



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. 1609 / prot.  
15

Tiranë më 20.10.2021

REKOMANDIM

Nr. 56, datë 18.10.2021

PËR KONTROLLUESIN “KLINIKA EGIAN”

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 “KLINIKA EGIAN” (në vijim, “Kontrolluesi”),

KONSTATOVA SE:

Në zbatim të Urdhrit 140 datë 01.10.2021 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 shërbime në fushën e shëndetësisë, në shërbim të shëndetit të qytetarëve, të cilëve u siguron shërbim shëndetësor parandalues, diagnostikues dhe kurues sipas legjislacionit në fuqi. Kontrolluesi përpunon të dhëna personale

për kategorinë e subjekteve të të dhënave, “pacientë”, “punonjës”, “furnizues”. Përpunimi i të dhënave kryhet në mënyrë manuale dhe elektronike.

2. Për kategorinë pacient, të dhënat të cilat grumbullohen në kartelën e klinikës “Kartele personale” janë: “emër”, “atësi” “mbiemër”, “data e lindjes”, “numri personal i identifikimit”, “numri i sigurimit shëndetësor”, “qendra e punës”, “profesioni”, “adresa”, “data e hapjes së kartelës”, “numri i telefonit”, “sëmundje të mundshme”, “grupi i gjakut”, “rezusi”.

Gjithashtu, Kontrolluesi përpunon të dhëna elektronikisht, nëpërmjet sistemit “SOFT EXPRESS”. Të dhënat e grumbulluara janë: “tipi i klientit”, “kodi”, “emër”, “atësi” “mbiemër”, “data e lindjes”, “numri personal i identifikimit”, “shteti”, “qendra e punës”, “profesioni”, “adresa”, “numri i telefonit”.

Kontrolluesi nuk ka parashikuar asnjë afat për kohën e ruajtjes së të dhënave personale në kundërshtim me parimin e mbrojtjes së të dhënave personale, parashikuar në germën “d”, të pikës 1, të nenit 5 të ligjit nr. 9887, datë 10.03.2008 “Për mbrojtjen e të dhënave personale” i ndryshuar (në vijim “Ligji”).

Zyra e Komisionerit vlerëson se, Kontrolluesi ka detyrimin të përpunojë të dhënat personale për aq kohë sa e 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 informon subjektet e të dhënave “pacientë”, mbi qëllimin dhe mënyrat e përpunimit të të dhënave personale dhe sensitive, 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 Udhëzimin nr. 49 të Komisionerit, datë 02.03.2020 “Për mbrojtjen e të dhënave shëndetësore” (në vijim, “Udhëzimi nr. 49”).

Kontrolluesi disponon një sistem video-survejimi (CCTV) për mbikëqyrjen e ambienteve të brendshme si dhe ka vendosur tabela njoftuese mbi prezencën e sistemit të video-survejimit CCTV. Tabela informuese nuk paraqet elementët informues sipas parashikimeve të nenit 18 të Ligjit dhe modelit standard të miratuar me Udhëzimin nr. 3 datë 05.03.2010 të Komisionerit, “Mbi përpunimin e të dhënave personale me sistemin e video-survejimit në ndërtesa dhe mjedise të tjera” i ndryshuar (në vijim, “Udhëzimi nr. 3”).

Zyra e Komisionerit vlerëson se, informimi i subjekteve të të dhënave personale është një ndër detyrimet bazë të Kontrolluesit, pasi i mundëson atyre njohjen me të drejtat që u njeh Ligji, si dhe ushtrimin e këtyre të drejtave në praktikë. Mos përmbushja e këtij detyrimi, nga ana e Kontrolluesit, mund të sjellë pasoja të rënda sa i përket jetës private dhe bashkë me të, të drejtës së subjekteve të të dhënave për mbrojtjen e tyre.

4. Kontrolluesi ka lidhur kontratë bashkëpunimi me shoqërinë “*Intermedica Center SHPK*” me nr. 266 Prot., datë 01.12.2020, me objekt “...*lindja dhe lidhja e marrëdhënies së bashkëpunimit ndërmjet palëve në zbatim të legjislacionit në fuqi, ku Intermedica Center SHPK merr përsipër kryerjen e ekzaminimeve laboratorike klinike, biokimike, hormonale, bakteriologjike, citologjike, parazitologjie, etj*”. Konstatohet se, në kontratë nuk parashikohen detyrimet e palëve mbi përpunimin e të dhënave personale dhe sensitive, në kundërshtim me parashikimet e nenit 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 delegimit*”, 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.

5. 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 detyrimin për njoftim mbi përpunimin e të dhënave personale për të cilat është përgjegjëse, në kundërshtim me parashikimet e neneve 21 dhe 22 të Ligjit.

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.

6. Kontrolluesi nuk ka hartuar “*Rregullore 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 subjekti të dhënash), sigurinë e të dhënave, afatet e mbajtjes së të dhënave, masat teknike etj, në kundërshtim me nenin 27 të Ligjit.

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 aksesit 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 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, 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 subjektësh), 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 shpall pasojat e rënda që mund të vijnë për subjektet e të dhënave.

7. Kontrolluesi nuk ka ndërmarrë masa konkrete në kuadër të trajnimit të punonjësve që kanë akses dhe përpunojnë të dhëna personale lidhur me legjislacionin shqiptar në fuqi, për mbrojtjen e të dhënave personale. Grupi i inspektimit konstatoi mosplotësim të 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 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 të datës 19.10.2021 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 e 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, 20, 21, 27, 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 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 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;
5. 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;
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 administrimin 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:

- Brenda 30 (tridhjetë) ditëve, detyrimin e treguar në pikat 1, 2 , 3 dhe 5 më sipër;
- në mënyrë të vazhdueshme, detyrimin e treguar në pikën 4 më sipër;
- 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, Komisionerit 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 28.10.2021.

**KOMISIONERI**

**Besnik Dervishi**

