U D H Ë Z I M

Nr. 47, datë 14/09/2018

PËR
"PËRCAKTIMIN E RREGULLAVE PËR RUAJTJEN E SIGURISË SË TË DHËNAVE PERSONALE TË PËRPUNUARA NGA SUBJEKTET PËRPUNUESE TË MËDHA"

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, Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim Komisioneri),

UDHËZON:

1. Përcaktimin e masave të sigurisë teknike, organizative edhe në lidhje me personelin, për mbrojtjen e të dhënave personale të përpunuara nga subjektet përpunuese të mëdha, më poshtë referuar subjektet përpunuese të të dhënave personale, si dhe rregullat e bashkëpunimit të tyre me Komisionerin.

2. Për qëllime të këtij Udhëzimi, përkufizimet e mëposhtme kanë këto kuptime:
   a) *"Subjekte përpunuese të mëdha"* janë kontrolluesit ose përpunuesit të cilët përpunojnë të dhëna personale në mënyrë elektronike ose manuale, duke shfrytëzuar 6 e më shumë persona për të kryer përpunimin, qoftë në mënyrë të drejtpërdrejtë ose me anë të përpunuesve;
   b) *"Raport vlerësimi"* është raporti i rezultateve të kontrollit të fundit të sigurisë në sistemin e arkivimit;
   c) *"Politika e Sigurisë së Informacionit"* (më poshtë referuar *"PSI"*) është dokumenti me anë të të cilit subjekti përpunues i të dhënave i komunikon punonjësve të tij dhe kontraktorëve (përpunuesve) mënyrën e ndërtimit, zbatimit dhe operimit të Sistemit të Menaxhimit të Sigurisë së Informacionit (më poshtë referuar *"SMSI"*) për mbrojtjen e të dhënave.
   ç) *"Person i kontaktit"* është ai të cilit subjekti përpunues i ka dhënë akses në të dhënat personale.

3. Kategoritë kryesore të përdoruesve, që detyrohen të ruajnë sigurinë e të dhënave personale, janë:
   a) Administratorët e Sistemeve të Teknologjisë së Informacionit, Komunikimit (më tej të quajtur TIK) dhe të Sigurisë së tyre, të cilët zbatojnë këtë detyrim kur subjekti i cili përpunon të dhëna personale ka një sistem TIK të brendshëm dhe/ose të jashtëm të instaluar për të përmbushur këtë qëllim.
   b) Operatorët e të dhënave personale (të punësuarit, të kontraktuarit, etj), të cilët përpunojnë të dhëna personale me qëllim, përmbushjen e detyrave të tyre kur punojnë për subjektin përpunues të të dhënave personale.
   c) Të gjithë personat e caktuar nga subjekti përpunues për të përpunuar të dhënat në mënyrë manuale.

4. Përveç sa parashikohet në Udhëzimin për detyrimet e kontrolluesve përpara se të përpunojnë të dhënat personale, subjektet përpunuese duhet të përpunojnë të dhënat personale në përputhje me rregullat e përcaktuara edhe në këtë Udhëzim.

5. Dispozitat në lidhje me sigurinë e sistemit TIK janë të detyrueshme për ato subjekte që përpunojnë të dhëna personale në mënyrë elektronike. Për ato që përpunojnë të dhëna personale në mënyrë manuale, do të zbatohen vetëm dispozitat përkatëse për sigurinë fizike, sigurinë e ambientit dhe të personelit.

6. Komisioneri në çdo kohë mund t'i kërkojë subjektit përpunues të të dhënave personale të provojë nivelin dhe përmbajtjen e masave të sigurisë teknike, organizative edhe në lidhje me personelin me anë të një raport vlerësimi. Raporti i vlerësimit duhet të jetë hartuar nga subjekti përpunues jo më tepër se dy vjet përpara kërkesës së Komisionerit. Subjektet përpunuese duhet të paraqesin, brenda pesëmbëdhjetë ditëve nga dita e kërkesës, raportin e vlerësimit. Nëse vlerësimi nuk paraqitet në afat, Komisioneri i kërkon subjektit përpunues të të dhënave personale që me shpenzimet e tij të kryejë një kontroll të ri dhe të dorëzojë raportin e vlerësimit brenda tre muajve.

7. Kontrolli i sigurisë së sistemit të përpunimit të të dhënave mund të kryhet vetëm nga një auditues i pavarur dhe i paanshëm si dhe profesionalisht i kualifikuar, i cili nuk ka marrë pjesë në zhvillimin, zbatimin dhe drejtimin e Sistemit të Menaxhimit të Sigurisë së Informacionit të sistemit të arkivimit.

Kapitulli I
Sistemi i Menaxhimit të Sigurisë së Informacionit (SMSI) për mbrojtjen e të dhënave

8. Krijimi dhe mirëmbajtja e SMSI-së për mbrojtjen e të dhënave personale është i detyrueshëm për të gjithë subjektet përpunuese. Ky sistem bazohet në identifikimin, analizimin dhe në zbutjen e rreziqeve ndaj sigurisë së të dhënave personale duke marrë parasysh dobësitë e:

a) sistemeve TIK të përdorur për përpunimin e të dhënave personale;
b) të gjitha formave manuale të përpunimit të të dhënave personale;
c) sigurisë fizike, brenda dhe jashtë ambienteve, sigurisë së personelit dhe pajisjeve elektronike ose të lëvizshme.

9. Në rast se kontrolluesi përdor më shumë se një përpunues, çdo përpunues duhet të ketë vënë në zbatim një SMSI. Ndarja e përgjegjësive për mbrojtjen e të dhënave personale ndërmjet palëve duhet të shprehet qartë në dokumentacionin që rregullon marrëdhëniet e tyre kontraktore. Të gjitha këto kërkesa do të përmbushen pa cënuar marrëdhënien kontraktore të delegimit (outsourcing). Kur kontrolluesi përdor një përpunues, atij do t'i komunikohen vetëm pjesët e zbatueshme për SMSI-në, të cilat do të jenë ligjërisht të detyrueshme në një kontratë për përpunimin e të dhënave.

10. SMSI do të përcaktohet duke marrë parasysh standartet e sigurisë së informacionit, si më poshtë:

a) *"konfidencialitetin"*, duke siguruar që të dhënat të jenë të aksesueshme vetëm për personat e autorizuar;
b) *"integritetin"*, duke siguruar që të dhënat të jenë të sakta, të plota dhe duke ruajtur metodat e përpunimit të tyre;
c) *"disponueshmërinë"*, duke siguruar aksesin e përdoruesit të autorizuar në të dhënat dhe në sistemet e përpunimit;
ç) *"besueshmërinë"* e sistemeve TIK që janë përdorur për përpunimin e të dhënave dhe të personelit që i ka përdorur ato, duke garantuar që çdo aktivitet/veprim i tyre mbi të dhënat është i gjurmueshëm dhe i kontrollueshëm.

11. SMSI do të përfshijnë, në veçanti:
a) Analizën e Ndikimit në të Dhënat Personale. Përpara përpunimit të të dhënave personale, kontrolluesi ose përpunuesi duhet të kryejë një vlerësim të ndikimit të operacioneve të përpunimit që janë parashikuar në mbrojtjen e të dhënave personale duke evidentuar se ku këto operacione përpunimi mund të paraqesin rreziqe të veçanta ndaj të drejtave dhe lirive të subjekteve të të dhënave për shkak të natyrës, shtrirjes ose qëllimit të tyre;
b) Politikën e Sigurisë së Informacionit, përfshirë sigurinë e përpunimit të të dhënave personale;
c) Kontrollin e sigurisë së sistemit të arkivimit të të dhënave personale;
ç) Udhëzime të detajuara të sigurisë që mbulojnë fushat specifike;
d) Sigurinë fizike brenda dhe jashtë ambienteve;
dh) Sigurinë e personelit dhe pajisjeve elektronike të lëvizshme ose jo.

12. SMSI duhet të funksionojë në përputhje me aktet ligjore dhe nënligjore në fuqi, standardet teknike për sistemet e sigurisë së TIK-së, rregullat e praktikës së mirë në fushën e sigurisë së informacionit, dhe rekomandimet e hartuara nga organizata industriale profesionale, përfshirë bankat, telekomunikacionet, siguracionet, sigurimet shoqërore dhe kujdesin shëndetësor. SMSI duhet të jetë e përshtatur me nivelin e rreziqeve dhe dobësitë e sistemeve të përpunimit të të dhënave personale.

13. Në rast se përpunimi i të dhënave kryhet me anë të shërbimeve *"cloud computing"* ose me anë të përpunimit të lëvizshëm, do të zbatohen masa sigurie shtesë (p.sh aktivizimi i shërbimit kundër- vjedhjes në kompjuterin portabël ose në telefonin smart). Të gjitha pajisjet që shërbejnë si mbartës të dhënash do të kodohen.
Ruajtja e të dhënave në këto shërbime bëhet në përputhje me qëllimin e mbledhjes së tyre. Të dhënat mbahen në tejkalim të afatit vetëm pas informimit paraprak të subjektit dhe dhënies së pëlqimit prej tij në mënyrë të qartë si dhe duke i dhënë/rezervuar të drejtën për të refuzuar. Procesi i shkatërrimit realizohet në mënyrë të pakthyeshme.
Të dhënat personale që përpunohen me anë të këtyre shërbimeve nuk duhet të transferohen jashtë territoreve të shteteve anëtare të Bashkimit Europian dhe Shqipërisë, pa marrë më parë opinionin e autoritetit përgjegjës për mbrojtjen e të dhënave personale.

14. Subjektet përpunuese përcaktojnë hapat që duhen ndërmarrë në rast incidentesh të shkeljes së sigurisë së të dhënave personale. Pas rezultatit të analizës së riskut, duhet të propozohet zbutja e duhur e rreziqeve në një nivel të pranueshëm. SMSI duhet të përfshijë

edhe marrëveshjet specifike për vazhdimësinë e veprimtarisë tregtare, për vendosjen e të cilave zbatohen standardet teknike dhe rekomandimet e vëna në dispozicion për publikun.

15. Dokumentacioni i SMSI-së mbahet nga personi i kontaktit për çështjet e mbrojtjes së të dhënave, i emëruar nga subjekti përpunues i të dhënave personale. Ky dokumentacion duhet të vihet në dispozicion të Komisionerit me kërkesën e tij brenda afatit të përcaktuar në kërkesë nga data e marrjes dijeni.

Kapitulli II
Politika e Sigurisë së Informacionit

16. PSI duhet të hartohet dhe zbatohet përkatësisht nga subjekti përpunues i të dhënave personale.

17. PSI hartohet dhe mbahet në përputhje me rregullat e sigurisë së informacionit, siç përcaktohen nga aktet ligjore dhe nënligjore në fuqi dhe legjislacioni ndërkombëtar që rekomandohet nga standardet e përcaktuara të sigurisë, si dhe rekomandimet e Komisionerit. Analiza e riskut është pjesë përbërëse e PSI-së. Dokumenti i PSI-së specifikon qartë objektivat e sigurisë dhe përcakton masat teknike, organizative edhe në lidhje me personelin, për zbutjen e kërcënimeve dhe rreziqeve që prekin sistemet e arkivimit.

18. Në strukturimin e PSI-së, i kushtohet vëmendja e duhur standardeve teknike të sigurisë së informacionit, kodeve të praktikës së mirë, si dhe rekomandimeve e udhëzimeve të veçanta të miratuara nga Komisioneri. PSI-ja do të mbulojë aspektet e mëposhtme të sigurisë së informacionit të të dhënave personale:

a) Vlerësimin dhe trajtimin e riskut përmes kryerjes së analizës së riskut ndaj sigurisë së informacionit të subjektit përpunues;
b) Politikën e Sigurisë e cila nënkupton miratimin dhe zbatimin e dokumentit që vërteton mbështetjen dhe angazhimin që ka struktura drejtuese e subjektit ndaj sigurisë së informacionit;
c) Organizimin e sigurisë së informacionit nëpërmjet marrjes së masave për mbrojtjen e informacionit dhe sistemeve të tij nga aksesi i paautorizuar dhe nëpërmjet kryerjes së kontrolleve të sigurisë.
ç) Menaxhimin e aseteve duke përditësuar inventarin e të gjitha mjeteve të përpunimit dhe klasifikimin e kushteve të sigurisë për të përcaktuar se çfarë do të mbrohet, pse dhe si;
d) Sigurinë e burimeve njerëzore nëpërmjet marrjes së masave të sigurisë për punonjësit që rekrutohen, lëvizin dhe largohen nga subjekti përpunues;
dh) Sigurinë fizike dhe mjedisore nëpërmjet mbrojtjes së pajisjeve kompjuterike;
e) Menaxhimin e komunikimeve dhe operacioneve nëpërmjet kontrolleve të sigurisë teknike në sisteme dhe rrjete kompjuterike;
ë) Kontrollin e aksesit nëpërmjet kufizimit të të drejtave të aksesit në rrjet, sisteme, aplikime, funksione dhe të dhëna;

f) Blerjen, zhvillimin dhe mirëmbajtjen e sistemeve të përpunimit të informacionit nëpërmjet ndërtimit të sigurisë në aplikacione;

g) Menaxhimin e shkeljeve të sigurisë së informacionit (referuar si incidente) nëpërmjet parashikimit dhe dhënies së kundër përgjigjes ndaj shkeljeve të sigurisë së informacionit;

gj) Menaxhimin e vazhdimësisë së veprimtarisë tregtare nëpërmjet mbrojtjes, ruajtjes dhe rikuperimit të proceseve e sistemeve kritike;

h) Sigurimin e pajtueshmërisë me politikat e veçanta të sigurisë së informacionit, standardet, ligjet dhe rregulloret.

19. Gjatë zbatimit të dispozitave të këtij Kapitulli, trajtohen në mënyrë të veçantë nga PSI-ja:

a) Përpunimi i të dhënave sensitive;

b) Menaxhimi i të drejtave të aksesit;

c) Rreziqet që vijnë nga aksesi në rrjetet publike, veçanërisht nga Interneti.

20. PSI-ja specifikon objektivat bazë të sigurisë që duhet të arrihen për mbrojtjen e sistemit të arkivimit të të dhënave personale kundër shkeljes së sigurisë së saj dhe në veçanti ajo duhet të:

a) përcaktojë objektiva të sigurisë bazë dhe masa për sigurinë minimale të kërkuar;

b) përcaktojë masa teknike, organizative edhe në lidhje me personelin për sigurimin e të dhënave personale në sistemin e arkivimit dhe mënyrën e përdorimit të tyre;

c) bëjë përshkrimin e sistemit të arkivimit dhe lidhjen e tij me shkelje të mundshme të sigurisë;

ç) bëjë përkufizimin e kufijve që përcaktojnë rreziqet e mbetura.

21. Analiza e sigurisë së sistemit të arkivimit nënkupton një analizë të detajuar të gjendjes së sigurisë duke përfshirë, në veçanti:

a) Analizën e riskut, në të cilën identifikohen kërcënimet që prekin pjesë individuale të sistemit të arkivimit, të afta të shkelin sigurinë apo funksionimin e tij; rezultati i analizës së riskut do të jetë një listë e kërcënimeve që mund të rrezikojnë konfidencialitetin, integritetin dhe disponueshmërinë e të dhënave personale të përpunuara, ndërkohë që ajo do të deklarojë edhe shkallën e riskut të mundshëm, propozimet e masave për eliminimin apo minimizimin e ndikimit të riskut dhe një listë të rreziqeve të mbetura;

b) Përdorimin e standardeve të sigurisë dhe përcaktimin e metodave të tjera dhe mjeteve për mbrojtjen e të dhënave personale; vlerësimin e përshtatshmërisë së masave të sigurisë të propozuara nga standardet e sigurisë të aplikuara, metodat dhe mjetet do të përbëjnë një pjesë të analizës së sigurisë së sistemit të arkivimit.

c) Hartimin e rregulloreve të detajuara mbi sigurinë të cilat do të specifikojnë dhe zbatojnë rezultatet që dalin nga SMSI sipas kushteve konkrete të sistemit të arkivimit të vënë në punë të cilat do të përfshijnë, në veçanti:

i. përshkrimin e masave teknike, organizative edhe në lidhje me personelin të përcaktuara në SMSI dhe përdorimin e tyre në kushtet konkrete;

ii. shtrirjen e kompetencave dhe përshkrimin e veprimtarive të lejuara të

personave individualë që i gëzojnë ato të drejta, mënyrën e identifikimit të tyre dhe verifikimin gjatë aksesimit në sistemin e arkivimit;

iii. objektin e përgjegjësisë së personave të ngarkuar dhe të Personit të Kontaktit;

iv. mënyrën, formën dhe periodicitetin e kryerjes së aktiviteteve të inspektimit të fokusuara në vëzhgimin e sigurisë së sistemit të arkivimit;

v. procedurat gjatë avarive, dështimeve dhe situatave të tjera të jashtëzakonshme, duke përfshirë masat parandaluese për kufizimin e zhvillimit të situatave të jashtëzakonshme dhe mundësive për një restaurim efikas të gjendjes njësoj si përpara avarisë.

Kapitulli III
Raste të veçanta të përpunimit

22. Për subjektet që përpunojnë të dhëna personale në mënyrë manuale zbatohet dispozitat e mëposhtme:

a) Të gjitha dokumentet e përpunuara në mënyrë manuale ruhen të sigurta në mënyrë që të parandalohet përhapja, shkatërrimi, humbja e paligjshme, si në vendin e punës ashtu edhe gjatë transferimit të tyre;

b) Vënia në dispozicion e kopjeve të kërkuara, mund të kryhet me kusht që të jetë i mundur gjurmimi i përdorimit të tyre të mëtejshëm deri në shkatërrimin ose anonimizimin e tyre;

c) Me mbarimin e periudhës së ruajtjes, dokumentet:

i. arkivohen, në rast se ekziston një detyrim i tillë ligjor; ose

ii. shkatërrohen fizikisht në mënyrë të pakthyeshme; ose

iii. bëhen anonime duke i kthyer të dhënat personale që ato mbajnë të palexueshme, në mënyrë të parevokueshme.

ç) Në rast se nuk është përcaktuar nga legjislacioni në fuqi, i cili rregullon përpunimin e veçantë të të dhënave, periudha e mbajtjes së të dhënave përcaktohet nga çdo kontrollues në përputhje me qëllimin e mbledhjes së të dhënave. Për çdo ndryshim në afatin e ruajtjes, kontrolluesi rivlerëson kohën e ruajtjes si dhe njofton subjektin e të dhënave. Pas përfundimit të periudhës së mbajtjes së të dhënave, subjekti i të dhënave hiqet në mënyrë të pakthyeshme nga të gjithë sistemet aktive të përpunimit të të dhënave, automatik, manual apo të anonimizuar.

23. Për subjektet që përpunojnë të dhëna sensitive, si në mënyrë manuale ashtu edhe elektronike, rregullat shtesë të mëposhtme do të jenë të zbatueshme, përkatësisht për çdo mënyrë përpunimi:

a) Vëmendje e veçantë i kushtohet parandalimit të përhapjes së paligjshme:

i. në rast përpunimi manual, SMSI parashikon procedura shtesë specifike për trajtimin e dokumenteve shkresore me qëllim parandalimin e aksesit nga persona të paautorizuar në të dhënat personale që përmbajnë këto dokumente, gjatë gjithë ciklit jetësor të tyre;

ii. në rast transferimi elektronik të të dhënave personale, kanalet e transmetimit apo dokumentet që përmbajnë këto të dhëna do të kodohen, duke përdorur mënyra kodimi në përputhje me rezultatet e analizës së riskut të kryer më parë.

iii. në rast përdorimi të mjeteve elektronike portative si mbartës të informacionit, të dhënat do të kodohen përpara se të largohen nga mjediset e subjektit përpunues të të dhënave. Ky kodim këshillohet të kryhet gjithashtu edhe për të dhënat jo-senstitive.

Kapitulli IV
Trajnimi i personelit të Subjektit Përpunues të të Dhënave Personale

24. Personeli i Subjektit përpunues të të dhënave personale trajnohet rregullisht për mbrojtjen e të dhënave personale. Trajnimi kryhet sipas planit të përcaktuar më poshtë:

a) Personeli që përpunon të dhëna personale trajnohet të paktën një herë në vit;

b) Personeli përveç përcaktimit në shkronjën *"a"*, trajnohet për të gjithë rastet e veçanta të listuara më poshtë:

i. Pas çdo ndryshimi thelbësor të ligjit për mbrojtjen e të dhënave personale,

ii. Pas çdo ndryshimi thelbësor të kuadrit ligjor evropian për mbrojtjen e të dhënave personale, i cili paraprakisht publikohet në faqen zyrtare të Komisionerit,

iii. Pas ndryshimit të organizimit të SMSI-së, veçanërisht të PSI-së,

iv. Pas ndryshimit të procedurave të veçanta të sigurisë së përpunimit të të dhënave personale të subjektit përpunues.

Qëllimi i trajnimit dhe forma e organizimit të tij duhet të zbatohen në përputhje me dispozitat e këtij udhëzimi.

25. Subjekti përpunues i të dhënave personale siguron trajnim profesional për personat e ngarkuar të caktuar. Komisioneri mund t'i kërkojë Subjektit përpunues të të dhënave personale të sigurojë prova për zhvillimin e trajnimit profesional.

Kapitulli V
Kontrolli i Sigurisë së Informacionit të Subjektit Përpunues të të Dhënave Personale

26. Kontrolli i sigurisë së informacionit (të dhënave personale) nga subjektet përpunuese kryhet jo më pak se një herë në vit.
Komisioneri mund të kërkojë vënien në dispozicion të raporteve të kontrollit.

Kapitulli VI
Personi i Kontaktit në subjektet përpunuese

27. Subjekti përpunues i të dhënave personale është përgjegjës për mbikëqyrjen e brendshme të mbrojtjes së të dhënave personale të përpunuara. Çdo subjekt që i nënshtrohet këtij udhëzimi do të autorizojë me shkrim të paktën një person të ngarkuar,

për të kryer këtë mbikëqyrje. Subjekti përpunues do të njoftojë Komisionerin për autorizimin e vetëm një personi të kontaktit, edhe në rast se ai mund të emërojë disa për mbikëqyrjen e brendshme të mbrojtjes së të dhënave personale. Nëse subjekti zëvendëson personin e kontaktit, ai duhet të njoftojë Komisionerin jo më vonë se 14 ditë nga data e zëvendësimit.

28. Përpunuesi objekt i këtij udhëzimi emëron një ose më shumë persona të ngarkuar, përgjegjës për garantimin e sigurisë së përshtatshme të të dhënave personale, kur vepron në emër të Kontrolluesit. Përpunuesit e vegjël të kontraktuar nga subjekti përpunues që i nënshtrohet këtij udhëzimi, gjithashtu këshillohet të emërojnë një Person të ngarkuar.

29. Personi i kontaktit mund të jetë çdo person që plotëson kushtet e mëposhtme:

a) gëzon zotësi të plotë juridike dhe për të vepruar;
b) gëzon integritet;
c) ka arsim të lartë juridik ose shkenca kompjuterike;
ç) shquhet për aftësi profesionale dhe figurë të pastër etiko-morale;
d) ka eksperiencë pune jo më pak se 5 vjet në profesionin e juristit ose të ekspertit të IT, ose ka punuar më shumë se 3 vjet në institucionin e Komisionerit me detyrën e juristit ose ekspertit IT;
dh) nuk është dënuar me vendim të formës së prerë për kryerjen e një vepre penale.

Ai dorëzon vërtetim të gjendjes gjyqësore të përditësuar, e cila mbahet nga kontrolluesi gjatë kryerjes së funksionit të tij.

30. Përpara fillimit të përpunimit të të dhënave personale në sistemin e arkivimit, personi i kontaktit vlerëson riskun e shkeljes së të drejtave dhe lirive të subjekteve të të dhënave. Kjo analizë është pjesë përbërëse e Analizës së Ndikimit në të Dhënat Personale.

31. Personi i kontaktit, në kohën e duhur, njofton me shkrim subjektin përpunues të të dhënave për çdo rrezik shkelje të të drejtave të subjekteve të të dhënave, përfshirë shkeljen e legjislacionit për mbrojtjen e të dhënave personale.

32. Në rast se, pas njoftimit të personit të kontaktit, subjekti përpunues i të dhënave personale, dështon në marrjen e masave të duhura për trajtimin e problemit në kohën e duhur, personi i kontaktit njofton Komisionerin pa vonesë.

33. Brenda 30 ditëve nga data e përfundimit të mbikëqyrjes së brendshme, Subjekti përpunues i të dhënave personale që ka autorizuar personin e kontaktit do të njoftojë Komisionerin. Njoftimi duhet të përmbajë:

a) emrin, adresën, numrin e identifikimit (NIPT-in) dhe/ose përfaqësuesit ligjor të subjektit;
b) gjeneralitetet e personit të kontaktit;
c) pozicionin e personit të kontaktit brenda subjektit përpunues;
ç) datën e emërimit më shkrim të personit të kontaktit;
d) deklaratën e subjektit përpunues ku përcaktohet se personi i kontaktit plotëson kushtet e parashikuara në pikën 29.

34. Personi i kontaktit ka këto detyra dhe përgjegjësi:

a) është përgjegjës për mbikëqyrjen e brendshme, të përmbushjes së detyrimeve për mbrojtjen e të dhënave personale nga ana e Subjektit përpunues të të dhënave personale;

b) jep këshilla për personat përgjegjës;

c) është përgjegjës për zbatimin e masave teknike, organizative, edhe në lidhje me personelin, si dhe mbikëqyr zbatimin e tyre në praktikë. Në veçanti, ai do të sigurojë dokumentacionin e SMSI-së që provon hartimin dhe mirëmbajtjen e duhur të saj;

ç) në rast kontraktimi të një përpunuesi nga ana e subjektit përpunues të të dhënave personale, personi i kontaktit është përgjegjës për mbikëqyrjen e brendshme të veprimtarisë së përpunuesit, për përmbajtjen dhe hartimin e kontratës me shkrim për Përpunuesin. Gjatë kohëzgjatjes së marrëdhënies kontraktuale apo autorizimit, personi i kontaktit do të verifikojë respektimin e kushteve të miratuara, duke përfshirë edhe angazhimin dhe ndryshimin e Përpunuesve, në rast se ka.

d) është përgjegjës për mbikëqyrjen e brendshme të transferimeve ndërkombëtare të të dhënave personale;

dh) është përgjegjës për dorëzimin e dokumentacionit të sistemeve të arkivimit për regjistrim të veçantë dhe shpalljen e ndryshimeve dhe çregjistrimin e sistemeve të arkivimit nga regjistri i veçantë. Ai mban të dhëna të sistemeve të arkivimit që nuk janë subjekt regjistrimi dhe i vendos ato në dispozicion të kujtdo që ligjërisht ka të drejtë të ketë akses në to;

e) është përgjegjës për bashkëpunimin e nevojshëm me Komisionerin në përmbushjen e detyrave brenda përgjegjësive të tij;

ë) me kërkesën e Komisionerit, ai është i detyruar t'i paraqesë autorizimin me shkrim mbi bazën e të cilit ai vepron, si dhe dëshmi për shkallën e njohurive të fituara në trajnime profesionale.

35. Pas caktimit të personit të kontaktit për mbikëqyrjen e brendshme të mbrojtjes së të dhënave personale, Subjekti përpunues i të dhënave personale përjashtohet nga detyrimi për të paraqitur për regjistrim sistemet e arkivimit të të dhënave jo-sensitive.

36. Personi i kontaktit siguron mbajtjen e rregullt të një inventari të sistemeve të arkivimit të të dhënave personale të përpunuara nga Subjekti përpunues i të dhënave personale, përfshirë të dhënat personale të përjashtuara nga detyrimi për regjistrim në autoritetin e Komisionerit.

37. Aksesi në këtë inventar të sistemeve të arkivimit të të dhënave personale i ofrohet autoritetit të Komisionerit dhe subjekteve të të dhënave personale, të dhënat e të cilëve përpunohen në sistemin e veçantë të arkivimit, mbi bazën e një kërkese, pa vonesë.

38. Subjekti përpunues i të dhënave personale është i detyruar t'i mundësojë personit të kontaktit të zbatojë mbikëqyrjen e brendshme të mbrojtjes së të dhënave personale në mënyrë të pavarur dhe të pranojë propozimet e ligjshme të tij. Njoftimi i mangësive ose bërja e një kërkese nga personi i kontaktit në lidhje me përmbushjen e detyrimeve të tij nuk duhet të bëhet nxitje apo arsye për kryerjen e një veprimi nga ana e subjektit, në dëm të personit të kontaktit.

39. Komisioneri ka të drejtë ti komunikojë dhe kërkojë subjektit përpunues të të dhënave personale për të autorizuar një person tjetër të ngarkuar për mbikëqyrjen e brendshme të mbrojtjes së të dhënave personale, me kusht që të jetë vërtetuar se ai i cili fillimisht ka qenë i autorizuar, ka dështuar ose nuk ka përmbushur në mënyrë të mjaftueshme detyrimet e tij, ose ka vlerësuar gabimisht ose ka aplikuar gabimisht në praktikë të drejtat dhe detyrimet e subjektit të parashikuara nga ky akt, ose nuk përmbush kushtet profesionale apo etike.

40. Subjekti përpunues i të dhënave personale është i detyruar të përmbushë kërkesën e Komisionerit në kohën e duhur dhe të autorizojë, brenda 15 ditëve, një person tjetër për mbikëqyrjen e brendshme.

41. Nëse nuk është e mundur, për arsye objektive, të zbatohet afati i përcaktuar në pikën 40, Komisioneri do të ofrojë një muaj shtesë për subjektin përpunues të të dhënave personale.

Kapitulli VII
Rregullat e pajtueshmërisë

42. Rregullat e mëposhtme ndiqen për të garantuar pajtueshmërinë e duhur me këtë udhëzim:

a) Të miratohet përqasja formale e analizës së riskut ndaj sigurisë së informacionit, bazuar mbi standardet e sigurisë së informacionit, në mënyrë që mbrojtja e të dhënave personale të jetë pjesë e pandarë e SMSI-së brenda subjektit përpunues;

b) Nëse subjekti përpunues ka vendosur të certifikojë pajtueshmërinë e tij me standardet teknike të sigurisë, ai duhet të vendosë në dispozicion të Komisionerit këtë certifikatë. Procesi i certifikimit për pajtueshmërinë me standardet e sigurisë së informacionit do të përfshijë edhe identifikimin, menaxhimin dhe zbutjen e dobësive dhe rreziqeve të sigurisë së të dhënave personale;

c) Shkeljet e rënda të sigurisë së të dhënave personale duhet të raportohen menjëherë te Komisioneri. Në rast se është emëruar personi i kontaktit atëherë kjo është detyrë e tij.

43. Raportet e përditësuara të kontrollit mund të jenë plotësisht të pranueshme si një provë e pajtueshmërisë së subjektit përpunues me ligjin për mbrojtjen e të dhënave personale, vetëm pasi hapat e mësipërme të jenë zbatuar dhe ai të ketë ruajtur çertifikimet e pajtueshmërisë me standardet e sigurisë së informacionit që mbulojnë edhe përpunimin e të dhënave personale.

44. Përpara se të lidh një marrëveshje kontraktore që përfshin përpunimin e të dhënave personale, kontrolluesi ka detyrimin të kontrollojë Përpunuesin për pajtueshmërinë e tij me ligjin për mbrojtjen e të dhënave personale.

45. Komisioneri, mbi këtë bazë, mund t'i kërkojë personit të kontaktit të kryejë një pjesë

të procedurave të inspektimit, përfshirë kontrollin paraprak të dosjeve të të dhënave personale që përmbajnë të dhëna sensitive.

46. Për zbatimin e këtij udhëzimi ngarkohen të gjithë kontrolluesit publik e privat në territorin e Republikës së Shqipërisë, të përcaktuar në shkronjën a) të pikës 2 të këtij udhëzimi.

47. Moszbatimi i kërkesave të këtij udhëzimi, përbën shkelje të ligjit për mbrojtjen e të dhënave personale dhe dënohet sipas nenit 39 të ligjit për mbrojtjen e të dhënave personale , i ndryshuar.

48. Udhëzimi nr. 21, datë 24.09.2012 *"Për përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga kontrolluesit e mëdhenj"* i ndryshuar, shfuqizohet.

Ky udhëzim hyn në fuqi pas botimit në fletoren zyrtare.

KOMISIONERI

Besnik Dervishi