

UDHËZIM
Nr. 48, datë 14.9.2018
PËR CERTIFIKIMIN E SISTEMEVE
TË MENAXHIMIT TË SIGURISË SË INFORMACIONIT, TË DHËNAVE PERSONALE
DHE MBROJTJES
SË TYRE

Në mbështetje të shkronjës “F”, pika 1, të nenit 31 dhe të nenit 27, të ligjit nr. 9887, datë 10.3.2008, “Për mbrojtjen e të dhënave personale”, të ndryshuar, dhe në përshtatje me Rregulloren (EU) 2016/679 të Parlamentit Evropian dhe të Këshillit, datë 27 prill 2016, “Mbi mbrojtjen e personave fizikë në lidhje me përpunimin e të dhënave personale dhe lëvizjen e lirë të këtyre të dhënave, si dhe shfuqizimin e direktivës 95/46/EC (Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave), Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale

UDHËZON:

Neni 1

Objekti

Objekti i këtij udhëzimi është certifikimi i sistemeve të menaxhimit për sigurinë e informacionit, të dhënave personale dhe mbrojtjes së tyre, në përputhje me legjislacionin për mbrojtjen e të dhënave personale, si dhe përcaktimi i mekanizmit të certifikimit dhe vlefshmërisë së tij.

Neni 2

Fusha e zbatimit

Ky udhëzim zbatohet për të gjitha subjektet që bëjnë pjesë në fushën e zbatimit të ligjit nr. 9887, datë 10.3.2008, “Për mbrojtjen e të dhënave personale”, të ndryshuar (në vijim “kontrolluesit”), të cilët do të aplikojnë pranë organizmit të akredituar për certifikimin e sistemeve të menaxhimit të sigurisë së informacionit, të të dhënave personale dhe mbrojtjes së tyre.

Neni 3

Përkufizime

1. Termat dhe përkufizimet e përdorur sipas ligjit nr. 9887, datë 10.3.2008, të ndryshuar, do të zbatohen dhe do të kenë të njëjtin kuptim për efekt të këtij udhëzimi.

2. “Organizëm i akredituar” nënkupton një organizëm certifikues të akredituar nga organi përgjegjës i akreditimit dhe i autorizuar nga Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim “Komisioneri”) në cilësinë e autoritetit mbikëqyrës, sipas kriterëve të përcaktuara në nenin 7, i cili kryen vlerësimin e përputhshmërisë së përpunimit të të dhënave personale me legjislacionin përkatës, nëpërmjet kontrollit të ushtruar në mënyrë të pavarur.

3. “Certifikatë konformiteti/përputhshmërie” është dokumenti që lëshohet nga organizmi i akredituar ndaj/për kontrolluesve/it që plotësojnë kriteret ligjore për përpunimin e të dhënave, pa cenuar, në çdo rast, veprimtarinë e Komisionerit.

4. Për efekt të këtij udhëzimi gjejnë zbatim edhe termat dhe përkufizimet e përcaktuara në Standardin Ndërkombëtar ISO/IEC 27001.

Neni 4

Certifikimi dhe detyrat e kontrolluesit

1. Certifikimi kërkohet nga kontrolluesi dhe kryhet nëpërmjet një procesi transparent.

2. Certifikimi jepet për një periudhë deri në tre vjet, me të drejtë rinovimi, kur organizmi i akredituar konstaton se kërkesat përkatëse vazhdojnë të përmbushen.

3. Certifikimi anulohet, nëse është rasti, nga organizmi i akredituar, kur kërkesat për certifikim nuk janë përmbushur apo nuk po përmbushen.

4. Kontrolluesi i cili ia nënshtron përpunimin që kryen mekanizmit të certifikimit, vendos në dispozicion të organizmit të akredituar informacionin dhe aksesin e plotë në aktivitetet e tij përpunuese, të cilat janë të nevojshme për kryerjen e procedurës së certifikimit.

Neni 5

Sistemi i menaxhimit të sigurisë

Kontrolluesi krijon, mirëmban dhe përmirëson në vazhdimësi një sistem menaxhimi të sigurisë së

informacionit, në përputhje me kërkesat e Standardit Ndërkombëtar ISO/IEC 27001, sipas versionit më të fundit të përditësuar.

Neni 6

Regjistri i subjekteve të certifikuara

1. Pranë Zyrës së Komisionerit krijohet regjistri i kontrolluesve të certifikuar për sistemin e menaxhimit të sigurisë së informacionit, të dhënave personale dhe mbrojtjes së tyre.
2. Organizmi i akredituar njofton rast pas rasti Komisionerin, për kontrolluesit e certifikuar.
3. Organizmi i akredituar njofton zyrën e Komisionerit për arsyet e dhënies apo të anulimit të certifikimit të kërkuar, me qëllim demonstrimin e ekzistencës së masave të përshtatshme të sigurisë.
4. Regjistri i kontrolluesve të certifikuar për sistemin e menaxhimit të sigurisë së informacionit, të dhënave personale dhe mbrojtjes së tyre, publikohet në faqen zyrtare të Komisionerit.

Neni 7

Organizmi i akredituar

1. Organizmi i akredituar është subjekti i autorizuar nga Komisioneri për kryerjen e kontrolleve të pavarura për certifikimin e sistemeve të menaxhimit të sigurisë së informacionit, të dhënave personale dhe mbrojtjes së tyre.
2. Organizmi i akredituar ushtron veprimtarinë e tij në zbatim dhe në përputhje me parimin e transparencës në raport me Komisionerin dhe grupet e interesit.
3. Organizmi i akredituar ushtron në mënyrë të pavarur veprimtarinë e kontrollit pranë kontrolluesve.
4. Organizmi i akredituar ushtron veprimtarinë e kontrollit pranë kontrolluesve, me qëllim mbikëqyrjen e përputhshmërisë së sistemit të tyre të menaxhimit të sigurisë së informacionit, të dhënave personale dhe mbrojtjes së tyre me legjislacionin e mbrojtjes së të dhënave personale.
5. Në veprimtarinë e kontrollit, organizmi i akredituar vlerëson edhe zbatimin e kërkesave të udhëzimit nr. 47, datë 14.9.2018, të Komisionerit, “Për përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga kontrolluesit e mëdhenj”.
6. Organizmi i akredituar lëshon certifikatën e përputhshmërisë për kontrolluesit, sipas modelit të miratuar nga Komisioneri, bashkëlidhur këtij udhëzimi.
7. Për përpunimin e të dhënave sensitive, sipas nenit 7, pika 2, shkronja “c”, të ligjit për mbrojtjen e të dhënave personale dhe të dhënave personale, sipas nenit 9, paragrafi 1, certifikata e lëshuar nga organizmi i akredituar, ndikon në lëshimin/dhënien e autorizimit nga Komisioneri.

Neni 8

Kriteret për autorizim

1. Çdo subjekt që kërkon të autorizohet nga Komisioneri për të certifikuar kontrolluesit, në përputhje me këtë udhëzim, duhet:
 - a) Shoqëria (ortakët, ekspertët apo auditorët e saj) të ketë eksperiencë në fushën e certifikimeve sipas standardit ISO/IEC 27001 për një periudhë prej të paktën 10 vitesh.
 - b) Shoqëria të jetë akredituar nga organi përgjegjës i akreditimit në Republikën e Shqipërisë, në përputhje me standardin ISO/IEC 17021-1:2015, “Vlerësimi i konformitetit - Kërkesa për organizmat që kryejnë vlerësimin dhe certifikimin e sistemeve të menaxhimit”, si organizëm certifikimi i sistemeve të menaxhimit të sigurisë së informacionit në përputhje me standardin ISO/IEC 27001.
 - c) Të rezultojë i suksesshëm në zbatimin e legjislacionit për mbrojtjen e të dhënave personale, në rast kontrolli nga zyra e Komisionerit;
 - d) Të ketë të përcaktuar personin përgjegjës për mbrojtjen e të dhënave personale;
 - dh) Të depozitojë procedurat përkatëse të trajtimit të një ankese nga subjektet e të dhënave personale;
 - e) Të provojë pavarësinë dhe ekspertizën e tij në lidhje me objektin e certifikimit;
 - ë) Të depozitojë procedurat për dhënien, rishikimin periodik dhe anulimin e certifikimit të mbrojtjes së të dhënave;
 - f) Të ketë të përcaktuar procedurat dhe strukturat për të administruar ankesat për shkelje të certifikimit apo mbi mënyrën se si certifikimi ka qenë ose është duke u zbatuar nga ana e kontrolluesit ose e përpunuesit dhe të bëjë transparente këto procedura e struktura për subjektet e të dhënave dhe publikun;
 - g) Të depozitojë pranë zyrës së Komisionerit procedurat lidhur me shmangien e konfliktit të interesit në ushtrimin e detyrës dhe të funksioneve të tij në përputhje me këtë udhëzim;
 - gj) Organet certifikuese, të cilat kanë nivel të përshtatshëm ekspertize në lidhje me mbrojtjen e të dhënave,

duhet të japin dhe rinovojnë certifikimin, pa cenuar funksionet dhe kompetencat e zyrës së Komisionerit, pasi të informojnë këtë të fundit, me qëllim që ai t'i lejojë të ushtrojnë funksionet e tyre.

2. Komisioneri revokon autorizimin për organizmin e akredituar, kur kushtet për autorizimin nuk janë duke u përmbushur ose kur veprimet e ndërmarra nga organizmi i akredituar rezultojnë në shkelje të legjislacionit për mbrojtjen e të dhënave personale.

3. Komisioneri revokon certifikimin për kontrolluesin (kur organizmi i akredituar nuk e ushtron këtë detyrim) ose urdhëron organizmin e akredituar të mos lëshojë certifikatën nëse nuk përmbushen kriteret për certifikim.

Neni 9

Regjistri i organizmave të akredituar

Zyra e Komisionerit regjistron të gjithë organizmat e akredituar në një regjistër dhe i publikon ata në faqen zyrtare.

Neni 10

Modeli i menaxhimit të sigurisë së informacionit, të dhënave personale dhe mbrojtjes së tyre

1. Modelet e menaxhimit të kontrolluesve të certifikuar nga organizmi i akredituar, sipas këtij udhëzimi, do të konsiderohen se janë në zbatim dhe përmbushin kërkesat e legjislacionit në fuqi për mbrojtjen e të dhënave personale.

2. Organet inspektuese, në varësi të Komisionerit, për efekt të programimit të aktivitetit të tyre të kontrollit, do të mbajnë parasysh certifikimin e përputhshmërisë që zotëron subjekti objekt kontrolli, të lëshuar nga organizmi i akredituar, sipas këtij udhëzimi.

Neni 11

Dispozita të fundit

1. Moszbatimi i kërkesave të këtij udhëzimi është objekt i sanksioneve të ligjit nr. 9887/2008, "Për mbrojtjen e të dhënave personale", të ndryshuar.

2. Për zbatimin e këtij udhëzimi ngarkohen kontrolluesit objekt i këtij udhëzimi.

Neni 12

Hyrja në fuqi

Ky udhëzim hyn në fuqi pas botimit në Fletoren Zyrtare.

**KOMISIONERI
Besnik Dervishi**

SHTOJCA 1

{Logo e organizmit të akredituar}

Certifikatë Konformiteti/përputhshmërie

Lëshuar për:

[Subjekti kontrollues (i certifikuar)]

Selia: Rr....., nr. - Shqipëri

NUIS: 0000000000000000

[Organizmi i akredituar] certifikon se Sistemi i Menaxhimit të Sigurisë së Informacionit, të Dhënave Personale dhe Mbrojtjes së tyre është kontrolluar dhe rezulton të jetë në përputhje me kërkesat e ligjit nr. 9887/2008, “Për mbrojtjen e të dhënave personale” dhe akteve nënligjore dalë në zbatim të tij, si dhe në përputhje me kërkesat e standardit

ISO/IEC 27001:.....

Për aktivitetet e përfshira në deklaratën e zbatueshmërisë

Certifikata nr.: ____ Kodi/et IAF: ____

Data e lëshimit të certifikatës:

Data e skadencës së certifikatës:

Për organizmin akreditues

[emër/mbiemër i përfaqësuesit]

[nënshkrimi]

Adresa e organizmit akreditues: _____

Për sqarime lidhur me qëllimin, zbatueshmërinë dhe vërtetësinë e kësaj certifikate, mund të kontaktoni në numrin [_____].