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. 410/7 prot. Tiranë, më 28.04.2026

VENDIM

Nr. 13, datë 28.04.2026

PËR KONTROLLUESIN SHOQËRIA "LOFT CONSTRUCTION" SHPK

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 i Republikës së Shqipërisë*" (në vijim, "*Kodi i Procedurave Administrative*"), procesverbalit të hetimit, si dhe provave të administruara në përfundim të hetimit administrativ në ngarkim të Kontrolluesit Shoqëria "Loft Construction" shpk (në vijim, "*Kontrolluesi*"),

KONSTATOHET SE:

Në zbatim të Urdhrit nr. 27, datë 6.02.2026 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim, "*Komisioneri*"), u organizua grupi i punës i cili kreu hetimin administrativ pranë Kontrolluesit, me objekt:

- *Zbatimi 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 grupit të hetimit, procesverbalin e konstatimit dhe provat e administruara gjatë ushtrimit të hetimit pranë Kontrolluesit, vëren se:

1. Kontrolluesi është i regjistruar në Qendrën Kombëtare të Biznesit me NUIS M12124033B me objekt aktiviteti: "*Ndërtime civile dhe industriale, rikonstruksion dhe mirëmbajtje godinash civile industriale, veshje fasada*, etj."

Kontrolluesi mbledh dhe përpunon të dhëna personale për kategorinë e të dhënave "*punonjës*", "*klientë*", "*vizitorë*" etj. Përpunimi i të dhënave personale kryhet në mënyrë manuale dhe elektronike.

2. Kontrolluesi ka krijuar në platformën "*Facebook*" dhe "*Instagram*" profile zyrtare, në të cilën pasqyron veprimtari të ndryshme, duke ilustruar nëpërmjet fotografive dhe videove, të dhënat e subjekteve, punonjës, pjesëmarrës, etj.

   U konstatua se, të dhënat e subjekteve më sipër përpunohen/publikohen në rrjetin social "*Facebook*" dhe "*Instagram*", në kundërshtim me parimet e mbrojtjes së të dhënave personale dhe kriteret për përpunimin e të dhënave, të parashikuara në nenet 6 dhe 7 të Ligjit, si dhe pa marrë pëlqimin e tyre, sipas parashikimit të nenit 8 të Ligjit.

   Zyra e Komisionerit vlerësoi se, përpunimi i të dhënave personale të subjekteve të të dhënave, përmes publikimit të fotografive të subjekteve të të dhënave në platforma si "*Facebook*" dhe "*Instagram*", pa marrë paraprakisht "*Pëlqimin*", bie në kundërshtim me nenet 6 dhe 7 të Ligjit.

   Bazuar në nenin 8 të Ligjit, "*Pëlqim*" është çdo element tregues i vullnetit të subjektit të të dhënave, i dhënë lirisht, i informuar dhe i qartë, nëpërmjet të cilit ai, me anë të një deklarate ose me çdo lloj shfaqjeje tjetër të padyshimtë pohuese të vullnetit, shpreh dakordësinë për përpunimin e të dhënave personale, që lidhen me të për një ose më shumë qëllime specifike.

3. Kontrolluesi ka të instaluar sistemin e video-survejimit (CCTV), përmes së cilit kryen mbikëqyrjen e ambienteve të brendshme dhe të jashtme ku ushtron veprimtarinë e tij. Nga analizimi i planvendosjes së kamerave, konstatohet se disa prej tyre janë të instaluara dhe orientuara në mënyrë të tillë që monitorojnë ambientet e jashtme të ndërtesës, duke përfshirë edhe ambiente të tjera, rrugë kalimi dhe qytetarë, si dhe ambientet e posteve të punës në kundërshtim me pikën 2, të nenit 6 dhe nenin 7 të Ligjit, Udhëzimin nr. 03, datë 30.04.2025, "*Për përpunimin e të dhënave personale nga sistemet e video survejimit*" (në vijim, "*Udhëzimi nr. 3*") dhe Udhëzimin nr. 11, datë 08.09.2011, "*Mbi përpunimin e të dhënave të punonjësve në sektorin privat*", i ndryshuar (në vijim, "*Udhëzimi nr. 11*").

   Nga verifikimet e kryera në sistemin e video-survejimit (CCTV), rezulton se të dhënat imazhe/video, ruhen përtej afatit ligjor, në kundërshtim me parimin e ruajtjes në kohë, sipas pikës 5, të nenit 6 të Ligjit dhe Udhëzimin nr. 3, të Komisionerit.

   Zyra e Komisionerit vlerëson se, një nga mjetet e rëndësishme të përpunimit të të dhënave personale është edhe sistemi i video-survejimit (CCTV). Të dhënat e ruajtura në këto sisteme, si: "imazhe" e "video", janë të dhëna personale dhe përpunimi i tyre duhet të jetë në përputhje me parashikimet e Ligjit, si dhe aktet e miratuara nga Komisioneri në lidhje me mbledhjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale, gjatë kryerjes së aktivitetit nga Kontrolluesi.

Gjithashtu vlerësohet se periudha e mbajtjes së të dhënave nuk duhet të kalojë kufirin maksimal të afatit të lejuar, për përmbushjen e qëllimit të video-survejimit. Të dhënat e mbajtura me anë të sistemit të video-survejimit duhet të ruhen për një periudhë jo më të gjatë se 30 ditë, dhe në momentin që qëllimi ka përfunduar duhet të realizohet shkatërrimi i të dhënave imazhe/video, në të kundërt përpunimi i mëtejshëm i të dhënave konsiderohet i paligjshëm, sipas parashikimeve të pikës 5, të nenit 6 të Ligjit dhe të Udhëzimit nr. 3 të Komisionerit.

Nga verifikimi në vend i sistemit të video-survejimit (CCTV), si dhe nga shqyrtimi i dokumentacionit të vënë në dispozicion, është konstatuar se Kontrolluesi nuk ka miratuar një rregullore të brendshme për administrimin, aksesin, ruajtjen dhe fshirjen e të dhënave imazh/video të përpunuara përmes këtij sistemi, në kundërshtim me nenin 28 të Ligjit.

Për shkak të volumit dhe kategorive të të dhënave personale që përpunon, si dhe natyrës së veprimtarisë së tij, e cila kërkon masa të shtuara teknike dhe organizative për garantimin e sigurisë së të dhënave personale, Zyra e Komisionerit vlerëson se Kontrolluesi është i detyruar të hartojë rregulla/politika të brendshme specifike për mënyrën e përpunimit të të dhënave personale, nivelet e aksesit, afatet e ruajtjes së të dhënave, etj., nëpërmjet sistemit të video-survejimit (CCTV), në përputhje me nenin 28 të Ligjit.

4. Nga shqyrtimi i dokumentacionit të vendosur në dispozicion rezulton se, Kontrolluesi disponon rregullore të brendshme "*Mbi trajtimin e të dhënave personale nga punonjësit e Loft Contruction shpk*". Nga shqyrtimi i përmbajtjes së saj, si dhe nga analizimi në tërësi i provave të mbledhura gjatë hetimit administrativ, rezulton se, rregullorja parashikon vetëm afatin për ruajtjen maksimale të filmimeve (deri në 30 ditë), por nuk përcakton afatet e mbajtjes së të dhënave, që administrohen nga Kontrolluesi, në ushtrim të veprimtarisë së tij. Gjithashtu, mungojnë parashikime mbi mënyrën e përpunimit të të dhënave personale, si mënyra e mbledhjes, regjistrimit, ruajtjes dhe asgjësimit të tyre, me qëllim garantimin e përpunimit të ligjshëm dhe sigurisë së të dhënave, në përputhje me proceset përpunuese që kryen, sipas parashikimeve të nenit 27 dhe 28 të Ligjit.

   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.

   Gjithashtu, në rregullore duhet të përcaktohen në mënyrë të detajuar rregulla dhe procedura organizative për të gjitha aspektet e përpunimit të të dhënave, duke përfshirë, mënyrën e përpunimit, masat e sigurisë fizike, teknike dhe administrative, ruajtjen dhe konfidencialitetin e të dhënave, aksesin, si dhe afatet e ruajtjes së të dhënave. Plotësimi i rregullores me të gjithë elementët ligjorë të përcaktuar në pikën

1 të nenit 27 të Ligjit, konsiderohet një detyrim shumë i rëndësishëm, në zbatim të nenit 27 dhe 28 të Ligjit, për të mundësuar shmangien e pasojave të rënda që mund të vijnë për subjektet e të dhënave.

5. Rezulton se, Kontrolluesi nuk ka marrë masat e duhura teknike dhe organizative për të garantuar një nivel sigurie të përshtatshëm ndaj rrezikut, duke përfshirë, ndër të tjera, *pseudonimizimin dhe enkriptimin e të dhënave personale; aftësinë për të garantuar konfidencialitetin, integritetin, disponueshmërinë dhe qëndrueshmërinë e sistemeve dhe të shërbimeve të përpunimit; aftësinë për të rivendosur disponueshmërinë dhe aksesin në të dhënat personale brenda një kohe të arsyeshme në rast incidenti fizik ose teknik; një proces për testimin, shqyrtimin dhe vlerësimin e rregullt të efikasitetit të masave teknike dhe organizative për të garantuar sigurinë e përpunimit* etj., në kundërshtim me parashikimet e nenit 28 të Ligjit dhe Vendimit nr. 6, datë 05.08.2013 të Komisionerit "*Për përcaktimin e rregullave të hollësishme për sigurimin e të dhënave personale*" (në vijim, "*Vendimi nr. 6*").

   Gjithashtu, konstatohet se Kontrolluesi nuk mban dokumentacion mbi veprimtaritë e përpunimit, me qëllim demonstrimin e përputhshmërisë me ligjin, në formë të shkruar dhe në format elektronik, sipas parashikimeve të nenit 27 të Ligjit.

   Kontrolluesi, duke marrë në konsideratë natyrën e veprimtarisë së tij, nuk ka marrë masa për të krijuar, zbatuar, mirëmbajtur dhe përmirësuar në mënyrë të vazhdueshme një Sistem Menaxhimi të të Dhënave Personale (*Privacy Information Management System "PIMS"*), sipas Udhëzimit nr. 09, datë 20.11.2025 "*Për kriteret e përgjithshme për certifikimin dhe për dhënien e vulave dhe të shenjave të mbrojtjes së të dhënave personale*" (në vijim, "*Udhëzimi nr. 09*") .

   Kuadri ligjor evropian mbi mbrojtjen e të dhënave personale, të cilin Ligji transpozon, dhe praktika më e mirë evropiane, e konsideron certifikimin si një mekanizëm përputhshmërie me Ligjin[1] dhe për të inkurajuar zbatimin e tij, i krijon rast pas rasti kontrolluesve që e zbatojnë atë në mënyrë efektive, një pozitë preferenciale në kryerjen e disa veprimtarive përpunuese të caktuara, siç janë për shembull transferimet ndërkombëtare. Në këtë kuadër, në zbatim të nenit 37 të Ligjit, i cili parashikon dhe rregullon mekanizmin e certifikimit, Komisioneri ka miratuar Udhëzimin nr. 08 datë 20.11.2025 "*Për kriteret shtesë për akreditimin e organizmave certifikues*" (në vijim, "*Udhëzimi nr. 08*") dhe Udhëzimin nr. 09.

   Udhëzimi nr. 09 referon në Sistemet e Menaxhimit të të Dhënave Personale (*Privacy Information Management System "PIMS"*) dhe Komisioneri inkurajon kontrolluesit, të cilët për shkak të natyrës së veprimtarisë së tyre, e kanë të nevojshëm ngritjen e një sistemi të tillë me qëllim standardizimin dhe rregullimin e veprimtarisë përpunuese dhe garantimin e sigurisë së përpunimit të të dhënave personale, të zbatojnë Udhëzimin nr. 08 dhe nr. 09.

[1] *Pika 3 e nenit 22, pika 3 e nenit 23, pika 3 e nenit 28*

Në rastin konkret, Zyra e Komisionerit ka vlerësuar se, 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 duhet të krijojë, mirëmbajë dhe administrojë një sistem menaxhimi të të dhënave personale (PIMS) në përputhje me parashikimet e Udhëzimit nr. 09.

Bazuar në nenin 28 të Ligjit dhe nenin 13 të Udhëzimit nr. 09, Kontrolluesi duhet të marrë masa konkrete teknike dhe organizative që garantojnë nivel të përshtatshëm për rrezikun, masa të cilat duhet të rishikohen në mënyrë periodike për të siguruar efektivitet të vazhdueshëm.

6. Rezulton se, Kontrolluesi aplikon për punëmarrësit deklaratën e konfidencialitetit, si aneks i kontratës së punës. Megjithatë, nga analizimi i përmbajtjes së saj, evidentohet se nuk parashikohen të drejtat dhe detyrimet për ruajtjen e konfidencialitetit në përputhje me parashikimet e legjislacionit për mbrojtjen e të dhënave personale për nëpunësit që kanë akses në të dhënat personale, në kundërshtim me nenin 30 të Ligjit.

   Zyra e Komisionerit vlerëson se, qëllimi i nënshkrimit të "*Deklaratës së Konfidencialitetit*" është që të gjithë punonjësit, të cilët kanë akses për arsye profesionale në procese përpunuese dhe në të dhënat personale, të kuptojnë qartë dhe drejtë, detyrimet dhe përgjegjësitë që ata kanë mbi përpunimin e të dhënave personale dhe ruajtjen e konfidencialitetit.

7. Nga verifikimi në vend, ka rezultuar se Kontrolluesi e ka të organizuar rrjetin e brendshëm të intranetit me pajisje kompjuterike, të cilat nuk janë të qendërzuara sipas modelit të *domain controller*-it apo ekuivalente, duke sjellë mungesën e një arkitekture të unifikuar për administrimin e përdoruesve, autorizimeve dhe politikave të sigurisë. Kjo mënyrë organizimi rrit rrezikun për akses të paautorizuar, mungesë gjurmueshmërie dhe dobësi në menaxhimin e privilegjeve, në kundërshtim me kërkesat e nenit 27 dhe 28 të Ligjit për garantimin e konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave personale përmes masave të përshtatshme teknike.

   Gjithashtu, masat e sigurisë teknike të sigurisë që përdor Kontrolluesi për infrastrukturën e teknologjisë së informacionit, nuk i përgjigjen standardeve më të mira ndërkombëtare, duke mos ofruar mekanizma të avancuar filtrimi, monitorimi dhe parandalimi të ndërhyrjeve (IPS/IDS, etj.), çka cenon kërkesën e nenit 28 të Ligjit për zbatimin e masave teknike të përshtatshme në raport me rrezikun.

   Zyra e Komisionerit ka vlerësuar se kontrolluesit, në referim të kërkesave të përcaktuara në nenin 28 të Ligjit, duhet të zbatojnë masat e duhura teknike dhe organizative për të siguruar një nivel të përshtatshëm ndaj rrezikut. Në vlerësimin e nivelit të përshtatshëm të sigurisë duhet të merren parasysh veçanërisht rreziqet që shkaktohen nga përpunimi, specifikisht, nga shkatërrimi aksidental ose i paligjshëm, humbja, ndryshimi, përhapja e paautorizuar ose aksesi në të dhënat personale të transmetuara, të ruajtura ose të përpunuara në çfarëdolloj mënyre.

8. Nga verifikimi *on-site* i infrastrukturës së teknologjisë së informacionit, si dhe nga shqyrtimi i procedurave rregulluese të Kontrolluesit, rezulton se:

    - Kontrolluesi nuk ka hartuar dhe miratuar plane të dokumentuara për menaxhimin e riskut, përfshirë identifikimin, analizimin dhe vlerësimin e rreziqeve që lidhen me përpunimin e të dhënave personale, si dhe nuk ka përcaktuar teknikat dhe mekanizmat përkatës të menaxhimit dhe monitorimit të performancës së masave të sigurisë, në kundërshtim me detyrimin për të garantuar një nivel sigurie të përshtatshëm sipas parimit të llogaridhënies;
    - Kontrolluesi nuk ka të hartuar planin e politikave të vazhdueshmërisë së biznesit, dokumente këto që do të duhet të përmbanin politikat dhe objektivat që sigurojnë vijueshmërinë e punës;
    - Kontrolluesi nuk ka të specifikuar/dokumentuar kohën maksimale në të cilën shërbimet dhe sistemet nuk mund të jenë funksionale, si dhe nuk janë planifikuar masa që në rast dështimi të një/disa pajisjeve të mos ndikohet në funksionimin e sistemeve dhe shërbimeve të ofruara;
    - Kontrolluesi nuk ka kryer auditime të brendshme me qëllim garantimin e mirëfunksionimit të këtyre teknikave për menaxhimin e riskut (ose në mungesë të teknikave, identifikim të riskut);
    - Politikat mbi gjurmët (*log*-et) për infrastrukturën mbështetëse TIK, nuk zbatohen sipas një procedure të rregulluar, me risk në qasje të paautorizuar në të dhëna, kërcënim të sigurisë në fushën e teknologjisë së informacionit dhe mungesë transparence.

    Gjithashtu, konstatohet se masat e ndërmarra në drejtim të *backup*-it janë të pamjaftueshme dhe nuk japin siguri në mbështetjen e planit të vazhdueshmërisë së biznesit (BCP) dhe planit të rimëkëmbjes nga katastrofa (DRP), në kundërshtim kjo me masat e sigurisë së informacionit. Nuk u gjetën procedurat e rikrijimit (*restore*) të *backup*-it të të dhënave me qëllim testimin e tyre për t'u siguruar që ato janë të efektshme dhe që mund të ekzekutohen brenda kohës së lejuar. Këto procedura duhet të testohen rregullisht, sistematikisht dhe vazhdimisht.

    Për sa më sipër, konstatohet se Kontrolluesi nuk ka marrë masa organizative dhe teknike të përshtatshme për të mbrojtur të dhënat personale nga shkatërrime të paligjshme, aksidentale, humbje aksidentale, për të mbrojtur aksesin ose përhapjen nga persona të paautorizuar, veçanërisht në këtë rast kur përpunimi i të dhënave kryhet nëpërmjet komunikimeve elektronike, në kundërshtim me parashikimet e nenit 28 të Ligjit dhe Vendimit nr. 6 të Komisionerit.

    Zyra e Komisionerit vlerëson se, mungesa e një plani të strukturuar për menaxhimin e riskut, e reflektuar në mos hartimin e procedurave për identifikimin, analizimin dhe vlerësimin e rreziqeve, si dhe në mungesën e auditimeve të brendshme dhe monitorimit të vazhdueshëm të masave të sigurisë, cenon drejtpërdrejt parimin e llogaridhënies sipas nenit 6 dhe detyrimet e nenit 28 të Ligjit. Pa një analizë të bazuar në risk, Kontrolluesi nuk është në gjendje të përcaktojë masa të përshtatshme teknike

dhe organizative, duke krijuar ekspozim të lartë ndaj incidenteve të sigurisë, aksesit të paautorizuar dhe përpunimeve të paligjshme të të dhënave personale.

Në të njëjtën kohë, mungesa e planeve të vazhdueshmërisë së biznesit (BCP) dhe e planeve të rikuperimit nga katastrofat (DRP), si dhe mos përcaktimi i parametrave kritikë, si koha maksimale e ndërprerjes së shërbimeve (RTO/RPO), tregojnë një mungesë të planifikimit për garantimin e disponueshmërisë dhe integritetit të të dhënave. Këto mangësi rrisin ndjeshëm rrezikun që, në rast dështimi teknik apo incidenti kibernetik, të dhënat personale të mos rikuperohen brenda një afati të pranueshëm ose të humbasin në mënyrë të pakthyeshme, duke cenuar të drejtat dhe interesat e subjekteve të të dhënave.

Gjithashtu, mungesa e procedurave të rregulluara për administrimin e *log*-eve dhe pamjaftueshmëria e masave të *backup*-it, e shoqëruar me mungesën e testimit të rregullt të rikthimit të të dhënave (*restore*), tregon se masat e sigurisë janë të paplota dhe jo efektive në praktikë. Në këto kushte, Kontrolluesi nuk garanton gjurmueshmërinë e veprimeve mbi të dhënat, transparencën dhe aftësinë për të reaguar ndaj incidenteve, duke qenë në kundërshtim me kërkesat e nenit 28 të Ligjit dhe Vendimit nr. 6 të Komisionerit.

9. Konstatohet se, aktivitetet kryesore të Kontrolluesit janë procese përpunimi, të cilat, për shkak të natyrës, fushës së zbatimit ose qëllimeve të tyre, kërkojnë monitorim të rregullt e sistematik të subjekteve të të dhënave në një shkallë të gjerë. Megjithatë, Kontrolluesi nuk ka emëruar një nëpunës të mbrojtjes së të dhënave personale, në kundërshtim me nenin 33 të Ligjit.

   Zyra e Komisionerit vlerëson se, aktivitetet e Kontrolluesit përfshijnë procese përpunimi të të dhënave personale që, për shkak të natyrës dhe mënyrës së realizimit të tyre, karakterizohen nga monitorim i vazhdueshëm i subjekteve të të dhënave. Konkretisht, përdorimi i sistemit të video-survejimit (CCTV) për mbikëqyrjen e ambienteve të punës dhe hapësirave përreth, si dhe publikimi i vazhdueshëm i imazheve dhe videove në rrjetet sociale, që përfshijnë punonjës, klientë dhe persona të tretë, përbëjnë forma të përpunimit të cilat realizohen në mënyrë të strukturuar dhe të përsëritur në kohë.

   Në këtë kuptim, këto procese përpunimi përbëjnë monitorim të rregullt dhe sistematik të subjekteve të të dhënave, pasi ato nuk janë të rastësishme apo sporadike, por pjesë integrale e ushtrimit të veprimtarisë së Kontrolluesit.

   Në këto kushte, në përputhje me nenin 33 të Ligjit, Kontrolluesi ka detyrimin për caktimin e një nëpunësi për mbrojtjen e të dhënave personale, i cili do të sigurojë mbikëqyrjen e respektimit të legjislacionit në fuqi dhe përputhshmërinë e proceseve përpunuese me kërkesat ligjore.

   Gjithashtu, bazuar në pikën 3, të nenit 34 të Ligjit, Kontrolluesi ka detyrimin për të publikuar të dhënat e nëpunësit të mbrojtjes së të dhënave, në mënyrë që subjektet e të dhënave të mund ta kontaktojnë atë, për të gjitha çështjet që lidhen me përpunimin

e të dhënave të tyre personale dhe ushtrimin e të drejtave të tyre, sipas këtij ligji, si dhe për t'ia njoftuar ato Zyrës së Komisionerit.

Në përfundim të hetimit administrativ, referuar provave dhe konstatimeve në vend, grupi i hetimit administrativ hartoi procesverbalin përkatës, një kopje e të cilit i është dërguar Kontrolluesit në rrugë postare dhe në formë elektronike.

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, është paraqitur në seancën dëgjimore, të datës 24.03.2026, të organizuar nga Zyra e Komisionerit, gjatë të cilës ka deklaruar angazhimin për rikuperimin e shkeljeve të konstatuara gjatë hetimit administrativ, si dhe bashkëpunimin me Komisionerin për të siguruar që çdo mangësi të adresohet në përputhje me Ligjin.

Gjithashtu, nga ana e Kontrolluesit, me shkresën e datës 19.03.2026, protokolluar pranë Zyrës së Komisionerit me nr. 410/5 prot., datë 24.03.2026, është përcjellë dokumentacioni mbi masat e marra në funksion të përmbushjes së detyrimeve të Ligjit dhe parashtrimeve lidhur me konstatimet e grupit të hetimit, si më poshtë:

- Lidhur me pikën 2 të procesverbalit të hetimit administrativ, Kontrolluesi pretendon se "*Pëlqimi*" është marrë vazhdimisht nga ana e punonjësve dhe lidhur me këtë ka përcjellë dokumentacion provues.

  Zyra e Komisionerit vlerëson se ky pretendim nuk qëndron. Veprimi i Kontrolluesit për të publikuar fotografi dhe video të punonjësve, pjesëmarrësve dhe subjekteve të tjera në profilet zyrtare në "*Facebook*" dhe "*Instagram*", pa marrë më parë pëlqimin e tyre, përbën shkelje të drejtpërdrejtë të parimeve themelore të mbrojtjes së të dhënave personale. Sipas neneve 6 dhe 7 të Ligjit, çdo përpunim i të dhënave personale duhet të jetë i ligjshëm, i drejtë dhe transparent, dhe të bazohet në një nga kushtet e përcaktuara. Gjithashtu, neni 8 i Ligjit përcakton qartë se pëlqimi duhet të jetë i lirë, i informuar dhe i shprehur qartë. Mungesa e këtij pëlqimi paraprak e bën përpunimin të paligjshëm, duke ekspozuar Kontrolluesin ndaj përgjegjësisë dhe duke cenuar të drejtën e subjekteve për privatësi.

- Lidhur me pikën 3 të procesverbalit të hetimit administrativ, nga ana e Kontrolluesit pretendohet se është ri pozicionuar planvendosja e kamerave të survejimit vetëm në drejtim të portës së hyrjes së ambientit, duke bashkëlidhur mbi këtë fakt fotot dhe provat përkatëse. Gjithashtu, lidhur me afatin e ruajtjes së pamjeve imazh/video nga ana e Kontrolluesit pretendohet se janë marrë masat përkatëse për respektimin e detyrimeve ligjore dhe reflektimin e tyre në rregulloren e përditësuar.

  Zyra e Komisionerit vlerëson se ky pretendim nuk qëndron. Së pari, disa kamera janë orientuar në mënyrë të tillë që monitorojnë ambiente të jashtme të ndërtesës, duke përfshirë rrugë kalimi dhe qytetarë të panjohur, si dhe ambiente të posteve të punës, në kundërshtim me pikën 2 të nenit 6 dhe nenin 7 të Ligjit, si dhe me

Udhëzimin nr. 3 dhe Udhëzimin nr. 11. Ky lloj monitorimi përpunon të dhëna personale të personave, që nuk kanë asnjë lidhje me veprimtarinë e Kontrolluesit, duke cenuar të drejtën e tyre për privatësi dhe duke shkelur parimin e proporcionalitetit. Së dyti, të dhënat imazhe/video ruhen përtej afatit ligjor prej 30 ditësh, në kundërshtim me parimin e ruajtjes në kohë sipas pikës 5 të nenit 6 të Ligjit dhe Udhëzimit nr. 3 të Komisionerit. Mbajtja e tyre më gjatë se sa është e nevojshme për përmbushjen e qëllimit të video-survejimit e bën përpunimin të paligjshëm, dhe në mungesë të shkatërrimit të menjëhershëm pas përfundimit të afatit, Kontrolluesi mban përgjegjësi për përpunimin e mëtejshëm.

- Lidhur me konstatimet në pikat 5 dhe 6, të procesverbalit, nga ana e Kontrolluesit janë marrë masat duke ndërtuar një domain controller me server dhe *Active Directory* ku çdo punonjës që ka akses në këtë sistem, ka kredencialet e tij dhe akses të kufizuar. Gjithashtu, është realizuar ruajtja e log-eve të sistemit nga vetë sistemi, i cili mban shënime (logs) lidhur me hyrjen dhe kohën e hyrjes në sistem.

  Zyra e Komisionerit vlerëson se ky pretendim nuk qëndron. Organizimi i rrjetit të brendshëm të intranetit nga Kontrolluesi paraqet dobësi serioze në sigurinë e të dhënave personale. Pajisjet kompjuterike nuk janë të qendërzuara sipas një modeli *domain controller*-i ose ekuivalent, duke sjellë mungesën e një arkitekture të unifikuar për administrimin e përdoruesve, autorizimeve dhe politikave të sigurisë. Kjo mënyrë organizimi rrit ndjeshëm rrezikun për akses të paautorizuar, mungesë të gjurmueshmërisë dhe dobësi në menaxhimin e privilegjeve, në kundërshtim me kërkesat e neneve 27 dhe 28 të Ligjit për garantimin e konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave personale.

  Për më tepër, masat e sigurisë teknike të përdorura për infrastrukturën e IT-së nuk i përgjigjen standardeve më të mira ndërkombëtare, duke mos ofruar mekanizma të avancuar filtrimi, monitorimi dhe parandalimi të ndërhyrjeve (si IPS/IDS). Kjo cenon kërkesën e nenit 28 të Ligjit për implementimin e masave teknike të përshtatshme në raport me rrezikun, duke ekspozuar të dhënat personale ndaj rreziqeve të shkatërrimit aksidental ose të paligjshëm, humbjes, ndryshimit, përhapjes së paautorizuar ose aksesit të paligjshëm.

- Lidhur me konstatimet në pikën 8 të procesverbalit, nga ana e Kontrolluesit është përgatitur Plani i *Backup*, Procedura e *Backup*, Analiza e Riskut, Masat teknike dhe organizative, informimi i subjekteve dhe trajnimi i stafit lidhur me detyrimet e reja ligjore, me qëllim shmangien e çdo incidenti të mundshëm në të ardhmen.

  Zyra e Komisionerit vlerëson se ky pretendim nuk qëndron. Kontrolluesi nuk ka zbatuar një sistem të strukturuar dhe të dokumentuar për menaxhimin e riskut lidhur me përpunimin e të dhënave personale, duke shkelur parimin e llogaridhënies sipas nenit 6 dhe detyrimet e nenit 28 të Ligjit. Konkretisht, mungojnë identifikimi, analizimi dhe vlerësimi i rreziqeve, si dhe teknikat përkatëse të menaxhimit dhe monitorimit të masave të sigurisë. Gjithashtu, nuk ekziston asnjë plan i vazhdueshmërisë së biznesit (BCP) apo plan i rimëkëmbjes nga katastrofa (DRP),

duke përfshirë përcaktimin e kohës maksimale të lejuar të ndërprerjes së shërbimeve.

Në përfundim u vlerësua se, shkeljet e konstatuara gjatë procesit të hetimit administrativ, të tilla si: mos dokumentimi për veprimtaritë përpunuese të Kontrolluesit në funksion të përputhshmërisë me Ligjin; mungesa e masave tekniko-organizative; mos zbatimi i detyrimit për konfidencialitetin dhe caktimin e nëpunësit për mbrojtjen e të dhënave personale, në kuptim të shkronjës "a", të pikës 1, të nenit 94 të Ligjit, si dhe shkelja e parimeve dhe kritereve ligjore të përpunimit të të dhënave personale, në kuptim të shkronjës "a", të pikës 2, të nenit 94 të Ligjit, përbëjnë kundërvajtje administrative dhe sanksionohen me gjobë, si më poshtë:

"*1. Bazuar edhe në rrethanat e përcaktuara në pikën 2 të nenit 93 të këtij ligji, përbëjnë kundërvajtje administrative dhe dënohen me gjobë deri në 1 000 000 000 (një miliard) lekë, ose në rastin e një shoqërie tregtare deri në 2% të xhiros totale vjetore globale për vitin financiar paraardhës, cilado është më e lartë, shkeljet e detyrimeve:*
a) të kontrolluesit dhe përpunuesit, sipas neneve 8, pika 6, e 11, të kapitullit III, të pjesës II të këtij ligji, me përjashtim të nenit 22 të këtij ligji;

2. Bazuar edhe në rrethanat e përcaktuara në pikën 2 të nenit 93, përbëjnë kundërvajtje administrative dhe dënohen me gjobë deri në 2 000 000 000 (dy miliardë) lekë, ose në rastin e një shoqërie tregtare, deri në 4% të xhiros totale vjetore globale për vitin financiar paraardhës, cilado që është më e lartë, shkeljet e mëposhtme:

a) moszbatimi i parimeve themelore të përpunimit, përfshirë kushtet për dhënien e pëlqimit, sipas neneve 6, 7, 8 e 9, të këtij ligji;

Në këto kushte, Komisioneri vlerësoi se, dokumentacioni i paraqitur nuk përmbush kërkesat e parashikuara nga Ligji dhe nuk mund të konsiderohet si provë e mjaftueshme për të vërtetuar ekzistencën e masave të nevojshme organizative dhe teknike që Kontrolluesi ka detyrimin të zbatojë, në përputhje me legjislacionin në fuqi. Rrjedhimisht, aktet e referuara nuk prodhojnë efekt juridik për qëllime të zbatimit të Ligjit.

Në rrethanat e shqyrtimit të kësaj çështje, Komisioneri evidenton shkallën e bashkëpunimit nga ana e Kontrolluesit. Gjithashtu, në llogaritjen e masës së sanksionit administrativ me gjobë, Komisioneri ka marrë në konsideratë xhiron vjetore të deklaruar nga Kontrolluesi, si dhe rëndësinë e proceseve përpunuese.

Sa më sipër, mbështetur në dispozitat e Udhëzimit nr. 06, datë 16.07.2025, "*Për miratimin e metodologjisë për përllogaritjen e masës së sanksioneve administrative*", veçanërisht në pikat 4 dhe 5, të Nënkapitullit 2.1 të Kapitullit 2 dhe të Kapitullit 4, Komisioneri ka vlerësuar në mënyrë të drejtë dhe transparente masën e sanksionit administrativ ndaj Kontrolluesit, sipas përcaktimeve të neneve 93 dhe 94 të Ligjit, duke u bazuar në kufijtë minimalë të përllogaritjes.

Komisioneri vlerëson faktin se, shkeljet e konstatuara janë serioze. Ato lidhen me garantimin e parimeve dhe kritereve për përpunimin e ligjshëm të të dhënave, si dhe marrjen e masave të përshtatshme tekniko-organizative për sigurinë e të dhënave

personale. Gjithashtu, vendimi i Komisionerit bazohet në mënyrën e reagimit të Kontrolluesit për rikuperimin e shkeljeve të konstatuara.

PËR KËTO ARSYE:

Në zbatim të neneve 6, 7, 8, 27, 28, 30, 33, 81-84, pikës 1 të nenit 87, nenit 93, shkronjës "a" të pikës 1 dhe shkronjës "a" të pikës 2 të nenit 94, si dhe nenit 95 të Ligjit, dhe të ligjit nr. 49/2012 "*Për gjykatat administrative dhe gjykimin e mosmarrëveshjeve administrative*", i ndryshuar, si dhe ligjit nr. 10279, datë 20.05.2010 "*Për kundërvajtjet administrative*", Komisioneri,

V E N D O S I:

1. Dënimin e Kontrolluesit Shoqëria "*Loft Construction*" shpk, me gjobë në masën **1,010,000** (një milion e dhjetë mijë) Lekë, për shkelje të neneve 6, 7 dhe 8 të Ligjit;

2. Dënimin e Kontrolluesit Shoqëria "*Loft Construction*" shpk, me gjobë në masën **707,000** (shtatë qind e shtatë mijë) Lekë, për shkelje të neneve 27, 28, 30 dhe 33 të Ligjit;

3. Kontrolluesi, Shoqëria "*Loft Construction*" shpk, urdhërohet të marrë masa për marrjen dhe administrimin e "*Pëlqimit*" të subjekteve të të dhënave në përputhje me parimet dhe kriteret ligjore të sanksionuara në nenet 6, 7 dhe 8 të Ligjit;

4. Kontrolluesi, Shoqëria "*Loft Construction*" shpk, urdhërohet të marrë masa për përcaktimin e planeve të kamerave përmes sistemit të video-survejimit (CCTV), si dhe përcaktimin e afateve kohore për ruajtjen e të dhënave, për të gjithë proceset e përpunimit, 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;

5. Kontrolluesi, Shoqëria "*Loft Construction*" shpk, në zbatim të nenit 27 dhe 28 të Ligjit, urdhërohet të marrë masa për përditësimin e rregullores "*Për mbrojtjen e të dhënave personale*", duke parashikuar në të, 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, përcaktimin e niveleve të aksesit, afatet e ruajtjes, etj.;

6. Kontrolluesi, Shoqëria "*Loft Construction*" shpk, në zbatim të nenit 30 të Ligjit, duhet të reflektojë në mënyrë të qartë dhe të drejtë detyrimet dhe përgjegjësitë në "*Deklaratën e Konfidencialitetit*" me punëmarrësit të cilët kanë akses në mbledhjen, përpunimin dhe ruajtjen e të dhënave personale;

7. Kontrolluesi, Shoqëria "*Loft Construction*" shpk, urdhërohet të marrë masa për caktimin e nëpunësit për mbrojtjen e të dhënave personale, sipas parashikimeve të neneve 33 dhe 34 të Ligjit, si dhe të njoftojë Zyrën e Komisionerit për caktimin e tij;

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

   (i) menjëherë - detyrimin e përcaktuar në pikën 4) të dispozitivit të këtij vendimi;
   (ii) vazhdimisht - detyrimin e përcaktuar në pikën 3) të dispozitivit të këtij vendimi;
   (iii) brenda 15 (pesëmbëdhjetë) ditëve - detyrimin e përcaktuar në pikën 5) të dispozitivit të këtij vendimi;
   (iv) brenda 30 (tridhjetë) ditëve - detyrimet e përcaktuara në pikat 6) dhe 7) të dispozitivit të këtij vendimi;

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

9. Kontrolluesi, Shoqëria "*Loft Construction*" shpk, duhet të njoftojë Komisionerin për masat e marra brenda 60 (gjashtëdhjetë) ditëve, duke filluar nga data e marrjes dijeni të këtij vendimi;

10. Vendimi për dënimin me gjobë përbën "titull ekzekutiv" dhe zbatohet nga kundërvajtësi (Kontrolluesi), brenda 10 (dhjetë) ditëve nga data e njoftimit. Për ekzekutimin e gjobës ngarkohet shërbimi përmbarimor gjyqësor;

11. Kundër këtij Vendimi mund të bëhet ankim në Gjykatën Administrative të Shkallës së Parë Tiranë, brenda 45 (dyzetë e pesë) ditëve nga data e njoftimit.

Ky Vendim u shpall sot, më datë 28.04.2026.

KOMISIONERI

Besnik Dervishi