



**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 HETIMIT SEKTORIAL DHE SIGURISË SË TË DHËNAVE

Nr.167 prot.

Tiranë më 17.01.2023

**VENDIM**

**Nr. 01, datë 17.01.2023**

**PËR KONTROLLUESIN “TORONTO GROUP” 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”), neneve 77-112 të 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 “Toronto Group – Spitali Jopublik Amavita” (në vijim, “Kontrolluesi”),

**KONSTATOVA SE:**

Në zbatim të Urdhrit nr.156, datë 26.09.2022 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim, “Komisioneri”), u krye hetimi administrativ pranë Kontrolluesit, me objekt:

- Verifikimi i zbatimit të detyrimeve sipas Rekomandimit nr. 38, datë 29.07.2021 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale për kontrolluesin “Toronto Group” SHPK.

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

1. Gjatë zhvillimit të veprimtarisë së tij, Kontrolluesi përpunon të dhëna personale për kategoritë e subjekteve të të dhënave “punëmarrës”, “pacientë”, “klientë” dhe “furnizues”. Përpunimi i të dhënave kryhet në mënyrë manuale dhe elektronike.

Kontrolluesi nuk ka publikuar “politikat e privatësisë” në faqen online [www.spitaliamavita.al](http://www.spitaliamavita.al), në kundërshtim me parashikimet e nenit 18 të Ligjit, dhe në përmbushje të pikës 2 të Rekomandimit.

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, datë 02.03.2020 të Komisionerit “Për mbrojtjen e të dhënave shëndetësore” (në vijim, “Udhëzimi nr. 49”).

Informimi i subjekteve të të dhënave personale është një nga detyrimet bazë të Kontrolluesit pasi u jep mundësinë subjekteve të të dhënave personale të njihen me të drejtat që gëzojnë dhe mundësinë e ushtrimit të tyre në praktikë. Mos përbushja e këtij detyrimi nga ana e Kontrolluesit mund të sjellë pasoja të rënda sa i përket privatësisë dhe përpunimit të të dhënave personale të subjekteve të të dhënave, dhe konsiderohet mos përbushje e detyrimit për informim, të sanksionuar në nenin 18 të Ligjit. Në këtë kuadër, publikimi i rubrikës “politikat e privatësisë” në faqen online të Kontrolluesit përbush më së miri qëllimin e informimit përkundrejt subjekteve të të dhënave, të cilët aksesojnë dhe ngarkojnë të dhëna personale në faqe.

## 2. Kontrolluesi ka lidhur kontrata bashkëpunimi me palë të treta, konkretisht:

- ✓ Kontrata e datës 01.01.2021, mes palëve, “Spitali Amavita- Toronto Group” SHPK dhe “Swiss Medical Center” SHPK;
- ✓ Kontrata e datës 16.06.2020 dhe nr.156 prot., midis “Shoqëria Toronto Group” SHPK dhe “Intermedica Center” SHPK;
- ✓ Kontrata mes palëve “Spitali Amavita- Toronto Group” SHPK dhe “JETO IVD” SHPK (mbi menaxhimin e CCTV) e cila është lidhur, në 23.11.2022, dy muaj, pas njohjes nga ana e Kontrolluesit me Urdhrin nr. 156, datë 26.09.2022, të Komisionerit.

Në këto kontrata nuk janë përfshirë detyrimet sipas parashikimeve të 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 delegimi”, i ndryshuar (në vijim, “Udhëzimi nr. 19”).

Zyra e Komisionerit vlerëson se, në rastet e delegimit të përpunimit të të dhënave Kontrolluesi duhet të miratoj një kontratë, që palët duhet të përdorin në rast të këtij delegimi, me anë të së cilës të garantojë përcaktimin e rregullave në marrëdhënien e tij me përpunuesin, me qëllim që delegimi i përpunimit të këtyre të dhënave të përpunuesit të jetë në përputhje me legjislacionin në fuqi.

Në rastet e delegimit të përpunimit të të dhënave dhe/ose shërbimit, Kontrolluesi duhet të sigurohet që përpunuesi të garantojë përpunim të ligjshëm dhe të sigurt të të dhënave.

3. Kontrolluesi nuk ka marrë masa në lidhje me përditësimin e “Njoftimit” pranë Zyrës së Komisionerit, mbi përpunimin e të dhënave për të cilat është përgjegjës, në zbatim të neneve 21 dhe 22 të Ligjit, dhe në përmbushje të pikës 3 të Rekomandimit.

Zyra e Komisionerit vlerëson se realizimi i përditësimit për ndryshimin e gjendjes së Njoftimit të përpunimit të të dhënave është i rëndësishëm pasi i jep mundësinë subjekteve të të dhënave 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 jep Ligji.

4. Kontrolluesi disponon Rregullore “Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale”, në përmbushje të pikës 4 të Rekomandimit, por konstatohet se Rregullorja nuk parashikon 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 Kontrolluesit.

Zyra e Komisionerit vlerëson se, hartimi i një Rregullore specifike “Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale”, në të cilën të parashikohen rregulla dhe procedura teknike-organizative mbi mënyrën e përpunimit të të dhënave personale (për çdo kategori subjektësh), sigurinë e të dhënave, konfidencialitetin, afatet e mbajtjes së të dhënave, nivelet e aksesit 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.

5. Kontrolluesi nuk ka marrë 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 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”) për shkak të cilësisë si subjekt përpunues i madh, si dhe për shkak të natyrës së veçantë të veprimtarisë (sensitive) që Kontrolluesi ushtron dhe në përmbushje të pikës 5 të “Rekomandimit”.

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 nenit 27 të Ligjit dhe Udhëzimit nr. 47.

Në përfundim të hetimit administrativ, referuar provave dhe konstatimeve në vend, grupi i inspektimit hartoi procesverbalin përkatës i cili u refuzua të nënshkruhet nga Kontrolluesi.

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 ligjor i Kontrolluesit, është paraqitur në seancën dëgjimore, datë 14.12.2022, të organizuar nga Zyra e Komisionerit dhe ka paraqitur pretendimet e tij me shkrim si më poshtë:

1. Në lidhje me konstatimin se, në faqen online [www.spitaliamavita.al](http://www.spitaliamavita.al) nuk janë të pasqyruara "politikat e privatësisë", ju bëjmë me dije se Kontrolluesi ka përgatitur materialin e politikave të privatësisë që do të vendoset tek faqja e web-it, por për shkak se ka përfunduar hosti i faqes e ka patur të pamundur për ta publikuar.

Zyra e Komisionerit, vlerëson se Kontrolluesi ka patur në dispozicion një afat kohor prej 12 muajsh, për të reflektuar, dhe zbatuar detyrimet e Rekomandimit.

2. Sa i përket konstatimit për përditësimin për ndryshimin e gjendjes së Njoftimit rezulton se ky detyrim është përmbushur.

Zyra e Komisionerit vlerëson se pretendimet e Kontrolluesit nuk qëndrojnë pasi Kontrolluesi nuk ka kryer përditësimin përkatës për ndryshimin e gjendjes së njoftimit të përpunimit të të dhënave, sa i përket:

- ✓ Deklarimit në rubrikën 7, "marrësi i të dhënave personale", Kontrolluesi nuk ka deklaruar subjekte të treta tek të cilët përhap të dhëna.

3. Sa i përket konstatimit se, Kontrolluesi në kontratat e bashkëpunimit që ka realizuar me palë të treta, nuk ka përfshirë detyrimet e nenit 20 të Ligjit dhe Udhëzimit nr. 19, Kontrolluesi argumenton se: "Ekziston marrëveshja e konfidencialitetit midis "Spitalit Amavita- Toronto Group" SHPK dhe "Swiss Medical Center" SHPK, por ky dokument nuk i ishte bashkëngjitur kontratës gjatë hetimit administrativ. Kjo marrëveshje konfidencialiteti e lidhur me shoqërinë ekziston që prej datës 01.01.2021. Gjithashtu midis Kontrolluesit dhe JETO IVD SHPK është lidhur një aneks kontrate në të cilën janë shtuar detyrimet e palëve sipas nenit 20 të Ligjit dhe Udhëzimit nr.19 të Komisionerit".

Zyra e Komisionerit konstaton se, Kontrolluesi si gjatë hetimit administrativ dhe gjatë seancës dëgjimore nuk paraqiti asnjë provë për të vërtetuar pretendimet e tij.

4. Në lidhje me rregulloren "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale", sqarojmë se në kreun 5 të kësaj Rregulloreje janë parashikuar masat teknike-organizative për mbrojtjen e të dhënave personale. Gjithashtu janë ndërrmarë masat konkrete për trajnimin e punonjësve që kanë akses dhe përpunojnë të dhëna personale. Është caktuar një person që merret me përpunimin e të dhënave personale dhe mirëmbajtjen e sistemit të menaxhimit, ku është përpiluar dhe një aneks

*kontrate, ku parashikohet administrimi dhe mirëmbajtja e sistemit të menaxhimit (neni 9).*

Zyra e Komisionerit vlerëson se pretendimet e Kontrolluesit nuk qëndrojnë pasi “Rregullorja për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale” është pothuajse identike me rregulloren tip që gjendet në faqen zyrtare të Zyrës së Komisionerit, dhe jo një rregullore specifike “Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale”, në të cilën të parashikohen rregulla dhe procedura teknike-organizative mbi mënyrën e përpunimit të të dhënave personale (për çdo kategori subjektësh), sigurinë e të dhënave, konfidencialitetin, afatet e mbajtjes së të dhënave, nivelet e aksesit etj., në zbatim të nenit 27 të Ligjit, pasi shmang pasojat e rënda që mund të vijnë për subjektet e të dhënave.

Ndërsa sa i takon pretendimeve të Kontrolluesit se ka marrë masa për mirëmbajtjen e sistemit të menaxhimit së sigurisë së informacionit, Zyra e Komisionerit, vlerëson se dokumentacioni i vendosur në dispozicion nga Kontrolluesi (*Rregullore për masa për trajnimin, administrimin, mirëmbajtjen e sistemit të sigurisë së informacionit (SMSI) në Spitalin Amavita për punonjësit që kanë akses dhe përpunojnë të dhëna personale*) nuk dokumenton faktin se është plotësuar detyrimi në lidhje me ngritjen, administrimin dhe mirëmbajtjen e sistemit të menaxhimit së sigurisë së informacionit (SMSI). Konkretisht, referuar pikës 11 të Udhëzimit nr. 47 të Komisionerit, SMSI për mbrojtjen e të dhënave personale duhet të përmbajë:

- 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.*

Sa më sipër, Zyra e Komisionerit vlerëson se masat e ndërmarra nga Kontrolluesi janë të pamjaftueshme në raport më veprimtarinë që kryen. Zbatueshmëria dhe dokumentimi i procedurave dhe politikave në lidhje më sigurinë e informacionit, është një ndër masat kryesore që duhet të ndërmarrë Kontrolluesi, në lidhje me sigurinë dhe funksionimin e sistemeve të teknologjisë së informacionit, në zbatim të detyrimeve të parashikuara në Udhëzimin nr. 47.

Në përfundim, shkeljet e konstatuara gjatë ushtrimit të hetimit administrativ, në kuptim të germave “b”, “ç”, “d” e “dh” të pikës 1 të nenit 39 të Ligjit, përbëjnë kundërvajtje administrative dhe sanksionohen me gjobë, si më poshtë:

*b) kontrolluesit, që nuk përmbushin detyrimin për të informuar, të përcaktuar në nenin 18 të këtij ligji, dënohen me 10 000 deri në 300 000 lekë;*

*ç) kontrolluesit ose përpunuesit që nuk përmbushin detyrimet e përcaktuara në nenin 20 të këtij ligji, dënohen me 10 000 deri në 300 000 lekë;*

*d) kontrolluesit, që nuk përmbushin detyrimin për të njoftuar, sipas përcaktimit në nenin 21 të këtij ligji, dënohen me 10 000 deri në 500 000 lekë;*

*dh) kontrolluesit ose përpunuesit, që nuk marrin masat e sigurisë së të dhënave dhe nuk zbatojnë detyrimin për ruajtjen e konfidencialitetit, të përcaktuara përkatësisht në nenet 27 dhe 28 të këtij ligji, dënohen me nga 10 000 deri në 150 000 lekë;*

Në bazë të pikës 2 të nenit 39 të Ligjit, personat juridikë, për kundërvajtjet e mësipërme administrative, dënohen me dyfishin e gjobës së përcaktuar në pikën 1 të këtij neni.

Për zgjedhjen e masës së gjobës, Zyra e Komisionerit ka parasysh faktin e mos përmbushjes së detyrimeve të lëna në Rekomandim, të cilat lidhen me mungesën e përpunimit të ligjshëm të të dhënave, garantimin e të drejtave të subjekteve të të dhënave, marrjes së masave të përshtatshme teknike dhe organizative për sigurinë e të dhënave.

### **PËR KËTO ARSYE:**

Sa më sipër, në zbatim të neneve 18, 20, 21, 22, 27, 29, 30, 39 (pika 1, gërmat “b”, “ç”, “d” dhe “dh”), si dhe nenet 40 dhe 41 të Ligjit,

### **V E N D O S A:**

1. Dënimin e Kontrolluesit me gjobë në vlerën 150 000 (njëqind e pesëdhjetë mijë) Lekë, për shkelje të detyrimit të përcaktuar në nenin 18 të Ligjit;
2. Dënimin e Kontrolluesit me gjobë në vlerën 150 000 (njëqind e pesëdhjetë mijë) Lekë, për shkelje të detyrimit të përcaktuar në nenin 20 të Ligjit;
3. Dënimin e Kontrolluesit, me gjobë në vlerën 100 000 (njëqind mijë) Lekë, për shkelje të detyrimit të përcaktuar në nenin 27 të Ligjit;
4. Kontrolluesi, të marrë masat për të rishikuar marrëveshjet e bashkëpunimit me përpunuesit duke specifikuar detyrimet midis palëve, dhe të monitorojë në vijimësi zbatimin e detyrimeve të përcaktuara në marrëveshjet me përpunuesit, sipas dispozitave të parashikuara në nenin 20 të Ligjit dhe Udhëzimin nr. 19 të Komisionerit;
5. Kontrolluesi, në zbatim të neneve 21 dhe 22 të Ligjit, të kryejë përditësimin e “Njoftimit”, në lidhje me ndryshimin e gjendjes së përpunimit të të dhënave personale për të cilat është përgjegjës;

6. Kontrolluesi, në zbatim të nenit 27 të Ligjit, të marrë masa për hartimin e Rregullores “Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale”, duke parashikuar masa konkrete teknike dhe organizative për mbrojtjen e të dhënave personale, për çdo kategori të dhënash dhe për çdo proces përpunimi, mënyrat e përpunimit të të dhënave, të drejtat e subjekteve të të dhënave, etj;
7. 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;
8. Në zbatim të pikës 1 të nenit 32 të Ligjit, të përmbushen detyrimet sipas këtij akti brenda afateve si vijon:
  - (i) brenda 15 (pesëmbëdhjetë) ditëve, detyrimet e parashikuara në pikat 4 dhe 5 më sipër;
  - (ii) brenda 30 (tridhjetë) ditëve, detyrimet e parashikuara në pikën 6 më sipër;
  - (iii) brenda 45 (dyzetë e pesë) ditëve, detyrimet e përcaktuara në pikën 7 më sipër.Afatet e sipërpërmendura fillojnë nga data e marrjes dijeni të këtij akti.
9. Kontrolluesi të njoftojë Zyrën e Komisionerit për masat e marra.
10. Gjoha arkëtohet nga kundërvajtësi në Buxhetin e Shtetit, jo më vonë se 30 (tridhjetë) ditë nga komunikimi i këtij Vendimi. Me kalimin e këtij afati, ky Vendim kthehet në titull ekzekutiv dhe ekzekutohet në mënyrë të detyrueshme nga Zyra e Përmbarimit.
11. Kundër këtij Vendimi mund të bëhet ankim në Gjykatën Administrative të Shkallës së Parë Tiranë, brenda 30 (tridhjetë) ditëve nga komunikimi i këtij Vendimi.

Ky Vendim u shpall sot më datë 17.01.2023.

**KOMISIONERI**

**Besnik Dervishi**