REPUBLIKA E SHQIPËRISË

KOMISIONERI PËR TË DREJTËN E INFORMIMIT DHE MBROJTJEN E TË DHËNAVE PERSONALE
DREJTORIA E PËRGJITHSHME PËR MBROJTJEN E TË DHËNAVE PERSONALE
DREJTORIA E ANKESAVE DHE HARMONIZIMIT

Nr. 1523/6 prot. Tiranë më 26.10.2021

REKOMANDIM

Nr. 54, datë 26.10.2021

PËR KONTROLLUESIN "*SPITALI RAJONAL KUKËS*"

Në mbështetje të neneve 29, 30, 31 dhe 32 të ligjit nr. 9887, datë 10.03.2008 "*Për mbrojtjen e të dhënave personale*" i ndryshuar (në vijim, "*Ligji*"), neneve 77-112 të ligjit nr. 44/2015 "*Kodi i Procedurave Administrative të Republikës së Shqipërisë*" (në vijim, "*Kodi i Procedurave Administrative*"), si dhe provave të administruara në ngarkim të kontrolluesit *"Spitali Rajonal Kukës"* (në vijim, *"Kontrolluesi"*),

KONSTATOVA SE:

Në zbatim të Urdhrit 134 datë 15.09.2021 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim, "*Komisioneri*"), si dhe në mbështetje të Rezolutës së Kuvendit të Republikës së Shqipërisë, datë 03.06.2021 *"Për miratimin e veprimtarisë së Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, për vitin 2020"*, u krye hetim administrativ pranë Kontrolluesit, 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.

Komisioneri, pasi shqyrtoi relacionin e hetimit administrativ, procesverbalin e konstatimit dhe provat e administruara gjatë ushtrimit të hetimit pranë Kontrolluesit, vëren se:

1. Kontrolluesi ofron kujdesin mjekësor me anë të poliklinikës së specialiteteve, shërbimin e Pranim – Urgjencës, laboratorit klinik – biokimi dhe bakteriologjik dhe shërbimin me shtretër në specialitetet e veta.

2. Në kuadër të veprimtarisë që kryen, Kontrolluesi përpunon të dhëna personale për kategoritë, *"pacient"*, *"punonjës"* dhe *"vizitorë"*. Përpunimi i të dhënave kryhet në mënyrë manuale dhe elektronike. Për kategorinë pacient, të dhënat të cilat grumbullohen në kartelën e klinikës *"Gjeneralitetet e pacientit"* janë: *"adresa"*, *"numri i telefonit"*, *"emër"*, *"mbiemër"*, *"data e lindjes"*, *"gjinia"*, *"punësimi"*, *"sëmundje të mundshme"*. Përpunimi i të dhënave personale kryhet në mënyrë manuale dhe elektronike duke mos parashikuar asnjë afat kohor për ruajtjen e tyre, në kundërshtim me parimet e mbrojtjes së të dhënave personale, parashikuar në germën "*d*", të pikës 1, të nenit 5 të Ligjit.

   Zyra e Komisionerit vlerëson se Kontrolluesi ka detyrimin të përpunojë të dhënat personale për aq kohë sa ka të nevojshme për të arritur qëllimin duke mos tejkaluar atë dhe në momentin që qëllimi ka përfunduar lind detyrimi të realizojë shkatërrimin/fshirjen e tyre, në të kundërt përpunimi i mëtejshëm i të dhënave konsiderohet i paligjshëm.

3. Kontrolluesi ka lidhur kontrata me palë të treta: Kontratë Shërbimi me Operatorët BNT Electronics me objekt *"Mirëmbajtje e Përqendruar "Ful Risk" e Skanerit"*. Nga verifikimi i kontratave me palën e tretë, rezulton se nuk janë reflektuar detyrimet sipas parashikimeve në nenin 20, të Ligjit dhe Udhëzimit nr. 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"*).

   Zyra e Komisionerit vlerëson se në rastin e delegimit të përpunimit të të dhënave personale, Kontrolluesi duhet të sigurohet që përpunuesi të garantojë përpunim të ligjshëm dhe të sigurt të të dhënave. Detyrimet e përpunuesit për përpunimin e të dhënave personale, parashikohen në nenin 20 të Ligjit dhe rregullohen me aplikimin e Udhëzimit nr. 19.

4. Nga verifikimi i kryer në regjistrin elektronik të subjekteve kontrolluese, në protokollin e Zyrës së Komisionerit si dhe nga hetimi administrativ i ushtruar, rezulton se Kontrolluesi nuk ka përmbushur detyrimet që burojnë nga nenet 21 dhe 22 të Ligjit, mbi njoftimin për përpunimin e të dhënave personale për të cilat është përgjegjës.

   Zyra e Komisionerit vlerëson se realizimi i detyrimit për njoftim është i rëndësishëm, pasi i jep mundësinë subjekteve të të dhënave që të informohen mbi përpunimin që kryen kontrolluesi dhe realizimin e detyrimeve ligjore. Kjo i jep mundësi reale subjektit të të dhënave për të ushtruar në mënyrë korrekte të drejtat që i rezervojnë shprehimisht dispozitat e Ligjit.

5. Kontrolluesi nuk disponon rregullore *"Për mbrojtjen e të dhënave personale"*, në të cilën të parashikohen proceset, procedurat, masat teknike dhe organizative sipas parashikimeve të nenit 27 të Ligjit, me qëllim garantimin e përpunimit të ligjshëm

dhe sigurisë së të dhënave, në përputhje me proceset përpunuese të Spitalit. Kontrolluesi nuk ka marrë masa të përshtatshme sigurie, të cilat duhet të parashikojnë zhvillimet më të fundit teknologjike, natyrën sensitive të të dhënave që lidhen me shëndetin dhe vlerësimin e rrezikut të mundshëm, me qëllim parandalimin e rreziqeve të tilla si aksesi i paautorizuar tek të dhënat, shkatërrimi, humbja, përdorimi, pamundësia e aksesit të tyre, etj., në përputhje me parashikimet e nenit 27 të Ligjit, dhe pikës 4 të nenit 8 të Udhëzimin nr. 49 të Komisionerit, datë 02.03.2020 *"Për mbrojtjen e të dhënave shëndetësore"* (në vijim, *"Udhëzimi nr. 49"*).

Zyra e Komisionerit vlerëson se hartimi i një *"Rregulloreje specifike për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale"*, në të cilën të parashikohen rregulla dhe procedura organizative specifike mbi mënyrën e përpunimit të të dhënave personale (për çdo kategori subjektesh), sigurinë e të dhënave, konfidencialitetin, afatet e mbajtjes së të dhënave, etj., konsiderohet një detyrim shumë i rëndësishëm në zbatim të nenit 27 të Ligjit, pasi shmang pasojat e rënda që mund të vijnë për subjektet e të dhënave.

6. 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. Grupi i kontrollit konstaton mosplotësim të detyrimeve në lidhje 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 të Komisionerit, datë 14.09.2018 *"Për përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga subjektet përpunuese të mëdha"*, (në vijim, *"Udhëzimi nr.47")* për shkak cilësisë si subjekt përpunues i madh, si dhe për shkak të natyrës së veçantë të veprimtarisë që Kontrolluesi ushtron.

   Zyra e Komisionerit vlerëson se për shkak të cilësisë si subjekt i madh, si dhe për shkak të natyrës së veprimtarisë që ushtron (të dhënat mjekësore konsiderohen sensitive), e cila kërkon masa të shtuara teknike dhe organizative për garantimin e sigurisë së të dhënave personale, Kontrolluesi duhet të ndërmarrë masa konkrete 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, sipas parashikimit të nenit 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 organizata të akredituara dhe autorizuara sipas parashikimeve të Udhëzimit nr. 48.

Në përfundim të hetimit administrativ, referuar provave dhe konstatimeve në vend, grupi i hetimit administrativ hartoi procesverbalin përkatës, një kopje e të cilit i është

dërguar Kontrolluesit me rrugë postare. 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.

Përfaqësuesi i Kontrolluesit është paraqitur në seancë dëgjimore dhe nëpërmjet shkresës Nr. 933 Prot., datë 14.10.2021 paraqiti pretendimet si më poshtë.

- Lidhur me afatin e ruajtjes së të dhënave, bëjmë me dije se kartelat mbahen në sektorin e kostos deri në tre muaj nga dalja e të sëmurit nga spitali pastaj dërgohen në arshivë (kartotekë) ku dhe i nënshtrohen rregullave siç parashikohen në ligjin nr. 9154, datë 06.11.2003 "*Për arkivat*".

Zyra e Komisionerit vlerëson se në tërësi Kontrolluesi nuk ka përcaktuar rregulla të shkruara lidhur me afatin e përpunimit të të dhënave personale. Gjatë zhvillimit të aktivitetit të tij Kontrolluesi përpunon një sasi të madhe të dhënash personale, të stafit si dhe të pacientëve (kujtojmë që të dhënat shëndetësore konsiderohen sensitive sipas parashikimit të nenit 7 të Ligjit) dhe konsiderohet e nevojshme që mos tejkalohet afati që i duhet për ta përmbushur qëllimin e përpunimit, në respektim të parimeve të mbrojtjes së të dhënave personale, sanksionuar në germën "d" të pikës 1 të nenit 5 të Ligjit.

- Lidhur me kontratat e lidhura me palë të treta, bëjmë me dije se në kontratën e shërbimit nr. 17 Prot., datë 03.08.2012 me operatorin ekonomik "*BNT Electronics*" nuk flitet për delegim përpunimi të dhënash ose për akses të operatorit në kompjuterin e mjekut imazherist, për më tepër rezultatet imazherike të skanerit nuk regjistrohen në ndonjë sistem kompjuterik.

Zyra e Komisionerit vlerëson se, në kontratë është përcaktuar si objekt kryerja e shërbimit të mirëmbajtjes të skanerit, ndërsa në pikën 3 të nenit 6 të kontratës është përcaktuar se në vlerën e kontratës përfshihen të gjitha shërbimet e mirëmbajtjes si parandaluese, korrigjuese, kalibrimit, si dhe kontrolli i sigurisë teknike. Në kontratë nuk është përcaktuar asnjë dispozitë ku të trajtohet mbrojtja e të dhënave personale. Nga vlerësimi i përmbajtjes së kontratës kuptohet se "*BNT Electronics*" në rolin e përpunuesit mund të aksesojë të dhënat personale që ndodhen në pajisje dhe është detyrim i Kontrolluesit të sigurohet që përpunuesi ofron masa të përshtatshme mbrojtëse për të dhënat që do të përpunojë sipas detyrimeve që parashikohen në nenin 20 të Ligjit dhe rregullohen me aplikimin e Udhëzimit nr. 19.

- Lidhur me plotësimin e detyrimit për njoftim, bëjmë me dije se kemi plotësuar formularin dhe e kemi dërguar me shkresën nr. 849 Prot., datë 27.09.2021.

- Lidhur me masat e sigurisë, bëjmë me dije se në zbatim të ligjit nr. 10 107, datë 30.03.2009 "*Për Kujdesin Shëndetësor në Republikën e Shqipërisë*" është Ministria e Shëndetësisë institucioni që ngre dhe mban një sistem unik të informacionit shëndetësor. Të gjitha institucionet që mbledhin të dhëna shëndetësore, janë të detyruara

t'i ofrojnë Ministrisë së Shëndetësisë akses për këtë informacion, duke ruajtur fshehtësinë. Sistemi menaxhohet nga Ministria dhe ndryshimet në sistem bëhen nga IT i Ministrisë.

Zyra e Komisionerit vlerëson se në kuptim të Ligjit dhe parashikimeve të Udhëzimit nr. 47 Kontrolluesi, për shkak të cilësisë si subjekt i madh, si dhe për shkak të natyrës së veprimtarisë që ushtron (të dhënat mjekësore konsiderohen sensitive) konsiderohet kontrollues i madh dhe duhet të ndërmarrë masa konkrete të krijojë, mirëmbajë dhe administrojë SMSI, e cila kërkon masa të shtuara teknike dhe organizative për garantimin e sigurisë së të dhënave personale.

Zyra e Komisionerit vlerëson gatishmërinë dhe bashkëpunimin e Kontrolluesit me grupin e kontrollit, gjatë ushtrimit të hetimit administrativ, si dhe angazhimin serioz të tij për të rikuperuar shkeljet e konstatuara. Plotësimi i këtyre detyrimeve nga ana e Kontrolluesit është mjaft i rëndësishëm pasi garanton përpunimin e ligjshëm, sigurinë e të dhënave personale dhe eviton mundësinë e përhapjes së tyre në mënyrë të paligjshme.

PËR KËTO ARSYE:

Në zbatim të neneve 5, 20, 21, 27, 29, 30, 31 (pika 1, germa "*a/1*"), si dhe 32 të Ligjit,

REKOMANDOJ:

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

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

3. Kontrolluesi në zbatim të neneve 21 dhe 22 të Ligjit, të ketë në vëmendje përditësimin e *"Njoftimit"*, në lidhje me ndryshimin e gjendjes së përpunimit të të dhënave personale për të cilat është përgjegjës;

4. Kontrolluesi në zbatim të nenit 27 të Ligjit, të hartojë një rregullore të posaçme, në të cilën të parashikohen masa teknike dhe organizative për mbrojtjen e të dhënave personale, 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 krijimin, mirëmbajtjen dhe administrimit të Sistemit të Menaxhimit të Sigurisë së Informacionit (SMSI) për mbrojtjen e të dhënave personale;

6. Kontrolluesi, për shkak të natyrës së veçantë të aktivitetit që ushtron, duhet të marrë masat e nevojshme për të vlerësuar mbi certifikimin e sistemeve të menaxhimit të

sigurisë së informacionit, të të dhënave personale dhe mbrojtjes së tyre, sipas parashikimeve të Udhëzimit nr. 48;

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

   - brenda 30 (tridhjetë) ditëve, detyrimin e treguar në pikat 1, 2 dhe 4 më sipër;
   - brenda 45 (dyzetë e pesë) ditëve, detyrimin e treguar në pikën 5 më sipër.

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

8. Kontrolluesi të njoftojë Komisionerin për masat e marra.

Në rast mospërmbushje 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 26.10.2021.

KOMISIONERI

Besnik Dervishi