R E P U B L I K A E S H Q I P Ë R I S Ë
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. 842/6 Prot. Tiranë, më 10.06.2025

REKOMANDIM

Nr. 31, datë 10.06.2025

PËR KONTROLLUESIN "GENIUS LAB"

Në mbështetje të neneve 81, 82, 83 dhe 84 të ligjit nr. 124/2024 "Për mbrojtjen e të dhënave personale", (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 Laboratori *"Genius Lab",* Tiranë (në vijim, "*Kontrolluesi*"),

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 52 datë 05.03.2025, të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, u krye hetimi administrativ pranë Kontrolluesit *"Genius Lab"* Tiranë (në vijim "*Kontrolluesi*"), me objekt:

- *Zbatim i ligjit nr. 124/2024 "Për mbrojtjen e të dhënave personale", 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. Laboratori mjekësor *"GeniusLab"*, me Nipt L91609004C, është qendër diagnostikuese mjekësore private, me shërbim mjekësor pediatrik, kirurgji, ORL, okulistik, kardiologji, import-export me shumicë e pakicë, depo farmaceutike dhe farmaci, aparatura dentare dhe aksesorët e tyre, trajnim, servis, mirëmbajtje, profilaksi të të gjithë aparaturave mjekësore, për laboratorë kimike, biologjike etj. Blerje dhe shitje pajisje mjekësore, blerje dhe shitje kite, reagentë, materiale mjekësore.

Kontrolluesi në kuadër të veprimtarisë që ushtron, përpunon të dhëna personale për kategoritë "*pacientë*"; "*staf administrativ*"*; "mjek"; "infermier"* etj. Përpunimi i të dhënave kryhet në mënyrë manuale dhe elektronike.

2. Kontrolluesi grumbullon në arkivin fizik dokumentacionin për stafin administrativ. Konstatohet se, në dosjet e personelit të larguar ruhen kopje të librezës së punës, vërtetim i aftësisë për punë, vizitat dhe ekzaminimet mjekësore si dhe diploma e universitetit.

   Nga analizimi i dokumenteve të cilat parashikojnë procedurat dhe masat për proceset përpunuese rezulton se, Kontrolluesi nuk ka parashikuar afate konkrete lidhur me kohën e ruajtjes së të dhënave personale, për dokumentacionin që administron në funksion të veprimtarisë që ushtron.

   Të dhënat e mbledhura nga Kontrolluesi ruhen, pa përcaktuar një afat konkret të ruajtjes së tyre, në kundërshtim me pikën 5, të nenit 6 të Ligjit, si dhe me Udhëzimin nr. 11, datë 08.09.2011 të Komisionerit "*Mbi përpunimin e të dhënave të punonjësve në sektorin privat*" i ndryshuar (në vijim, "*Udhëzimi nr. 11*").

   Zyra e Komisionerit vlerëson se, lidhur me kategoritë e të dhënave të grumbulluara, në funksion të ushtrimit të veprimtarisë së tij, Kontrolluesi duhet të parashikojë mbajtjen e të dhënave personale të grumbulluara në atë formë, që lejon identifikimin për një kohë të caktuar, por jo më tepër se sa është e nevojshme për të përmbushur qëllimin për të cilin të dhënat janë grumbulluar. Koha e ruajtjes së të dhënave personale duhet të përcaktohet nga Kontrolluesi, në përputhje me parashikimin e pikës 5, të nenit 6 të Ligjit.

3. Kontrolluesi disponon një grup politikash të periudhave të ndryshme kohore lidhur me sigurinë e informacionit, e konkretisht:

   1. Politika e sigurisë së informacionit;
   2. Akses në sistemin e-doctors;
   3. Politika e pranueshme e përdorimit të sistemeve të komunikimit;
   4. Information Security, User Awarenes Training;
   5. Tabela e masave për sigurinë kibernetike;
   6. Plani për implementimin e masave të sigurisë kibernetike;
   7. Doget e dokumentacionit;
   8. Politika e Sigurisë së Rrjetit;
   9. Politika e fjalëkalimit;
   10. Politika për back-up;
   11. Politika e përdorimit të pranueshëm të internetit;
   12. Politika e Sigurisë Fizike;
   13. Procesi i menaxhimit të aksesit të përdoruesit;
   14. Politika kundër malware.

Konstatohet se, mungojnë elementë të tjerë të sigurisë së të dhënave *si "Analiza e Ndikimit në të Dhënat Personale"*, *"Analiza e sigurisë së sistemit të arkivimit"* për të gjitha llojet e proceseve përpunuese gjatë ushtrimit të aktivitetit, *"Raport vlerësimi mbi sigurinë në sistemin e arkivimit elektronik dhe fizik*", *"Kontrolli i sigurisë së sistemit të përpunimit të të dhënave"*, etj., në kundërshtim me parashikimet e nenit 28 të Ligjit, dhe Udhëzimit 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*").

Zyra e Komisionerit vlerëson se, 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. Gjithashtu, (SMSI) lidhur me mbrojtjen e të dhënave personale, duhet të jetë në përputhje me parashikimet e Udhëzimit 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 të cilësisë si subjekt përpunues i madh, si dhe për shkak të natyrës së veçantë të veprimtarisë që Kontrolluesi ushtron.

4. Konstatohet se, kontrolluesi disponon *Rregullore të posaçme për "Mbrojtjen, Përpunimin, Ruajtjen dhe Sigurinë e të Dhënave Personale".* Nga shqyrtimi i përmbajtjes së rregullores, konstatohet se, ky akt, si dhe dokumentacioni i vendosur në dispozicion nga kontrolluesi, konkretisht: *"Deklarata për Përpunimin e të Dhënave Personale"* dhe *"Procedura për Menaxhimin, Arkivimin dhe Asgjësimin e të Dhënave Personale"* , kanë hyrë në fuqi më 01.06.2019. Megjithatë, këto akte i referohen legjislacionit të ri për mbrojtjen e të dhënave personale, ndërkohë që Ligji 124/2024 ka hyrë ne fuqi me datë 01.02.2025.

   Konstatohet se, të dhënat sensitive (të lidhura me shëndetin) të subjekteve të të dhënave që përpunohen nga Kontrolluesi, nuk identifikohen në rregullore, si dhe për këtë kategori të të dhënave personale nuk janë parashikuar rregulla dhe procedura organizative specifike, mbi mënyrën e përpunimit të tyre, sigurinë, konfidencialitetin, afatet e mbajtjes së të dhënave, nivelet e aksesit etj., sipas parashikimeve të nenit 28 të Ligjit.

   Zyra e Komisionerit vlerëson se, është i nevojshëm rishikimi i rregullores "*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*" dhe përshtatja e dispozitave të saj, në mënyrë të tillë që, të parashikohen në mënyrë të detajuar rregulla dhe procedura mbi kategoritë e të dhënave personale që përpunohen, mënyrën e përpunimit, masat e sigurisë dhe konfidencialitetit, afatet e ruajtjes, të drejtat e subjekteve të të dhënave, si dhe përcaktimin e niveleve të aksesit, me qëllim garantimin e përpunimit të ligjshëm dhe sigurisë së të dhënave, në përputhje me proceset përpunuese të Kontrolluesit dhe në zbatim të nenit 28 të Ligjit.

5. Kontrolluesi në kuadër të trajnimit të punonjësve që kanë akses dhe përpunojnë të dhëna personale ka ndërmarrë disa masa lidhur me legjislacionin për mbrojtjen e të dhënave personale. Megjithatë, nga verifikimi i moduleve trajnuese rezulton se, në përmbajtje të tyre nuk i referohen legjislacionit shqiptar në fuqi për mbrojtjen e të dhënave personale, si dhe proceseve përpunuese të Kontrolluesit, në kundërshtim me parashikimet e nenit 28 të Ligjit dhe Udhëzimit nr. 47 të Komisionerit.

   Zyra e Komisionerit vlerëson se, Kontrolluesi duhet të marrë masa konkrete në kuadër të trajnimit të punonjësve që kanë akses dhe përpunojnë të dhëna personale, bazuar në legjislacionin në fuqi për mbrojtjen e të dhënave personale si dhe në zbatim të Udhëzimit nr. 47 të Komisionerit.

   Gjithashtu, 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.

Në përfundim të hetimit administrativ, referuar provave dhe konstatimeve në vend, grupi i inspektimit hartoi procesverbalin përkatës, një kopje e të cilit i është vendosur në dispozicion Kontrolluesit nëpërmjet rrugës postare.

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, gjatë seancës dëgjimore, të zhvilluar më datë 28.04.2025, organizuar nga Zyra e Komisionerit, ka parashtruar pretendimet me shkrim, administruar me tonën nr. 842/5 prot., datë 28.04.2025, si dhe ka depozituar dokumentacion plotësues mbi konstatimet e procesverbalit të hetimit administrativ, si vijon:

- Rregullore për ruajtjen e të dhënave personale;
- Deklaratë për përpunimin e të dhënave personale;
- Formular për ndërprerjen e marrëdhënies së punës;
- Vlerësim i riskut (Gap Assessment Tool);
- Procedura për menaxhim, arkivim, dhe asgjësimin e të dhënave në GeniusLAB;
- Module trajnimi 'Kalimi nga Ligji i Mbrojtjes së të Dhënave Personale (2012) në Ligjin e ri (2024);

Në përfundim, Zyra e Komisionerit vlerëson 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 shmang mundësinë e përhapjes së tyre në mënyrë të paligjshme.

PËR KËTO ARSYE:

Në zbatim të neneve 6, 28, 81, 82, 83 dhe 84 të Ligjit,

REKOMANDOJ:

1. Kontrolluesi, të marrë masa për përcaktimin e afateve kohore për ruajtjen e të dhënave, në përputhje me pikën 5, të nenit 6 të Ligjit. Në momentin e përfundimit të qëllimit të përpunimit, Kontrolluesi duhet të realizojë shkatërrimin e këtyre të dhënave, pasi përpunimi i mëtejshëm i tyre konsiderohet i paligjshëm;

2. Kontrolluesi, në zbatim të nenit 28 të Ligjit, të përfshijë në rregulloren "*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*", 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.;

3. Kontrolluesi, me qëllim garantimin e sigurisë së të dhënave personale duhet të zbatojë detyrimet e përcaktuara në Udhëzimin nr. 47, lidhur me trajnimin e punonjësve që kanë akses dhe përpunojnë të dhëna personale si dhe krijimin, mirëmbajtjen dhe administrimin e Sistemit të Menaxhimit të Sigurisë së Informacionit (SMSI) për mbrojtjen e të dhënave personale;

4. 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;

5. Në zbatim të nenit 84 të Ligjit, të përmbushen detyrimet, sipas këtij akti brenda afateve, si vijon:

(i) brenda 15 (pesëmbëdhjetë) ditëve, detyrimet e treguara në pikën 1 më sipër;
(ii) brenda 30 (tridhjetë) ditëve, detyrimin e treguar në pikën 2 më sipër;
(iii) brenda 45 (dyzetë e pesë) ditëve, detyrimin e përcaktuar në pikën 3 më sipër;

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

6. Kontrolluesi të njoftojë Komisionerin për masat e marra;

7. Në rast mospërmbushje të detyrimeve të parashikuara në këtë akt, Komisioneri, bazuar në germën "a", pika 2, e nenit 83 të Ligjit, paralajmëron kontrolluesit ose përpunuesit se veprimet e përpunimit mund të rezultojnë në mosplotësim të dispozitave ligjore dhe u jep atyre rekomandime lidhur me përputhshmërinë me ligjin. Në rast shkeljesh serioze ose të qëllimshme të dispozitave ligjore, Komisioneri vepron sipas neneve 92, 93 dhe 94 të Ligjit, për vendosjen e sanksioneve administrative në përputhje me nenet përkatëse, si dhe në përputhje me legjislacionin në fuqi për kundërvajtjet administrative, në mënyrë të tillë që këto masa të jenë efektive, proporcionale dhe me karakter parandalues.

Ky Rekomandim u shpall sot, më 10.06.2025.

KOMISIONERI

Besnik Dervishi