësimi përfshin kontrollin e hollësishëm (*due diligence*) dhe zbatimin e parashikimeve kontraktuale për nënpërpunuesit, si dhe ruajtjen e të dhënave (evidencave) për marrjen e masave që demonstrojnë përmbushjen e parimit të përgjegjshmërisë.
3. Vlerësimi përfshin verifikimin nëse ekzistojnë procedura të dokumentuara për të identifikuar, menaxhuar dhe njoftuar cenimet ose shkeljet në të dhënat personale. Procedurat që i përgjigjen situatave të cenimit ose shkeljes së të dhënave personale testohen në mënyrë periodike nëpërmjet simulimit për të siguruar efektivitetin e tyre.
4. Klienti kryen njoftimet për cenimin ose shkeljen e dhënave personale pranë Komisionerit si dhe subjekteve të prekura në përputhje me nenin 29 të Ligjit nr.124/2024 “Për mbrojtjen e të dhënave personale”. Njoftimi përmban informacion të plotë dhe të kuptueshëm në lidhje me natyrën dhe masën e cenimit ose shkeljes, si dhe masat e ndërmarra për zbutjen e pasojave brenda kohës së kufizuar në dispozicion.
5. Klienti zbaton mbrojtjen e të dhënave në projektim (*privacy by design*) dhe në mënyrë të paracaktuar (*default*) si pjesë e sistemeve të integruara, shërbimeve dhe proceseve të tij. Masat teknike dhe organizative zbatohen me qëllim sigurimin që nëpërmjet mbrojtjes së të dhënave në mënyrë të paracaktuar (*default*), të përpunohen vetëm ato të dhëna personale që janë të nevojshme për qëllimin përkatës.
6. Klienti kryen vlerësime që përfshijnë konstatimin dhe dokumentimin e gjetjeve nga cenimi ose shkelja e të dhënave personale, me qëllim identifikimin e mundësive për përmirësim të vazhdueshëm. Mekanizimi përfshin një vlerësim të rregullt të politikave dhe proceseve të adresimit të cenimit ose shkeljes me qëllim sigurimin që çdo incident të shërbejë si mundësi për të forcuar mekanizmat parandalues dhe masat reaguese. Procesi mbështetet nga angazhimi i nivelit drejtues të klientit për përmirësim të vazhueshëm për masat e sigurisë dhe dokumentohet për të evidentuar zbatimin me efektivitet të tyre.

Neni 11
Ushtrimi i të drejtave nga ana e subjekteve të të dhënave

1. Klienti organizon proceset në mënyrë të atillë që të mundësojnë ushtrimin e të drejtave të subjekteve të të dhënave duke përfshirë:
   a) të drejtën për informim;
   b) të drejtën për akses;
   c) të drejtën për korrigjim dhe fshirje;
   ç) të drejtën për t'u harruar;
   d) të drejtën për kufizimin e përpunimit;
   e) të drejtën për transferueshmërinë e të dhënave;
   ë) të drejtën për të kundërshtuar;
   f) të drejtën për të mos iu nënshtruar vendimeve automatike.
2. Subjektet e të dhënave gëzojnë të drejtën për përgjigje brenda afateve të parashikuara në Ligj.
3. Klienti dokumenton dhe ruan të gjithë korrespondencën me subjektet e të dhënave. Sistemi i trajtimit të kërkesës përfshin verifikimin e identitetit të kërkuesit, regjistrimin e kërkesës, gjurmimin e ecurisë së trajtimit dhe rishikohet në mënyrë periodike për të verifikuar përmbushjen e detyrimeve ligjore brenda afatit.

Neni 12
Vlerësimi i rrezikut dhe vlerësimi i ndikimit në mbrojtjen e të dhënave

1. Klienti kryen vlerësim të rregullt të rreziqeve që lidhen me veprimet e përpunimit të të dhënave personale.
2. Vlerësimi merr në konsideratë mundësinë, shkallën dhe ndikimin e mundshëm në të drejtat dhe liritë e subjekteve të të dhënave.
3. Vlerësimi i ndikimit në mbrojtjen e të dhënave kryhet për veprimet e përpunimit që mund të shkaktojnë një rrezik të lartë të të drejtave dhe lirive themelore të individëve në përputhje me nenin 31 të Ligjit dhe rezultatet dokumentohen, vlerësohen dhe integrohen në proceset e menaxhimit të rrezikut. Vlerësimi i ndikimit në mbrojtjen e të dhënave përditësohet në rast se rreziku mund të ketë ndryshuar si rezultat i faktorëve të jashtëm, si ndryshime në legjislacion, teknologji apo politika organizative. Ky proces kryhet në mënyrë të vazhdueshme me qëllim sigurimin e përputhshmërisë dhe mbrojtjes së të dhënave personale.
4. Rezultatet e vlerësimit të ndikimit në mbrojtjen e të dhënave dhe vendimet për trajtimin e rrezikut, miratohen nga struktura drejtuese përkatëse sipas legjislacionit në fuqi dhe akteve të brendshme të klientit dhe efektiviteti i tyre i nënshtrohet monitorimit të vazhdueshëm. Rivlerësimet e bazuara në ngjarje të caktuara kryhen sa herë që veprimet e përpunimit ndryshojnë apo ka përditësime regullative.

Neni 13
Masat teknike dhe organizative

1. Klienti zbaton masat e nevojshme teknike dhe organizative që garantojnë nivel sigurie të përshtatshëm për rrezikun dhe përfshijnë:
   a) pseudonimizimin dhe enkriptimin;
   b) kontrollin e aksesit dhe menaxhimin e identitetit;
   c) aftësitë e qëndrueshmërisë dhe për të rivendosur disponueshmërinë;
   ç) testime të vazhdueshme dhe vlerësim të masave të sigurisë, duke përfshirë simulime të sulmeve dhe audite sigurie që janë të nevojshme për të garantuar përputhshmërinë me standardet ndërkombëtare dhe identifikuar vulnerabilitetet që mund të përbëjnë rrezik për të dhënat.
   d) testime të rregullta për depërtime dhe vlerësime vulnerabiliteti duke përfshirë edhe masat korrigjuese.
2. Masat e përmenduara në pikën 1 të këtij neni, rishikohen në mënyrë periodike për të siguruar efektivitet të vazhdueshëm. Klienti ndërmerr veprime të dokumentuara me karakter parandalues që përfshijnë monitorimin e vazhdueshëm dhe evidentimin e parregullsive.
3. Klienti ndërmerr masa të vazhdueshme për të rritur sigurinë e sistemeve, duke përfshirë analizimin e rezultateve të auditimit të sigurisë dhe testimeve, si dhe identifikimin e mundësive për përmirësim. Procesi përfshin bashkëpunimin me ekspertë të jashtëm dhe të brendshëm, përdorimin e raporteve të detajuara për dobësitë e sistemit dhe sugjerime për përmirësim. Pjesë e procesit konsiderohet edhe vlerësimi dhe përditësimi i politikave të sigurisë për të ruajtur një nivel të lartë mbrojtje kundër rreziqeve të reja.

Neni 14
Transferimi ndërkombëtar i të dhënave

1. Transferimi i të dhënave drejt vendeve të treta ose organizatave ndërkombëtare, kryhet vetëm në rast se ekzistojnë masa mbrojtëse sipas parashikimeve në Kreun IV të Ligjit.
2. Vlerësimi përfshin dokumentimin dhe ruajtjen e provave të mekanizmit të transferimit, të tilla si, vendimi i përshtatshmërisë, klauzolat standarde të mbrojtjes së të dhënave apo rregullat e detyrueshme të grupit të shoqërive tregtare. Përshtatshmëria e transferimit rishikohet në mënyrë periodike dhe lidhet me qëllimin specifik të përpunimit dhe bazën ligjore.
3. Vlerësimi evidenton qëllimin e transferimit të të dhënave dhe bazën ligjore përkatëse për këtë transferim. Informacioni pasqyrohet në mënyrë të qartë dhe të aksesueshme për inspektime të jashtme dhe auditin, si dhe për të siguruar transparencë dhe përputhshmëri në mbrojtjen e të dhënave.

Neni 15
Administrimi i brendshëm i klientit

1. Struktura drejtuese e klientit që i nënshtrohet vlerësimit duhet të tregojë aftësi në drejtim dhe angazhim në lidhje me Sistemin e Menaxhimit të të Dhënave Personale (*Privacy Information Management System "PIMS"*) duke:
   a) hartuar politika sigurie të harmonizuara me ISO/IEC 27701 dhe të përfshira në strategjitë e drejtimit të brendshëm dhe ato organizative;
   b) përcaktuar role dhe përgjegjësi të qarta për mbrojtjen e të dhënave, duke përfshirë caktimin e një nëpunësi për mbrojtjen e të dhënave, kur është e nevojshme;
   c) integruar objektivat e mbrojtjes së të dhënave në të gjithë strategjitë organizative të veprimtarisë tregtare dhe kuadrit SMSI, duke përfshirë indikatorë kyç të përformancës që i reflektojnë ato.
2. Klienti harton, dokumenton dhe mirëmban politika dhe procedura specifike për mbrojtjen e të dhënave personale.
3. Politikat përfshijnë përpunimin e të dhënave personale, ruajtjen, miratimin e organit(eve) drejtues(e) dhe transferimin ndërkombëtar dhe rishikohen e përditësohen në intervale kohore të përcaktuara. Verifikimet periodike nga niveli drejtues sigurojnë që politikat të zbatohen në mënyrë të vazhdueshme.
4. Klienti kryen trajnime për mbrojtjen e të dhënave dhe programe ndërgjegjësimi. Trajnimi organizohet bazuar në rolet dhe përgjegjësitë përkatëse, ka karakter të vazhdueshëm dhe dokumentohet si aftësim në menaxhimin e përgjegjësive që lidhen me të dhënat personale. Treguesit e efektivitetit janë të gjurmueshëm dhe përfshijnë përqindjet e stafit që ka kryer trajnimin, vlerësimin përkatës etj.
5. Klienti ruan informacion të dokumentuar mbi përpunimin e të dhënave personale në përputhje me parashikimet e nenit 27 të Ligjit. Dokumentimi përfshin kategoritë e të dhënave, qëllimin, bazën ligjore, periudhën e ruajtjes si dhe mekanizmat e transferimit.
6. Klienti zbaton procese të strukturuara për vlerësimin e rrezikut të mbrojtjes së të dhënave personale. Vlerësimi i ndikimit në mbrojtjen e të dhënave kryhet për veprime përpunimi që shkaktojnë rrezik të lartë, në përputhje me ISO/IEC 27701, pika 7.2.5, dhe neni 31 i Ligjit. Rezultatet e adresimit të rrezikut integrohen në Sistemin e Menaxhimit të të Dhënave Personale (*Privacy Information Management System "PIMS"*) dhe janë objekt i vlerësimit nga organi(et) drejtues(e).
7. Klienti planifikon dhe kryen audit të brendshëm të Sistemit të Menaxhimit të të Dhënave Personale (*Privacy Information Management System "PIMS"*) në përputhje me ISO/IEC 27701, pika 5.7.2, për të verifikuar përputhshmërinë me kushtet e mbrojtjes së të dhënave. Në rast se konstatohet mungesë përputhshmërie, klienti ndërmerr masa korrigjuese.
8. Klienti evidenton përmirësimin e vazhdueshëm të Sistemit të Menaxhimit të të Dhënave Personale (*Privacy Information Management System "PIMS"*) dhe siguron që ai të jetë efektiv, i përditësuar dhe në nivel të tillë që t'i përgjigjet ndryshimeve në veprimet e përpunimit apo kuadrit ligjor.

Neni 16
Pezullimi i certifikimit

1. Organizmi i certifikimit mund të pezullojë certifikimin e dhënë në përputhje me këtë udhëzim për një periudhë të caktuar kohe në rast se:
   a) monitorimi periodik ose rivlerësimi evidenton mospërputhje që nuk janë korrigjuar brenda afatit të përcaktuar;
   b) klienti nuk i vendos në dispozicion organizmit të certifikimit informacionin, dokumentacionin ose qasjen e kërkuar në kuadër të veprimtarisë së monitorimit;
   c) ndodhin ndryshime të rëndësishme në veprimet e përpunimit, në strukturën organizative ose në sistemin e menaxhimit që mund të ndikojnë në përputhshmëri dhe që nuk i janë njoftuar organizmit të certifikimit;
   ç) ka hetime të përfunduara nga Komisioneri ose autoritete të tjera kompetente që mund të ndikojnë në përputhshmërinë me kriteret e certifikimit.
2. Gjatë periudhës së pezullimit, klienti nuk duhet të përdorë vulën ose shenjën e mbrojtjes së të dhënave në lidhje me veprimin(et) e përpunimit që preken.
3. Organizmi i certifikimit dokumenton arsyet e pezullimit dhe njofton pa vonesë klientin dhe Komisionerin.

Neni 17
Shfuqizimi i certifikimit

1. Organizmi i certifikimit shfuqizon certifikimin në rast se:
   a) konstatohet që klienti nuk i plotëson më kriteret e certifikimit, duke përfshirë kërkesën për të mirëmbajtur funksionalitetin e Sistemit të Menaxhimit të Sigurisë së Informacionit (SMSI) dhe Sistemit të Menaxhimit të të Dhënave Personale (*Privacy Information Management System "*PIMS");
   b) janë konfirmuar shkelje të rënda ose të përsëritura të Ligjit;
   c) klienti rezulton në keqpërdorim të vulës ose shenjës së mbrojtjes së të dhënave ose jep informacion të rremë apo mashtrues;
   ç) procesi pëpunues i certifikuar ka përfunduar, është ndryshuar ndjeshëm ose është zëvendësuar pa një rivlerësim paraprak.
2. Pas shfuqizimit, organizmi i certifikimit njofton menjëherë me shkrim Komisionerin, duke parashtruar arsyet dhe përditëson regjistrin publik të subjekteve të certifikuara.
3. Klienti ndërpret menjëherë përdorimin e çdo reference, vule ose shenje certifikimi dhe i heq ato nga komunikimet publike dhe faqen zyrtare të internetit.

Neni 18
Procesi i ricertifikimit

1. Klienti, certifikimi i të cilit është pezulluar ose shfuqizuar sipas këtij udhëzimi, mund të kërkojë përsëri certifikim, vetëm pasi të ketë vërtetuar se shkaqet e pezullimit ose shfuqizimit nuk ekzistojnë më ose janë korrigjuar.
2. Procesi i ricertifikimit ndjek të njëjtat procedura vlerësimi dhe verifikimi si certifikimi fillestar.

Neni 19
Transferimi i certifikimit

1. Në rast se klienti kërkon transferim të certifikimit, organizmi i certifikimit vepron në përputhje me skemën e certifikimit dhe sigurohet që:
   a) klienti të ketë një certifikatë të vlefshme në momentin e aplikimit;
   b) organizmi i certifikimit merr një kopje të certifikatës ekzistuese, raportit të fundit të vlerësimit dhe dokumenteve mbi ankesat e paraqitura;
   c) organizmi i certifikimit vlerëson mospërputhshmëritë që ekzistojnë, gjetjet e vlerësimit të fundit, ankesat dhe masat korrigjuese;
2. Organizmi i certifikimit merr vendim në lidhje me transferimin e certifikimit brenda një muaji. Në rast se mungojnë dokumente ose ekzistojnë dyshime për përputhshmërinë e klientit, organizmi i certifikimit nuk e transferon atë dhe fillon procesin e certifikimit nga fillimi.

KREU IV
DISPOZITAT TRANZITORE DHE TË FUNDIT

Neni 20
Dispozita tranzitore

Certifikimet e dhëna përpara hyrjes në fuqi të këtij udhëzimi, në përputhje me Udhëzimin e Komisionerit nr. 48, datë 14.09.2018 "Për certifikimin e sistemeve të menaxhimit të sigurisë së informacionit, të dhënave personale dhe mbrojtjes së tyre" do të mbeten të vlefshme deri në përfundimin e tyre.

Neni 21
Dispozita përfundimtare

1. Të gjithë kontrolluesit/përpunuesit publik dhe privat në territorin e Republikës së Shqipërisë janë përgjegjës për respektimin dhe zbatimin e këtij udhëzimi.
2. Mosrespektimi i kërkesave të këtij udhëzimi përbën shkelje të Ligjit dhe sanksionohet, sipas nenit 94, të tij.

Ky udhëzim hyn në fuqi pas botimit në Fletoren Zyrtare.

KOMISIONERI

Besnik Dervishi