U D H Ë Z I M

Nr. 48, datë 14 / 09 /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 e nenit 31 dhe nenit 27 të ligjit nr. 9887, datë 10.03.2008 "Për mbrojtjen e të dhënave personale" i ndryshuar, dhe në përshtatje me Rregulloren (EU) 2016/679 të Parlamentit Evropian dhe 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 10.03.2008 "Për mbrojtjen e të dhënave personale" i 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 përdorura sipas Ligjit nr. 9887 datë 10.03.2008 i 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 kritereve 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 cënuar 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 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 ne 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 14/09/2018 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 akreditуar 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 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 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 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 cënuar 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

Rregjistri i Organizmave të Akredituar

Zyra e Komisionerit regjistron të gjithë Organizmat e Akredituar në një regjistër dhe i publikon ato 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", i 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 [_____]