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.1520/5 prot. Tiranë më 26.10.2021

REKOMANDIM

Nr. 52, datë 26.10.2021

PËR KONTROLLUESIN *"KLINIKA STOMATOLOGJIKE UNIVERSITARE"*

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 *"Klinikës Stomatologjike Universitare"* (në vijim, *"Kontrolluesi"*),

KONSTATOVA SE:

Në zbatim të Urdhrit 131 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 shërbim mjekësor të specializuar në fushën e Stomatologjisë, ndjekje dhe trajtim të pacienteve në sektorët Kirurgji, Terapi dhe Ortopedi. Gjithashtu ofron edukim universitar dhe pasuniversitar duke shërbyer si bazë

mësimdhënie për Fakultetin e Stomatologjisë, formimin e profilizuar pasuniversitar, edukimin e vazhdueshëm mjekësor stomatologjik dhe shërben si qendër kërkimore shkencore mbi bazën e praktikës mjekësore dhe përvojës së akumuluar.

2. Në kuadër të veprimtarisë që kryen, Kontrolluesi përpunon të dhëna personale për kategoritë *"pacient"*, *"student"* dhe *"punonjës"*. 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"* dhe *"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 nuk ka publikuar "*Politikat e Privatësisë*" në faqen zyrtare https://.ksu.al. Subjektet e të dhënave personale nuk informohen mbi qëllimin dhe mënyrën e përpunimit të të dhënave personale, personin që do t'i përpunojë të dhënat, të drejtat ligjore që gëzojnë, afatin e mbajtjes së të dhënave, dhe masat e sigurisë, në kundërshtim me parashikimet e nenit 18 të Ligjit dhe Udhëzimit nr. 49 të Komisionerit, datë 02.03.2020 "*Për mbrojtjen e të dhënave shëndetësore*" (në vijim, *"Udhëzimi nr. 49*").

   Zyra e Komisionerit vlerëson se çdo kontrollues që përpunon të dhëna personale, pavarësisht faktit nëse përpunimi bëhet në mënyrë elektronike apo manuale, dhe pavarësisht faktit nëse mbledh apo jo të dhëna personale nëpërmjet faqes zyrtare, ka detyrimin që të publikojë *"politikën e privatësisë"*, pasi kontakti paraprak i çdo subjekti të dhënash me kontrolluesin realizohet nëpërmjet faqes online të internetit.

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 përpunimin, ruajtjen dhe sigurinë 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 Klinikës.

   Kontrolluesi nuk ka ndërmarrë masa konkrete dhe efektive sigurie për të parashikuar 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.

   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 aplikon "*Deklaratë Konfidencialiteti*" me punëmarrësit të cilët kanë akses në mbledhjen, përpunimin dhe ruajtjen e të dhënave personale, në kundërshtim me parashikimet e nenit 28 të Ligjit. Gjithashtu, në kontratat individuale të punës nuk parashikohen dispozita për ruajtjen e konfidencialitetit dhe besueshmërisë.

   Zyra e Komisionerit vlerëson se qëllimi i nënshkrimit të *"Deklaratës së Konfidencialitetit"*, është që të gjithë punonjësit të cilët kanë akses në të dhënat personale, të kuptojnë qartë dhe drejtë detyrimet që ata kanë mbi përpunimin e të dhënave personale dhe ruajtjen e konfidencialitetit. Në aktin formal me titull *"Deklaratë Konfidencialiteti"*, dalë në zbatim të Vendimit nr. 6 të Komisionerit, datë 05.08.2013 "*Për përcaktimin e rregullave të hollësishme për sigurinë e të dhënave personale*" punëmarrësit informohen mbi përgjegjësitë në rast përhapje në mënyrë abuzive të të dhënave personale tek personat e paautorizuar.

7. 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. Konstatohet mosplotësim i detyrimeve për sa i takon ngritjes, administrimit dhe mirëmbajtjes së sistemit të menaxhimit së sigurisë së informacionit (SMSI), lidhur me mbrojtjen e të dhënave personale, të parashikuara në Udhëzimin 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 të 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, i cili u nënshkrua nga përfaqësuesit e Kontrolluesit. 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. Nëpërmjet shkresës nr. 95/2 Prot., datë 13.10.2021 ka pranuar shkeljet e konstatuara si dhe ka deklaruar angazhimin për rikuperimin e shkeljeve të konstatuara gjatë hetimit administrativ ushtruar.

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, 18, 21, 27, 28, 29, 30, 31 (pika 1, germa *"a/I"*), 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 dhe të

Udhëzimit nr. 49, si dhe të marrë masa për adresimin e konstatimeve të Komisionerit sa i takon përcaktimit të afateve për ruajtjen e të dhënave personale.

2. Kontrolluesi në zbatim të nenit 18 të Ligjit, të ndërmarrë hapa konkrete për informimin specifik të subjekteve të të dhënave 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 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 në zbatim të nenit 28 të Ligjit, të marrë masat e nevojshme të sigurisë dhe konfidencialitetit me qëllim shmangien e aksesit dhe përhapjes së të dhënave nga persona ose subjekte të paautorizuar;

6. 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;

7. 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;

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

   (i) brenda 30 (tridhjetë) ditëve, detyrimin e treguar në pikat 1, 2 dhe 4 më sipër;

   (ii) në mënyrë të vazhdueshme, detyrimet e treguara në pikën 3 dhe 5 më sipër;

   (iii) brenda 45 (dyzetë e pesë) ditëve, detyrimin e treguar në pikën 6 më sipër.

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

9. 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