REPUBLIKA E SHQIPËRISË
KOMISIONERI PËR TË DREJTËN E INFORMIMIT DHE MBROJTJEN E TË DHËNAVE PERSONALE

DREJTORIA E HETIMIT ADMINISTRATIV

Nr. 1165/3 prot. Tiranë më 11.11.2020

REKOMANDIM

Nr. 26, datë 11.11.2020

PËR KONTROLLUESIN "PEGASUS MED" SHPK

Në mbështetje të neneve 29, 30 dhe 32 të ligjit nr. 9887, datë 10.03.2008 "*Për mbrojtjen e të dhënave personale*" i ndryshuar (në vijim, "*Ligji*"), ligjit nr. 44/2015 "*Kodi i Procedurave Administrative të Republikës së Shqipërisë*" (në vijim "*Kodi i Procedurave Administrative*"), procesverbalit të hetimit administrativ dhe provave të administruara në ngarkim të kontrolluesit Pegasus MED SHPK,

KONSTATOVA SE:

Në zbatim të Urdhrit nr.150, datë 28.09.2020 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, u krye hetimi administrativ pranë kontrolluesit "Pegasus MED" SHPK (në vijim, "*Kontrolluesi*"), me objekt:

- Zbatimi i ligjit nr. 9887, datë 10.03.2008 "*Për mbrojtjen e të dhënave personale*" i ndryshuar dhe akteve të miratuara nga Komisioneri në lidhje me mbledhjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale, gjatë kryerjes së aktivitetit nga kontrolluesi *"Pegasus MED"* SHPK.

Zyra e Komisionerit, pasi shqyrtoi relacionin e hetimit administrativ, procesverbalin e konstatimit dhe provat e administruara gjatë ushtrimit të hetimit, vëren se:

1. Kontrolluesi ka si objekt të veprimtarisë tregtare "*Ushtrimin e veprimtarisë në fushën e kujdesit mjeksor, diagnostikimin e sëmundjeve të ndryshme, kryerjen e ekzaminimeve laboratorike, etj.*".

   Kontrolluesi mbledh dhe përpunon të dhëna personale dhe sensitive, ndër të tjera, edhe për kategoritë e subjekteve të të dhënave *"kandidatë për punë", "punonjës të larguar"* dhe *"pacientë"*. Të dhënat përpunohen në mënyrë manuale dhe elektronike.

Lidhur me kategorinë e subjekteve të të dhënave "*punonjës të larguar*", Kontrolluesi nuk ka parashikuar asnjë afat për kohën e ruajtjes së të dhënave personale, në kundërshtim me parimin e mbrojtjes së të dhënave personale, sanksionuar në germën "d" të nenit 5 dhe nenit 6 të Ligjit dhe me Udhëzimin nr. 11, datë 08.09.2011 për "*Përpunimin e të dhënave të punonjësve në sektorin privat*" të miratuar nga Komisioneri (në vijim *"Udhëzimi nr.11"*).

Kontrolluesi përpunon të dhënat personale dhe sensitive (shëndetësore) të pacientëve në Sistemin Informatik të Laboratorit (SLIS). Fillimisht, pacientët paraqesin të dhënat personale për t'u regjistruar në sistem. Të dhënat që kërkohen të detyrueshme për regjistrim janë emër, mbiemër, numër personal identifikimi dhe datëlindje, ndërsa të dhëna opsionale janë vendbanimi, numër telefoni, adresë emaili, etj.

Zyra e Komisionerit vlerëson se ruajtja e *numrit personal të identifikimit* të pacientëve është në tejkalim të qëllimit të përpunimit për ofrimin e shërbimeve laboratorike, në kundërshtim me parimet e mbrojtjes së të dhënave personale sanksionuar në gërmën *"c"* të pikës 1, të nenit 5 dhe nenit 6 të Ligjit.

2. Kontrolluesi nuk informon subjektet e të dhënave se cilat të dhëna personale janë të detyrueshme për t'u paraqitur dhe cilat janë vullnetare, qëllimin dhe mënyrat e përpunimit të të dhënave, masat e sigurisë, të drejtat e subjekteve të të dhënave dhe detyrimet e kontrolluesit.

   Zyra e Komisionerit vlerëson se mungesa e informimit mbi përpunimin e të dhënave personale është në kundërshtim me parashikimet e nenit 18 të Ligjit dhe Udhëzimin nr. 49, datë 02.03.2020 "*Për mbrojtjen e të dhënave shëndetësore*" (në vijim, *"Udhëzimi nr. 49"*).

3. Kontrolluesi ka lidhur një "akt marrëveshje" për rregullimin e të drejtave dhe detyrimeve të ndërsjellta të palëve në lidhje me shërbimet mjekësore që do të ofrohen nga institucioni shëndetësor privat, për të siguruarit me sigurim shëndetësor SIGAL si dhe aneks kontratë *"Për përpunimin e të dhënave personale nga një palë e tretë"*.

   Zyra e Komisionerit vlerëson se në *"akt marrëveshje"* dhe në aneks kontratë nuk është shprehur qartë qëllimi dhe parashikimet konkrete mbi detyrimet e palëve në lidhje me përpunimin e të dhënave personale, në kundërshtim me parashikimet në nenin 20 të Ligjit dhe Udhëzimit 19, datë 03.08.2012, të Komisionerit *"Mbi rregullimin e marrëdhënieve mes kontrolluesit dhe përpunuesit në rastet e delegimit të përpunimit të të dhënave dhe përdorimin e një kontrate tip në rastet e këtij delegimi"* i ndryshuar (në vijim, "*Udhëzimi nr.19*").

4. Kontrolluesi ka hartuar "*Rregulloren për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*", në zbatim të nenit 27 të Ligjit por përmbajtja e saj është e kufizuar dhe nuk reflekton detyrimet ligjore, sipas kategorive specifike të të dhënave personale që përpunon Kontrolluesi, si dhe kategorive të subjekteve të të dhënave në referim të parimeve ligjore dhe rregullave specifike të parashikuara në udhëzimet specifike të miratuara nga Komisioneri.

Zyra e Komisionerit vlerëson se është i nevojshëm rishikimi i këtij akti, në përputhje me të gjitha proceset përpunuese të të dhënave personale, përkufizimet, transferimin ndërkombëtar të të dhënave, etj.

5. Kontrolluesi nuk ka ndërmarrë masa konkrete në kuadër të trajnimit të punonjësve që kanë akses dhe përpunojnë të dhëna personale lidhur me legjislacionin në fuqi për mbrojtjen e të dhënave personale. Rezulton mosplotësim i detyrimeve në lidhje me ngritjen, administrimin dhe mirëmbajtjen e sistemit të menaxhimit së sigurisë së informacionit (SMSI) lidhur me mbrojtjen e të dhënave personale, të parashikuara nga Udhëzimi nr. 47, datë 14.09.2018, të Komisionerit "*Për përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga subjektet përpunuese të mëdha*" (në vijim, "*Udhëzimi nr. 47*").

   Zyra e Komisionerit vlerëson se, për shkak të cilësisë si subjekt përpunues i madh, si dhe për shkak të natyrës së veprimtarisë që ushtron, e cila kërkon masa të shtuara teknike dhe organizative për garantimin e sigurisë së të dhënave personale, Kontrolluesi, është i detyruar të krijojë, mirëmbajë dhe administrojë SMSI në përputhje me parashikimet e Udhëzimit nr. 47.

   SMSI për mbrojtjen e të dhënave personale duhet të bazohet në standardin ISO/IEC 27001, siç parashikohet në nenin 5 të Udhëzimit nr. 48, datë 14.09.2018, të Komisionerit "*Për certifikimin e sistemeve të sigurisë së informacionit, të dhënave personale dhe mbrojtjes së tyre*" (në vijim, "*Udhëzimi nr. 48*"), si dhe është një sistem i certifikueshëm, për qëllime përputhshmërie me standardin e sipërpërmendur, vetëm nga organizma të akredituar dhe autorizuar sipas parashikimeve të Udhëzimit nr. 48.

Në përfundim të hetimit administrativ, referuar provave dhe konstatimeve në vend, grupi i hetimit administrativ hartoi procesverbalin përkatës dhe, në respektim të së drejtës për t'u dëgjuar, në zbatim të neneve 87-89 të Kodit të Procedurave Administrative, Kontrolluesi është ftuar të marrë pjesë në seancë dëgjimore, përpara marrjes së vendimit përfundimtar nga ana e Komisionerit.

Gjatë seancës dëgjimore, përfaqësuesi i Kontrolluesit paraqiti pretendimet me shkrim, si dhe dokumente ilustruese për rikuperimin e shkeljeve të konstatuara gjatë hetimit administrativ si më poshtë:

- Lidhur me konstatimin se ruajtja e numrit personal të identifikimit (ID) të pacientëve është në tejkalim të qëllimit të përpunimit për ofrimin e shërbimeve laboratorike, Kontrolluesi u shpreh se të dhënat e një pacienti pa numrin personal të identifikimit ID, janë të pamjaftueshme për identifikimin e personit, që duhet t'i jepen përgjigjet e analizave.

- Lidhur me konstatimin e mosinformimit të subjekteve të të dhënave, Kontrolluesi ka rikuperuar mënyrën e informimit të pacientëve, në lidhje me përpunimin e të dhënave të tyre personale, ruajtjen e konfidencialitetit, etj.

- Sa i përket konstatimit se Kontrolluesi nuk ka respektuar detyrimet ligjore të parashikuara në nenin 20 të Ligjit dhe Udhëzimit nr. 19, Kontrolluesi ka informuar se, ka përgatitur një draft kontratë të re sipas parashikimeve ligjore.

- Sa i përket konstatimit për përditësimin e rregullores së brendshme "*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*" Kontrolluesi ka rishikuar dhe përditësuar rregulloren e brendshme "*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*".

- Lidhur me ekzistencën e SMSI për mbrojtjen e të dhënave personale, Kontrolluesi ka parashikuar trajnime në vazhdim të personelit, në lidhje me legjislacionin në fuqi, mbi mbrojtjen e të dhënave personale. Ndërkohë është shprehur se duhet akoma kohë për të ngritur sistemin e menaxhimit të sigurisë së informacionit (SIMS), lidhur me mbrojtjen e të dhënave personale.

Zyra e Komisionerit vlerëson bashkëpunimin e Kontrolluesit me grupin e kontrollit administrativ dhe reagimin e tij për rikuperimin e shkeljeve të konstatuara. Plotësimi i këtyre detyrimeve nga ana e Kontrolluesit është mjaft i rëndësishëm, pasi garanton përpunimin e ligjshëm, sigurinë e të dhënave personale dhe ndalon mundësinë e përhapjes së tyre në mënyrë të paligjshme.

Sa më sipër, në zbatim të neneve 5, 6, 20, 27, 29, 30, 31 (pika 1, gërma "a/1"), si dhe 32 të Ligjit,

REKOMANDOJ:

1. Kontrolluesi të ketë në vëmendje të vazhdueshme përpunimin e të dhënave personale në përputhje me dispozitat e parashikuara ne nenin 5 dhe 6 të Ligjit;

2. Kontrolluesi, në zbatim të nenit 18 të Ligjit, të ketë në vëmendje përmbushjen në vazhdim të detyrimit për informimin e subjekteve të të dhënave personale, për qëllimin dhe mënyrën e përpunimit të të dhënave personale, kategoritë e të dhënave të përpunuara, të drejtat ligjore që gëzojnë, afatin e mbajtjes së të dhënave dhe masat e sigurisë;

3. Kontrolluesi të përfshijë në marrëveshjet me përpunuesit përkatës detyrimet sipas parashikimeve të nenit 20 të Ligjit dhe Udhëzimit nr.19;

4. Kontrolluesi, në zbatim të nenit 27 të Ligjit, të përditësojë rregulloren e brendshme në përputhje me veprimtarinë dhe proceset përpunuese që kryen;

5. Kontrolluesi, me qëllim garantimin e sigurisë së të dhënave personale, të zbatojë detyrimet e përcaktuara në Udhëzimin nr. 47, lidhur me trajnimin e stafit të tij, si dhe sa i përket krijimit, mirëmbajtjes dhe administrimit të Sistemit të Menaxhimit të Sigurisë së Informacionit (SMSI) për mbrojtjen e të dhënave personale.

SMSI për mbrojtjen e të dhënave personale duhet të krijohet në përputhje me standardin ISO/IEC 270001, siç parashikohet në nenin 5 të Udhëzimit nr. 48, si dhe mund të certifikohet, për qëllime përputhshmërie me standardin në fjalë, nga organizma të akredituar dhe autorizuar në përputhje me dispozitat e këtij udhëzimi. Në këtë rast, Kontrolluesi, në zbatim të germës "b" të pikës 42 të Udhëzimit nr. 47, depoziton pranë Zyrës së Komisionerit një kopje të certifikatës së përputhshmërisë;

6. Në zbatim të pikës 1, të nenit 32, të Ligjit, të përmbushen detyrimet sipas këtij akti brenda afateve si vijon:

   (i) Vazhdimisht, detyrimet e parashkuara në pikat 1 dhe 2 më sipër;

   (ii) brenda 15 (pesëmbëdhjetë) ditëve, detyrimet e treguara në pikat 3 dhe 4 më sipër; dhe

   (iii) brenda 60 (gjashtëdhjetë) ditëve, detyrimin e treguar në pikën 5.

   Afatet e sipërpërmendura fillojnë nga data marrjes dijeni të këtij akti.

7. Kontrolluesi të njoftojë Komisionerin për masat e marra.

   Në rast mospërmbushjeje, të detyrimeve të parashikuara në këtë akt, Komisioneri vepron sipas pikës 2 të nenit 30 dhe nenit 39 të Ligjit të cilët parashikojnë se në rast shkeljesh serioze, të përsëritura ose të qëllimshme të Ligjit nga një kontrollues ose përpunues, veçanërisht në rastet e përsëritura të moszbatimit të rekomandimeve të tij, Komisioneri vendos sanksione administrative për kundërvajtjet administrative përkatëse dhe e denoncon publikisht ose e raporton çështjen në Kuvend dhe në Këshillin e Ministrave.

Ky Rekomandim u shpall sot, më datë 11.11.2020

KOMISIONERI

Besnik Dervishi