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

Nr. 37 Prot. Tiranë më 7.1.2021

REKOMANDIM

Nr. 01, datë 7.1.2021

PËR KONTROLLUESIN "SALUS TIRANA" SHA

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 "*Salus Tirana*" SHA (në vijim, "*Kontrolluesi*"),

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 152 datë 06.10.2020 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim, "*Komisioneri*"), 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 "*Salus Tirana*" SHA.

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

1. Kontrolluesi ka për objekt të aktivitetit ofrimin e shërbimeve shëndetësore dhe spitalore. Kontrolluesi përpunon të dhëna personale dhe sensitive për kategoritë e subjekteve të të dhënave "*punëmarrës*", "*punonjës të larguar*", "*kandidatë për punë*", "*pacientë*" dhe "*vizitorë*". Të dhënat personale përpunohen në kuadër të marrëdhënies së punës, ofrimit të shërbimeve shëndetësore, në kuadër të monitorimit të ambienteve dhe hyrje-daljeve për qëllime sigurie. Të dhënat personale përpunohen manualisht, si dhe nëpërmjet instrumenteve elektronike.

2. Kontrolluesi nuk ka parashikuar afate për ruajtjen e të dhënave personale/sensitive të pacientëve, që përpunohen manualisht dhe elektronikisht, në kundërshtim me germën "d" të pikës 1 të nenit 5 të Ligjit dhe nenit 5 të Udhëzimit nr. 49, datë 02.03.2020 "*Për mbrojtjen e të dhënave personale shëndetësore*" (në vijim, "*Udhëzimi nr. 49*").

   Sa i përket arkivës, u konstatua se në "*Rregulloren e brendshme për ruajtjen dhe menaxhimin e dokumentacionit të spitalit*" parashikohet vetëm një afat ruajtje i përgjithshëm, "*jo më pak se 10 vjet*", por nuk përcaktohet një afat maksimal ruajtje.

   Zyra e Komisionerit, duke patur parasysh që arkiva përmban disa lloje dokumentesh, vlerëson se është e nevojshme që të parashikohen afate specifike ruajtje në përputhje me qëllimin e përpunimit në lidhje me të dhënat personale.

   Gjithashtu, Zyra e Komisionerit vlerëson se kontrolluesi ka detyrimin të përpunojë të dhënat personale dhe sensitive për aq kohë sa ekziston qëllimi për të cilin janë grumbulluar dhe përpunuar më tej. Në momentin që qëllimi ka përfunduar është e nevojshme që Kontrolluesi, vetë ose nëpërmjet delegimit të një pale të tretë në cilësinë e përpunuesit, të realizojë shkatërrimin e tyre, në të kundërt përpunimi i mëtejshëm i të dhënave konsiderohet i paligjshëm.

3. Nga analizimi i formatit informues "*Shënim Informues për trajtimin e të dhënave personale*", rezulton se subjektet e të dhënave nuk informohen mbi mënyrën e përpunimit të të dhënave personale/sensitive (përpunimin manual ose elektronik, masat e marra në kuadër të sigurisë, afatet e ruajtjes, etj.) dhe elementet e tjera informuese, në kundërshtim me parashikimet në nenin 18 të Ligjit dhe Udhëzimin nr. 49.

   Në formatin e informimit parashikohet edhe informimi lidhur me mundësinë e transferimit të të dhënave personale/sensitive. Nënshkrimi i këtij formati nga subjektet e të dhënave nuk nënkupton dhënien e pëlqimit lidhur me transferimin ndërkombëtar të të dhënave.
   Subjektet e të dhënave nuk janë informuar në lidhje me marrësit e të dhënave personale në rastet e përhapjes dhe transferimit të të dhënave.

   "Politika e Privatësisë" në faqen e internetit nuk parashikon elementet e nevojshme për informim, në zbatim të nenit 18 të Ligjit.

   Referuar standarteve lidhur me njoftimet e punësimit, rezulton se "*kandidatët për punë*" nuk informohen në mënyrë të plotë, në zbatim të nenit 18 të Ligjit.

   Zyra e Komisionerit vlerëson se informimi i subjekteve të të dhënave personale dhe sensitive është një nga detyrimet bazë të Kontrolluesit, pasi iu mundëson atyre të njihen me të drejtat që iu janë akorduar me Ligj, si dhe iu mundëson, gjithashtu, ushtrimin e këtyre të drejtave në praktikë. Mospërmbushja 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 të dhënave të tyre personale.

4. Kontrolluesi ka lidhur kontrata me palë të treta, nëpërmjet të cilave është kryer edhe delegimi (*outsource*) i përpunimit të të dhënave personale. Nga analizimi i kontratave në fjalë, rezultojnë shkelje të dispozitave të nenit 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*").

   Kontrolluesi rezulton të ketë deleguar disa shërbime, konkretisht:

   a. **Shërbimi i kryerjes së ekzaminimeve laboratorike klinike, biokimike, hormonale, bakterologjike, citologjike, parazitologjike, etj., tek shoqëria "Intermedica-Center" Shpk.**

      Referuar përmbajtjes së kontratës dhe në mënyrë specifike nenit 7 të saj ("*Konfidencialiteti*"), rezulton se nuk janë parashikuar të gjithë elementet e nevojshëm sipas nenit 20 të Ligjit, duke veçuar garantimin e të drejtave të subjekteve të të dhënave personale, sipas gërmë "c", si dhe detyrimet e tjera sipas germave "ç" dhe "d" të pikës 1 të këtij neni. Kontrata nuk përmban elementet, detyrimet dhe garancitë që duhet të ofrojnë palët sipas parashikimeve të Udhëzimit 19 (kontratës tip të parashikuar në Aneksin 1 të saj).

      Në kontratë nuk janë parashikuar dhe kategoritë e të dhënave personale/sensitive që përhapen nga kontrolluesi drejt përpunuesit "Intermedica Center" Shpk.

   b. **Shërbimi i administrimit dhe mirëmbajtjes së *Software MEDarchiver*, deleguar te shoqëria "MEDArchiver" Srl;**

      Nga provat e vëna në dispozicion nuk rezulton të ketë një marrëveshje/kontratë midis palëve, por është vënë në dispozicion dokumenti me titull "*Ofertë për projekt kompjuterizues MEDarchiver për strukturën e re klinike në Tiranë*", datë 09.05.2011.

      Mungesa e kontratës midis palëve (kontrollues-përpunues), ku të parashikohen detyrimet e tyre në kuadër të mbrojtjes së të dhënave personale, është në kundërshtim me nenin 20 të Ligjit dhe Udhëzimit 19.

      Nëpërmjet këtij sistemi janë automatizuar të gjitha shërbimet spitalore që në bazë të tyre kanë të dhënat personale dhe sensitive të pacientëve, duke bërë të mundur edhe arkivimin elektronik të të dhënave.

Zyra e Komisionerit vlerëson se, në rastet e delegimit të përpunimit të të dhënave dhe/ose një shërbimi, 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 dhe në protokollin e Zyrës së Komisionerit, si dhe nga hetimi administrativ i ushtruar, rezultoi se Kontrolluesi ka përmbushur detyrimin për njoftim në zbatim të nenit 21 të Ligjit.

   Nga ana tjetër, nga analizimi i përmbajtjes së njoftimit, rezultoi se Kontrolluesi nuk ka kryer përditësimin përkatës për ndryshimin e gjendjes së njoftimit të përpunimit të të dhënave, sa i përket:

   i. Deklarimin në rubrikën 3 ("*Kategoritë e subjekteve të të dhënave personale që përpunohen*"), sa i përket kategorisë "***Vizitorë***" (të dhënat personale të të cilëve përpunohen nëpërmjet regjistrit të hyrje-daljeve dhe sistemit CCTV);

   ii. Deklarimin në rubrikën 7 ("*Marrësi i të dhënave personale*") të marrësit "*Intermedica-Center*" Shpk, drejt të cilit kontrolluesi i përhap të dhënat personale në zbatim të marrëveshjes, për delegimin e shërbimit të kryerjes së ekzaminimeve laboratorike klinike, biokimike, hormonale, bakterologjike, citologjike, parazitologjike;

   iii. Deklarimin në rubrikën 8 ("*Transferimi ndërkombëtar i të dhënave personale*") të shërbimit të administrimit dhe mirëmbajtjes së *Software MEDarchiver*, deleguar tek shoqëria "*MEDArchiver*" *Srl* (me seli në Itali);

   Zyra e Komisionerit vlerëson se realizimi i detyrimit për përditësimin e ndryshimit të gjendjes së njoftimit të përpunimit të të dhënave është i rëndësishëm, pasi i jep mundësinë subjekteve të të dhënave që të informohen për përpunimin e të dhënave të tyre, nga ana e Kontrolluesit, si dhe për realizimin e detyrimeve ligjore të Kontrolluesit. Kjo i jep mundësi reale subjekteve të të dhënave për të ushtruar të drejtat e tyre sipas Ligjit.

6. Kontrolluesi nuk ka ndërmarrë masa në kuadër të trajnimit të punëmarrësve që kanë akses dhe përpunojnë të dhëna personale, lidhur me legjislacionin në fuqi për mbrojtjen e të dhënave personale, si dhe vërehet 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 "*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.

   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 çertifikueshëm, 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.

Përfaqësuesit e Kontrolluesit janë paraqitur në seancën dëgjimore të organizuar nga Zyra e Komisionerit, deklaruan pretendimet e tyre dhe masat e marra në drejtim të rikuperimit të mangësive të konstatuara gjatë hetimit administrativ (të cilat në vijim i dërguan nëpërmjet emailit zyrtar të Zyrës së Komisionerit), si më poshtë:

- Lidhur me afatet për ruajtjen e të dhënave personale/sensitive të pacientëve, administratori i Kontrolluesit ka miratuar Urdhrin nr. 264, datë 16.12.2020 mbi ndryshimin e Rregullores së Brendshme "*Për ruajtjen dhe menaxhimin e dokumentacionit të spitalit*" dhe bashkëlidhur rregulloren e ndryshuar, të cilat janë administruar si provë në dosjen e hetimit administrativ;

- Lidhur me detyrimin për informim (neni 18 i Ligjit), kontrolluesi ka miratuar Urdhrin nr. 263, datë 16.12.2020 mbi ndryshimin e formatit informues *"Shënim Informues për trajtimin e të dhënave personale"*, bashkëlidhur formatin e ndryshuar, të cilat janë administruar si provë në dosjen e hetimit administrativ.

  Gjithashtu, sa i përket politikës së privatësisë në faqen *online* www.salus.al, në kuadër të detyrimit për informim, Kontrolluesi deklaron se ka marrë masa dhe ka realizuar ndryshimet përkatëse;

- Lidhur me kontratat e bashkëpunimit nëpërmjet të cilave Kontrolluesi ka kryer delegimin (*outsource*) e përpunimit të të dhënave personale/sensitive:

  - Kontrolluesi ka depozituar gjatë seancës, marrëveshjen e konfidencialitetit që ka nëshkruar me shoqërinë "Intermedica-Center" Shpk (në cilësinë e përpunuesit);

  - Sa i përket delegimit të shërbimit të administrimit dhe mirëmbajtjes së *Software MEDarchiver,* nga shoqëria "MEDArchiver" Srl, Kontrolluesi pretendon se forma juridike e bashkëpunimit mes palëve është përmes negocimit të ofertës dhe dakordësisë përfundimtare të termave të ofertës. Kjo shpreh vullnetin e palëve dhe konsiderohet ofertë përfundimtare e pranuar prej tyre. Për më tepër,

citohet se shoqëria "*MEDArchiver*" Srl e ushtron aktivitetin në shtetin Italian, i cili konsiderohet si vend me nivel të mjaftueshëm të mbrojtjes së të dhënave;

- Lidhur me detyrimin për njoftim, Kontrolluesi pretendon se për kategorinë e subjekteve të të dhënave vizitorë, të dhënat e tyre mbahen nëpërmjet një regjistri manual.

- Lidhur me marrjen e masave në kuadër të trajnimit të punëmarrësve që kanë akses dhe përpunojnë të dhëna personale dhe mosplotësim e detyrimeve në lidhje ngritjen, administrimin dhe mirëmbajtjen e sistemit të menaxhimit të sigurisë së informacionit (SMSI) lidhur me mbrojtjen e të dhënave personale, Kontrolluesi ka miratuar Urdhrin nr. 265, datë 16.12.2020, mbi trajnimin e punëmarrësve qe kanë akses dhe përpunojnë të dhëna personale dhe trajnimin mbi Udhëzimin nr. 47 dhe trajnim mbi rregulloren e brendshme mbi sigurinë e informacionit.

Në vijim të shqyrtimit të pretendimeve dhe masave të marra nga Kontrolluesi, Zyra e Komisionerit vlerëson se në tërësinë e tyre ato reflektojnë dakordësinë e Kontrolluesit në lidhje me konstatimet gjatë hetimit administrativ dhe angazhimin për t'i përmbushur detyrimet ligjore.

Zyra e Komisionerit vlerëson bashkëpunimin e Kontrolluesit me grupin e hetimit 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, 18, 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 dhe Udhëzimin nr. 49, si dhe të marrë masa për adresimin e konstatimeve të Komisionerit;

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 të kryejë përditësimin e njoftimit për ndryshimin e gjendjes së përpunimit të të dhënave personale dhe sensitive për të cilat është përgjegjës, në zbatim të neneve 21 dhe 22 të Ligjit;

5. Kontrolluesi, me qëllim garantimin e sigurisë së të dhënave personale dhe sensitive, 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 parashikuara në pikat 3 dhe 4 më sipër; dhe

   (iii) brenda 60 (gjashtëdhjetë ditëve), detyrimin e parashikuar në pikën 5 më sipër.

   Afatet e sipërpërmendura fillojnë nga data e 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 7.1.2021.

KOMISIONERI

Besnik Dervishi

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