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. 1132/6 prot.

Tiranë më 30.7.2021

VENDIM

Nr. 35, datë 30.7.2021

PËR KONTROLLUESIN QENDRA SPITALORE "*XHAFERR KONGOLI*", ELBASAN

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 Qendra Spitalore "*Xhaferr Kongoli*" Elbasan.

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 96, datë 28.06.2021 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 hetimi administrativ pranë Kontrolluesit Qendrës Spitalore "*Xhaferr Kongoli*" Elbasan (në vijim, *"Kontrolluesi"*), 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, dhe shërbimin me shtretër në specialitetet përkatëse. Kontrolluesi mbledh dhe përpunon të dhëna personale dhe sensitive për subjektet e të dhënave personale "*punëmarrës*", "*pacientë*" dhe "*vizitorë*". Përpunimi i të dhënave kryhet në mënyrë manuale dhe elektronike.

2. Në lidhje me përpunimin e të dhënave për kategorinë e subjekteve të të dhënave *"punëmarrës"*, konstatohet se në disa prej dosjeve të punëmarrësve ndodhet edhe dokumentacioni i kandidatit tjetër për të njëjtin pozicion pune. Dokumentacioni i kandidatit përmban diplomën, listën e notave, jetëshkrimin (Curriculum Vitae), dëshmi aftësish, etj., në kundërshtim me parashikimet e neneve 5 dhe 6 të Ligjit.

   Zyra e Komisionerit vlerëson se, lidhur me përpunimin e të dhënave për kategorinë e subjekteve "*kandidat për punë*", Kontrolluesi duhet të parashikojë mbajtjen e tyre në atë formë, që lejon identifikimin për një kohë të caktuar, por jo më tepër sesa është e nevojshme për përmbushjen e qëllimit të grumbullimit. Mbajtja e të dhënave të kategorisë "*kandidat për punë*" përtej qëllimit konsiderohet në shkelje me parashikimet e germës "d", të pikës 1 të nenit 5, me kriteret ligjore për përpunimin e të dhënave të përcaktuar në nenin 6 të Ligjit si dhe të Udhëzimit nr. 42, datë 20.07.2014 "*Për përpunimin e të dhënave personale të kandidatëve për punë*", i ndryshuar.

3. Kontrolluesi ka lidhur kontrata me palë të treta: Kontratë Shërbimi me "*BNT Electronics SHPK*" me nr. 2141/9 datë 09.02.2021, Kontratë Shërbimi me BOE "*Health & Life SHPK*" dhe "*Saer Medical SHPK*" me nr. 1023/1 Prot, datë 01.07.2021, me objekt "*Mirëmbajtje e përqendruar e pajisjeve të mëdha mjekësore, Loti 1 pajisje mjekësore të prodhuesit Phillips*", kontratë me nr. 2141/7 me shoqërinë "*Health & Life SHPK*", me objekt "*Mirëmbajtje të pajisjeve radiologjike, Loti 1 mirëmbajtje të aparateve grafi i prodhuesit Phillips dhe Loti 2 mirëmbajtje e aparatit mamografi i prodhuesit IMS*".

   Nga verifikimi i kontratave me palët e treta, rezulton se nuk janë reflektuar plotësisht detyrimet sipas parashikimeve në nenin 20 të ligjit.

   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, 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"*).

4. Nga verifikimi i kryer në regjistrin elektronik të subjekteve kontrolluese, në protokollin e Zyrës së Komisionerit, rezulton se kontrolluesi ka "*Njoftuar*" mbi përpunimin e të dhënave personale për të cilat është përgjegjës. Gjatë hetimit administrativ të ushtruar, është konstatuar se "*Njoftimi*" ka mangësi në deklarim sa i përket rubrikave të formularit si vijon:

   Rubrika 1: Ndryshimi i personit të kontaktit;

   Rubrika 4: Kategoritë e të dhënave personale që përpunohen-Imazhe nëpërmjet kamerave të sistemit të video-survejimit (CCTV);

   Konstatimet e mësipërme janë në kundërshtim me parashikimet e neneve 21 dhe 22 të Ligjit.

   Zyra e Komisionerit vlerëson se realizimi i detyrimit për përditësimin e ndryshimit të gjendjes së njoftimit 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 këtij të fundit. Kjo i jep mundësi reale subjekteve të të dhënave për të ushtruar të drejtat e tyre sipas Ligjit.

5. 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, mos përdorimi, pamundësia e aksesimit të tyre, në përputhje me parashikimet e nenit 27 të Ligjit, nenit 2 dhe pikës 4 të nenit 8 të Udhëzimin nr. 49,

   Kontrolluesi disponon rregullore *"Për mbrojtjen e të dhënave personale"* por, konstatohet se rregullorja nuk parashikon detyrimet e mësipërme, me qëllim garantimin e përpunimit të ligjshëm dhe sigurisë së të dhënave, në përputhje me proceset përpunuese të kontrolluesit.

   Konstatohet një mungesë e rregullimeve lidhur me nivelet e aksesit në të dhënat sensitive të pacientëve si dhe të atyre me COVID-19. Kontrolluesi nuk ka marrë masa për të përmirësuar rregulloret sektoriale për mbrojtjen e të dhënave personale, duke parashikuar dispozita konkrete, në mbështetje të Ligjit.

   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 subjekti të dhënash), 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 dhe Udhëzimit nr. 49, duke mundësuar shmangien e pasojave të 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. Rezulton mosplotësim i detyrimeve në lidhje me ngritjen, administrimin dhe mirëmbajtjen e sistemit të menaxhimit së sigurisë së informacionit (SMSI) për sa i takon mbrojtjes së të dhënave personale, të parashikuara nga Udhëzimi nr. 47, datë 14.09.2018 i 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 që Kontrolluesi ushtron.

   Zyra e Komisionerit vlerëson se, për shkak të cilësisë si subjekt përpunues i madh, si dhe për shkak të natyrës së veprimtarisë që ushtron (përpunon të dhëna sensitive), e cila kërkon masa të shtuara teknike dhe organizative për garantimin e sigurisë së të dhënave, 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", si dhe është një sistem i certifikueshëm, për qëllime përputhshmërie me standardin e sipërpërmendur, vetëm me organizma të akredituar dhe autorizuar sipas parashikimeve të Udhëzimit nr. 48.

   Gjithashtu, ndaj Kontrolluesit është zhvilluar hetim administrativ edhe më përpara, ku Komisioneri nëpërmjet Vendimit nr. 25, datë 13.05.2016 e ka sanksionuar me gjobë për shkelje të detyrimeve të nenit 27 dhe 28 të Ligjit.

Në përfundim të hetimit administrativ, në datën 06.07.2021, referuar provave dhe konstatimeve në vend, grupi i inspektimit hartoi procesverbalin përkatës i cili u nënshkrua nga Kontrolluesi pa paraqitur pretendime.

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 në datën 22.07.2021, përpara marrjes së vendimit përfundimtar nga ana e Komisionerit. Kontrolluesi nuk mori pjesë në seancë dëgjimore dhe nuk paraqiti pretendime me shkrim lidhur me shkeljet administrative të evidentuara gjatë kontrollit.

Si përfundim, shkeljet e konstatuara gjatë ushtrimit të hetimit administrativ, në kuptim të nenit 39, pika 1, germat "*a*", "*ç*", "*d*" dhe "*dh*" të Ligjit, përbëjnë kundërvajtje administrative dhe sanksionohen me gjobë, si më poshtë:

a) kontrolluesit, që përdorin të dhëna personale në kundërshtim me kreun II "Përpunimi i të dhënave personale", dënohen me 10 000 deri në 500 000 lekë;

ç) kontrolluesit ose përpunuesit, që nuk zbatojnë 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 detyrimet për ruajtjen e konfidencialitetit të përcaktuar përkatësisht në nenet 27 dhe 28 të këtij ligji, dënohen me 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 se shkeljet e konstatuara janë serioze. Ato lidhen me garantimin e parimeve dhe përpunimin e ligjshëm të të dhënave. Gjithashtu, vendimi i Komisionerit bazohet në mënyrën e reagimit të kontrolluesit për rikuperimin e shkeljeve të konstatuara.

PËR KËTO ARSYE:

Sa më sipër, në zbatim të neneve 5, 6, 20, 21, 27, 29, 30, 39 (pika 1, germat *"a", "b", "ç" dhe "d"*), si dhe nenet 40 dhe 41 të Ligjit,

V E N D O S A:

1. Dënimin e Kontrolluesit me gjobë në vlerën 100 000 (njëqind mijë) lekë, për shkelje të detyrimit të përcaktuar në nenin 20 të Ligjit;

2. Dënimin e Kontrolluesit me gjobë në vlerën 100 000 (njëqind mijë) lekë, për shkelje të detyrimit të përcaktuar në nenin 27 të Ligjit;

3. Kontrolluesi, të marrë masa për implementimin në praktikë të afateve për ruajtjen e të dhënave personale për kategorinë e subjekteve "*kandidat për punë*" duke përcaktuar edhe procedurat e shkatërrimit ose fshirjes së tyre pas përfundimit të këtij afati, në zbatim të nenit 5 të Ligjit. Për këto afate të informohen edhe subjektet e të dhënave;

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

5. Kontrolluesi, me qëllim garantimin e sigurisë së të dhënave personale duhet të zbatojë detyrimet e përcaktuara në Udhëzimin nr. 47, lidhur me krijimin, mirëmbajtjen dhe administrimin e 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 certifikohet, për qëllime përputhshmërie me standardin në fjalë, nga organizma të akredituar dhe autorizuar në përputhje me dispozitat e këtij udhëzimi.

Subjekti kontrollues, në zbatim të pikës 42 të Udhëzimit nr. 47, depoziton pranë Zyrës së Komisionerit kopje të certifikatës së përputhshmërisë.

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:

   (i) Menjëherë, detyrimet e parashikuara në pikën 4 më sipër;
   (ii) Brenda 15 (pesëmbëdhjetë) ditëve, detyrimet e parashikuara në pikën 3, më sipër;
   (iii) Brenda 45 ditëve, detyrimet e parashikuara në pikat 5 dhe 6, më sipër.

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

8. Kontrolluesi të njoftojë Zyrën e Komisionerit për masat e marra.

9. Gjoba 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.

10. 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 30.07.2021.

KOMISIONERI

Besnik Dervishi