



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. 1131/6 prot.

Tiranë më 30.07.2021

VENDIM

Nr. 36, datë 30.07.2021

PËR KONTROLLUESIN “SPITALI RAJONAL DURRËS”

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 Spitalit Rajonal Durrës,

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 95, datë 28.06.2021 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, 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 Spitalit Rajonal Durrës (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, laboratorit klinik - biokimi dhe baktoreologjik si dhe shërbimin me shtretër në specialitetet e përcaktuara me ligj. Shërbimi i

kirurgjisë në Spitalin Rajonal Durrës ka statusin e klinikës universitare. Spitali ka një staf prej 700 punonjësish, nga të cilët 124 mjekë dhe 348 infermierë, dhe pjesa tjetër staf administrativ.

Kontrolluesi mbledh dhe përpunon të dhëna personale dhe sensitive për subjektet e të dhënave personale "punëmarrës", "pacientë" dhe "vizitorë". Përpunimi i të dhënave realizohet në mënyrë manuale dhe elektronike.

2. Kontrolluesi ka publikuar në faqen zyrtare <http://www.srd.gov.al/>, "politikën e privatësisë" me qëllim informimin e subjekteve të të dhënave por, rezulton se ky informim nuk është i plotë dhe në funksion të aktivitetit të Kontrolluesit, lidhur me kategoritë e subjekteve të të dhënave të cilëve u përpunohen të dhënat, kategoritë e të dhënave personale që përpunohen, 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, masat e sigurisë, etj., në kundërshtim kjo 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").

Kontrolluesi në kuadër të garantimit të sigurisë së ambienteve ku ushtron veprimtarinë ka instaluar një sistem kamerash CCTV. Kontrolluesi nuk informon subjektet e të dhënave mbi prezencën e sistemit të video-survejjimit (CCTV), në kundërshtim me parashikimet e nenit 18 të Ligjit dhe Udhëzimit nr.3, datë 05.03.2010 mbi "Përpunimin e të dhënave personale me sistemin e video survejjimit 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 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 përmbushja 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.

3. Kontrolluesi ka lidhur kontrata me palë të treta: "Infosoft Software Development sh.p.k.", me nr. 919/3 Prot, datë 01.06.2021, dhe objekt "Mirëmbajtje Programi Financa 5", kontratë me nr. 784/8 me shoqërinë "B Pro sh.p.k.", dhe objekt "Shërbim mirëmbajtje të faqes zyrtare" në Spitalin Rajonal Durrës, si dhe kontratë nr. 1106/4 Prot., datë 01.07.2021, me bashkimin e Operatorëve (BOE), SAER Medical sh.p.k. dhe HELATH & LIGHT.

Nga shqyrtimi i kontratave, rezulton se nuk janë reflektuar detyrimet sipas parashikimeve në nenin 20, të Ligjit, 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 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.

4. Nga verifikimi i kryer në regjistrin elektronik të subjekteve kontrolluese, në protokollin e Zyrës së Komisionerit si dhe nga hetimi administrativ i ushtruar, rezultoi se Kontrolluesi e ka përbushur 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. Ky detyrim është përbushur nga Kontrolluesi pasi ka filluar hetimi administrativ.

Zyra e Komisionerit vlerëson se realizimi i detyrimit për njoftim dhe përditësimi mbi përpunimin e të dhënave personale, 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 në 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 aksesit 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 8/4 të Udhëzimit 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 zbatim të Ligjit.

Zyra e Komisionerit vlerëson se, hartimi i një "*Rregulloreje specifike për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*", ku 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. Rezultoni mosplotësimi i detyrimeve në lidhje me ngritjen, administrimin dhe mirëmbajtjen e sistemit të menaxhimit të 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”*).

Zyra e Komisionerit vlerëson se, për shkak të cilësisë si subjekt përpunues i madh, si dhe për shkak të natyrës së veprimtarisë që ushtron, kjo e fundit 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 certifikueshëm, 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 inspektimit hartoi procesverbalin përkatës i cili u nënshkrua nga përfaqësuesi i Kontrolluesit, duke u shprehur se pretendimet do i paraqisnin me shkrim brenda 3 (tre) ditëve.

Në respektim të së drejtës për t’u dëgjuar, në zbatim të neneve 87-89 të *Kodit të Procedurave Administrative*, Kontrolluesi është ftuar nga ana e Komisionerit përpara dhënies së vendimit të tij përfundimtar, të marrë pjesë në seancë dëgjimore.

Përfaqësuesi i Kontrolluesit, gjatë seancës dëgjimore të zhvilluar në datë 22.07.2021, ashtu si dhe në pretendimet me shkrim mbajti të njëjtin qëndrim, si vijon:

- Sa i përket konstatimit në lidhje me parashikimet e nenit 20, Kontrolluesi argumenton se: *“..APP-ja, harton dhe miraton me vendim formatin e DST-ve, dhe se ky institucion ka kompetencën ekskluzive etj.”*

Zyra e Komisionerit vlerëson se ky pretendim nuk qëndron, pasi APP-ja në ushtrim të detyrave të saj, ka për qëllim ndër të tjera, kryesisht dhe

ekskluzivisht, të sigurojë mirë përdorimin e fondeve publike dhe të ulë shpenzimet procedurale, pra mirë menaxhimin e fondeve publike nga Autoritetet Kontraktore. APP-ja, krijon standardet e dokumentacioneve dhe të sistemit elektronik, i monitoron ato si dhe kontratat që finalizohen pas procesit të prokurimit me fondet publike.

Marrëveshja e konfidencialitetit është krejt tjetër gjë, dhe e detyrueshme për t'u përmbushur nga Kontrolluesi. Monitorimi i këtij detyrimi, është kompetencë e Komisionerit. Detyrimet e Kontrolluesit dhe përpunuesit për përpunimin e të dhënave personale, në rastet e delegimit të përpunimit të të dhënave dhe/ose një shërbimi, parashikohen në nenin 20 të Ligjit dhe rregullohen me aplikimin e Udhëzimit nr.19.

- Sa i përket konstatimit në lidhje me parashikimet e nenit 18, Kontrolluesi argumenton se:

“..në bazë të ligjit nr.19/2016, “Për masat shtesë të sigurisë Publike”, çdo institucion është i detyruar të jetë i survejuar me kamera ndaj referuar konstatimeve të procesverbalit të kontrollit, etj.”

Zyra e Komisionerit vlerëson se, në kuadër të garantimit të sigurisë, Kontrolluesi mundet të instalojë sistem video-survejimi (CCTV), por gjithmonë duke mos anashkaluar detyrimin që, survejimi i ambienteve të jetë në përputhje me dispozitat e parashikuara në nenin 18 të Ligjit si dhe Udhëzimin nr. 3.

Tabela informuese mbi prezencën e sistemit të video-survejimit ka për qëllim informimin e subjekteve të të dhënave “nëpunës”, “pacientë”, “vizitorë”, etj., mbi përpunimin e të dhënave personale imazhe-video, ushtrimin e të drejtave të subjekteve të të dhënave në rast të cënimit të privatësisë, etj.

- Në lidhje me pretendimin e Kontrolluesit se: *“.. SRD-ja është përballur me situata të vështira që nga tërmeti i nëntorit 2019 dhe më pas për shkak të pandemisë Covid 19 etj..”*, Zyra e Komisionerit vlerëson se, ky argument nuk qëndron. Situata e shkaktuar nga pandemia COVID-19 nuk përbën shkak ligjor për kufizimin dhe mosrespektimin e të drejtës së çdo qytetari për mbrojtjen e të dhënave të tij personale dhe rrjedhimisht, për mosrespektimin e jetës së tij private, të cilat së bashku përbëjnë një kategori të drejtash vetjake të mbrojtura nga Kushtetuta (neni 35).

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 që, shkeljet e konstatuara janë serioze, dhe Kontrolluesi është në kushtet e nenit 30/2 të përsëritjes së shkeljeve dhe moszbatimit të Rekomandimeve të Komisionerit.

Ndaj Kontrolluesit janë zhvilluar hetime administrative të mëparshme, ku Komisioneri nëpërmjet Vendimeve respektive me Nr.21 datë 13.05.2016, dhe Nr.13, datë 27.05.2019, ka sanksionuar me gjobë Kontrolluesin, pikërisht për shkelje të detyrimeve të nenit 21 dhe 27 të Ligjit.

PËR KËTO ARSYE:

Sa më sipër, në zbatim të neneve 18, 20, 21, 27, 29, 30, 39, pika 1 germa “dh”, si dhe nenet 40 dhe 41 të Ligjit,

V E N D O S A:

- 1- Dënimin e Kontrolluesit, me gjobë në vlerën 200 000 (*dyqind mijë*) Lekë, për shkelje të detyrimit të përcaktuar në nenin 27 të Ligjit;
- 2- Kontrolluesi, në zbatim të nenit 18 të Ligjit, të marrë masa konkrete, për përmbushjen e detyrimit për informimin e subjekteve të të dhënave personale, për sa i përket tabelave informuese, si dhe mbi qëllimin dhe mënyrën e përpunimit të të dhënave, duke i detajuar ato në funksion të aktivitetit të tij në faqen zyrtare, rubrika “*Politika e Privatësisë*”;
- 3- Kontrolluesi, në zbatim të nenit 20 të Ligjit, të marrë masa për hartimin e marrëveshjes së Konfidencialitetit me të tretë, sipas parashikimeve të Udhëzimit nr.19, nëse afatet kontraktuale nuk kanë përfunduar;
- 4- Kontrolluesi, në zbatim të nenit 21 të Ligjit, të kryejë përditësimin e “*njoftimit*” në vazhdimësi, për sa i përket ndryshimit të gjendjes së përpunimit të të dhënave personale të cilat ai përpunon;

- 5- Kontrolluesi, në zbatim të nenit 27 të Ligjit, të hartojë “*Rregulloren për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*”, dhe ato sektoriale, duke parashikuar masa konkrete teknike dhe organizative për mbrojtjen e të dhënave personale, mënyrat e përpunimit të të dhënave, të drejtat e subjekteve të të dhënave, etj., në funksion të aktivitetit të tij, për çdo proces përpunimi dhe /ose delegimi mbi përpunimin e të dhënave personale, sensitive të subjekteve të të dhënave personale;
- 6- 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;
- 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- Kontrolluesi në zbatim të Kreut IV të Udhëzimit nr.47, të marrë masa konkrete, për trajnimin e stafit administrativ dhe mjekësor për mbrojtjen e të dhënave personale;
- 9- Kontrolluesi në zbatim të pikës 1 të nenit 32 të Ligjit, të përmbushë detyrimet sipas këtij akti brenda afateve si vijon:
 - (i) brenda 15 (pesëmbëdhjetë) ditëve, detyrimet e parashikuara në pikat 2 3, 4, 5;
 - (ii) brenda 45 (dyzetë e pesë) ditëve, detyrimin e parashikuar në pikën 6;
 - (iii) në vazhdimësi, detyrimin e parashikuar në pikën 8.
Afatet e sipërpërmendura fillojnë nga data e marrjes dijeni të këtij akti.
- 10- Kontrolluesi të njoftojë Zyrën e Komisionerit për masat e marra.
- 11- 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.

12- 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

