Nr. 2482/6 prot. Tiranë, më 05.11.2026

REKOMANDIM

Nr. 68, datë 05.11.2026

PËR KONTROLLUESIN, SHOQËRIA "UJËSJELLËS KANALIZIME TIRANË" SHA

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"), si dhe provave të administruara në ngarkim të Kontrolluesit "Ujësjellës Kanalizime Tiranë sh.a." (në vijim "Kontrolluesi"),

KONSTATOHET SE:

Në zbatim të Urdhrit nr. 168, datë 03.09.2026, të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim "Komisioneri"), u krye hetimi 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 hetimit administrativ dhe provat e administruara gjatë ushtrimit të hetimit pranë Kontrolluesit, vëren se:

1. Kontrolluesi është i regjistruar në Qendrën Kombëtare të Biznesit me NUIS L72320033P, me objekt aktiviteti "*Objekti i shoqërisë brenda territorit të bashkisë së krijuar sipas ligjit nr. 115/2014 "Për ndarjen administrative-territoriale të njësive të qeverisjes vendore në Republikën e Shqipërisë" është shërbimi i furnizimit me ujë të pijshëm i konsumatorëve dhe shitja e tij, mirëmbajtja e sistemit/sistemeve të furnizimit me ujë të pijshëm si dhe të impianteve të pastrimit etj.*"

   Ujësjellës Kanalizime Tiranë sh.a. është një shoqëri aksionare, e cila brenda territorit të bashkisë Tiranë ka për objekt të aktivitetit shërbimin e furnizimit me ujë të pijshëm të

konsumatorëve si dhe shitjen e tij, mirëmbajtjen e sistemeve të furnizimit me ujë të pijshëm dhe impianteve të pastrimit të tyre, prodhimi ose blerja e ujit për plotësimin e kërkesës së konsumatorëve etj. Shoqëria e ushtron veprimtarinë e saj në përputhje me lejet, autorizimet dhe licencat sipas legjislacionit në fuqi.

Në kuadër të veprimtarisë që ushtron, Kontrolluesi mbledh dhe përpunon të dhëna personale për kategorinë e të dhënave "personel", "abonentë/konsumatorë", "vizitorë" etj. Përpunimi i të dhënave personale kryhet në mënyrë manuale dhe elektronike.

2. Nga verifikimi i dokumentacionit të administruar në dosjet e personelit aktual dhe të larguar, ndër të tjera, rezulton se shoqëria administron edhe "certifikatë familjare" të nëpunësit. Nga shqyrtimi i rregullores së posaçme të shoqërisë "*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale në shoqërinë "Ujësjellës Kanalizime Tiranë" sh.a.*" nuk rezultoi që mbledhja dhe administrimi i kësaj kategorie të dhënash të jetë e parashikuar shprehimisht si pjesë e dokumentacionit të nevojshëm për administrimin e marrëdhënies së punës.

   Mbledhja dhe ruajtja e të dhënave që përmbahen në certifikatën familjare, përtej nevojës konkrete dhe pa një qëllim të përcaktuar të përpunimit, mund të çojë në përpunimin e të dhënave personale që nuk janë të nevojshme për qëllimin e administrimit të marrëdhënies së punës, në kundërshtim me parashikimet e pikës 3 të nenit 6 të Ligjit.

   Zyra e Komisionerit vlerëson se Kontrolluesi gjatë proceseve përpunuese duhet të vlerësojë përputhshmërinë me parimin e minimizimit të të dhënave, në kuptim të mbledhjes dhe përpunimit vetëm të atyre të dhënave që janë të përshtatshme, përkatëse dhe të domosdoshme në raport me qëllimin e përpunimit. Në këtë kuadër, duhet të analizohet nëse mbledhja dhe përpunimi i "certifikatës familjare" të nëpunësit është i justifikuar në çdo rast, pasi jo në të gjitha pozicionet e punës një e tillë është e nevojshme dhe proporcionale.

3. Konstatohet se procesi i lidhjes së kontratës me abonentin fillon me plotësimin e formularit të aplikimit. Nga shqyrtimi i formularit të vënë në dispozicion rezulton se në të mblidhen dhe përpunohen të dhëna personale, duke përfshirë ndër të tjera "emrin", "atësinë", "mbiemrin", "adresën e plotë", si dhe "kopje të certifikatës së pronësisë", "kontratës së shitblerjes/dhurimit/shërbimit" dhe "mjetit të identifikimit". Grupi i hetimit administrativ konstaton se Kontrolluesi nuk ka parashikuar në formularin e regjistrimit klauzolë informuese për mbledhjen dhe përpunimin e të dhënave personale të abonentit, në kundërshtim me nenet 13 dhe 14 të Ligjit.

   Zyra e Komisionerit vlerëson se sipas parashikimeve të nenit 13 të Ligjit, Kontrolluesi duhet të garantojë informimin e subjekteve të të dhënave personale lidhur me identitetin dhe të dhënat e kontaktit të Kontrolluesit, qëllimet dhe bazën ligjore të përpunimit, afatet e ruajtjes së tyre, të drejtat që gëzojnë subjektet e të dhënave personale, si dhe çdo informacion tjetër të kërkuar nga dispozitat përkatëse të Ligjit.

   Gjithashtu, Kontrolluesi duhet të sigurojë që informacioni në përpunimin e të dhënave personale t'u vihet në dispozicion subjekteve të të dhënave në momentin e mbledhjes së të dhënave, duke garantuar respektimin e parimit të ligjshmërisë.

4. Veprimtaria e Kontrolluesit për përpunimin e të dhënave personale realizohet, ndër të tjera, nëpërmjet sistemit elektronik "SMI Al-Billing/UKTSMI", i cili përdoret për administrimin e abonentëve, kontratave, faturimit, arkëtimeve, detyrimeve, leximeve të matësve, aktmarrëveshjeve, ankesave dhe proceseve të tjera të lidhura me ofrimin e shërbimit.

   Nga dokumentacioni teknik i administruar rezulton se sistemi përfshin bazën *Oracle uktsmi*, *skemat ukreader*, *uktbank*, *uktonline*, *ws* dhe *wstest*, aplikacionin *UK Reader*, shërbimet *online*, si dhe *webservice*-et e pagesave dhe integrimeve.

   Nëpërmjet këtij sistemi përpunohen kategori të ndryshme të të dhënave personale të abonentëve, përfshirë të dhëna identifikuese, NID, të dhëna kontakti dhe adrese, numrin e kontratës, të dhëna mbi matësin dhe konsumin, të dhëna mbi faturimin, pagesat dhe detyrimet financiare, aktmarrëveshjet, ankesat/kërkesat, informacionin mbi aksesin *online* dhe, sipas rastit, koordinatat e pikës së shërbimit.

   Moduli "Abonenti 360°" mundëson konsultimin e integruar të informacionit të abonentit/kontratës, faturave dhe pagesave, aktmarrëveshjeve, aksesit *online* dhe pozicionit të kontratës në hartë, kur për kontratën janë regjistruar koordinata. Sistemi parashikon gjithashtu funksionalitete për printimin dhe eksportimin e informacionit.

   Nga dokumentacioni i administruar rezulton se Kontrolluesi ka përcaktuar një procedurë për administrimin e aksesit, sipas së cilës aksesi i ri, ndryshimi i aksesit dhe çaktivizimi realizohen mbi bazën e kërkesës së dokumentuar dhe miratimit përkatës. Parashikohet gjithashtu çaktivizimi i llogarive në rast largimi, transferimi, përfundimi të afatit, pezullimi ose incidenti sigurie. Për administrimin e aksesit përdoret formulari "Kërkesë për akses në sistem", nëpërmjet të cilit përcaktohen të drejtat e kërkuara për funksionalitetet e sistemit dhe miratimi i tyre nga strukturat përgjegjëse.

   Sistemi përdor model aksesi të bazuar në role (*Role-Based Access Control – RBAC*). Sipas dokumentacionit të administruar, rezultojnë 157 role aktive, 157 forma aktive, 257 përdorues aktivë me role dhe 2,643 lidhje aktive përdorues-rol. Në dokumentacion janë identifikuar gjithashtu role kritike të lidhura me administrimin e përdoruesve, konfigurimet, tarifat, faturimin, anulimet, arkëtimin, pagesat kreditore, raportet financiare dhe auditimin.

   Gjithashtu, sistemi disponon mekanizma për regjistrimin e hyrjeve, daljeve, sesioneve dhe ndryshimeve të rëndësishme, ndërsa *tbllogu*, *tblaudit_event* dhe *tblaudit_detail* identifikohen si burime të evidencës teknike. Nëpërmjet funksionaliteteve "Aktiviteti i përdoruesve" dhe "Audit Sistemi" mund të konsultohen elemente të aktivitetit të përdoruesve dhe veprimet e realizuara në sistem, përfshirë, sipas rastit, përdoruesin, adresën IP, periudhën, kontratën, tabelën e databazës dhe operacionet *insert*, *update* dhe *delete*.

   Nga verifikimi i sistemit dhe dokumentacionit të administruar, në lidhje me masat teknike dhe organizative për mbrojtjen e të dhënave personale, konstatohet se:

- megjithëse është dokumentuar procedura për administrimin e aksesit dhe sistemi përdor model aksesi të bazuar në role, nuk u administruan procedura të rishikimeve periodike të 257 përdoruesve aktivë dhe 2,643 lidhjeve aktive përdorues-rol, nëpërmjet të cilave të evidentohet se të drejtat e aksesit vijojnë të jenë të nevojshme dhe në përputhje me funksionet aktuale të përdoruesve;
- nuk u administruan procedura që të dokumentojnë kryerjen periodike të rishikimit dhe ricertifikimit të të drejtave të aksesit (*access review/access recertification*), përfshirë identifikimin dhe heqjen e të drejtave që nuk rezultojnë më të nevojshme;
- megjithëse dokumentacioni identifikon role kritike, nuk u administruan procedura të rishikimeve periodike të llogarive me privilegje të larta, përdoruesve që i disponojnë këto role dhe vijimit të nevojës për privilegjet përkatëse;
- nuk u administrua një analizë apo evidencë e dokumentuar mbi ndarjen e detyrave, veçanërisht në lidhje me mundësinë e kombinimit në të njëjtën llogari të funksioneve që lidhen me administrimin e përdoruesve, konfigurimin, faturimin, anulimin, arkëtimin, pagesat dhe auditimin;
- nuk u administruan procedura të rishikimeve periodike nëpërmjet të cilave të dokumentohet zbatimi i parimit të privilegjit minimal (*least privilege*) për përdoruesit e sistemit;
- megjithëse për autorizimin e aksesit përdoret formular i posaçëm, nuk u administruan raporte ose procesverbale periodike të rakordimit ndërmjet të drejtave të miratuara dhe privilegjeve faktikisht aktive në sistem, me qëllim evidentimin e aksesit të tepërt, të papërdorur ose të mbetur aktiv pas ndryshimit të funksionit;
- megjithëse sistemi disponon funksionalitete për regjistrimin dhe auditimin e aktivitetit, nuk u administrua dokumentacion i plotë mbi afatin e ruajtjes së *log*-eve, kategoritë e ngjarjeve që regjistrohen, masat për mbrojtjen e *log*-eve nga ndryshimi ose fshirja, personat që kanë akses në to dhe periodicitetin e kontrollit të tyre;
- nuk disponohen raporte periodike të analizimit dhe monitorimit të *log*-eve që të evidentojnë kontrollin e aksesimeve të pazakonta, tentativave të dështuara të autentikimit, veprimeve të përdoruesve me privilegje të larta, ndryshimeve masive ose operacioneve të tjera anormale;
- sistemi mundëson printimin dhe eksportimin e informacionit, përfshirë eksportimin në Excel, ndërsa nuk u administrua evidencë e plotë mbi kufizimin e këtyre funksionaliteteve sipas rolit, regjistrimin e veprimeve të eksportimit dhe kontrollin e mëtejshëm të të dhënave personale pas eksportimit nga sistemi;
- nuk u administrua dokumentacion që të përcaktojë afatet e ruajtjes sipas kategorive të të dhënave personale që administrohen në SMI Al-Billing, si dhe mekanizmat teknikë për fshirjen, anonimizimin ose arkivimin e tyre pas përfundimit të afatit përkatës;
- nuk u administrua evidencë mbi mekanizmat e enkriptimit të të dhënave gjatë transmetimit, përfshirë komunikimet ndërmjet aplikacionit, databazës, shërbimeve *online* dhe sistemeve të integruara;
- nuk disponohen evidenca të mjaftueshme mbi mbrojtjen e të dhënave të ruajtura, përfshirë databazën dhe kopjet rezervë, si dhe, në rast përdorimi të enkriptimit, mbi administrimin dhe mbrojtjen e çelësave kriptografikë;
- duke marrë në konsideratë se arkitektura e dokumentuar përfshin skemat *ukreader*, *uktbank*, *uktonline*, *ws* dhe *wstest*, nuk u administrua dokumentacion i plotë mbi

llogaritë teknike/*service accounts*, qëllimin, privilegjet, kredencialet, afatet e vlefshmërisë dhe mënyrën e monitorimit të përdorimit të tyre;

- nuk u administruan procedura të plota mbi kufizimin, monitorimin dhe auditimin e aksesit të llogarive teknike dhe të integrimeve aplikacion-aplikacion, përfshirë *webservice*-et e pagesave dhe integrimeve;
- nuk u administrua dokumentacion mbi mekanizmat e autentikimit dhe autorizimit të *webservice*-eve/API-ve, mënyrën e mbrojtjes së kredencialeve dhe gjurmueshmërinë e kërkesave të realizuara nëpërmjet tyre;
- duke marrë në konsideratë ekzistencën e komponentit/skemës WSTEST, nuk u administrua dokumentacion i plotë mbi ndarjen logjike dhe teknike të mjedisit të testimit nga mjedisi i prodhimit;
- nuk u administrua evidencë që të përcaktojë nëse në mjediset e zhvillimit dhe testimit përdoren të dhëna reale personale dhe, në rast përdorimi të tyre, masat e zbatuara për kufizimin, maskimin, pseudonimizimin ose anonimizimin e këtyre të dhënave;
- nuk disponohet dokumentacion mbi procesin e menaxhimit të cenueshmërive teknike, përfshirë identifikimin e cenueshmërive, klasifikimin sipas nivelit të rrezikut, përcaktimin e afateve për korrigjimin e tyre dhe verifikimin pas korrigjimit;
- nuk disponohen raporte periodike të *vulnerability assessment* dhe/ose *penetration testing* për aplikacionin, databazën, shërbimet *web* dhe komponentët e tjerë të ekspozuar të sistemit;
- nuk u administruan procedura mbi procesin e menaxhimit të përditësimeve dhe *patch*-eve të sigurisë (*patch management*), përfshirë identifikimin e përditësimeve kritike, afatet e instalimit, testimin paraprak dhe verifikimin e instalimit të tyre;
- nuk u administrua evidencë mbi konfigurimin bazë të sigurisë (*security hardening*) të serverëve, databazës dhe komponentëve aplikativë, si dhe mbi rishikimin periodik të këtij konfigurimi;
- nuk disponohen procedura mbi krijimin dhe administrimin e kopjeve rezervë (*backup*), përfshirë periodicitetin, përmbajtjen, vendndodhjen e ruajtjes, afatin e mbajtjes, kufizimin e aksesit dhe mbrojtjen e tyre;
- nuk u administruan rezultate të testeve periodike të rikthimit nga kopjet rezervë (*restore testing*), nëpërmjet të cilave të evidentohet aftësia faktike për rikthimin e disponueshmërisë dhe aksesit në të dhënat personale pas një incidenti fizik ose teknik;
- nuk disponohen procedura të testimit periodik të mekanizmave të *Business Continuity*/*Disaster Recovery*, nëpërmjet të cilave të dokumentohet aftësia për rikthimin e funksionimit të SMI Al-Billing dhe komponentëve të tij kritikë pas një incidenti;
- nuk disponohen procedura mbi aksesin në distancë të zhvilluesve, mirëmbajtësve ose palëve të treta, përfshirë autorizimin paraprak, mekanizmin e autentikimit, kohëzgjatjen e aksesit, kufizimin e privilegjeve dhe regjistrimin/monitorimin e sesioneve;
- nuk disponohen procedura mbi procesin e menaxhimit të incidenteve të sigurisë që lidhen me SMI Al-Billing, përfshirë identifikimin, regjistrimin, klasifikimin, përshkallëzimin, trajtimin dhe dokumentimin e tyre;
- nuk u administruan procedura të mjaftueshme mbi testimin, vlerësimin dhe analizimin periodik të efektivitetit të masave teknike dhe organizative të zbatuara për sistemin.

Për sa më sipër, konstatohet se Kontrolluesi, pavarësisht përdorimit të një sistemi elektronik nëpërmjet të cilit administrohet një volum i konsiderueshëm të dhënash personale të abonentëve, nuk disponon një kuadër të dokumentuar të masave teknike-organizative për administrimin dhe sigurinë e këtij përpunimi, si dhe nuk rezulton të ketë dokumentuar në mënyrë të mjaftueshme masat e ndërmarra për të garantuar dhe demonstruar përputhshmërinë e veprimtarive të përpunimit me kërkesat e neneve 27 dhe 28 të Ligjit.

Gjithashtu, mungesa e procedurave të dokumentuara për administrimin e përdoruesve dhe privilegjeve, kontrollin dhe rishikimin e aksesit, regjistrimin dhe monitorimin e veprimeve, menaxhimin e incidenteve, cenueshmërive dhe përditësimeve, krijimin dhe rikthimin e kopjeve rezervë, vazhdimësinë e funksionimit, ruajtjen dhe fshirjen e të dhënave, si dhe testimin dhe vlerësimin periodik të efektivitetit të masave të sigurisë, nuk garanton në mënyrë të dokumentuar një nivel sigurie të përshtatshëm me rrezikun e përpunimit, në raport me natyrën, objektin, kontekstin dhe qëllimet e përpunimit të të dhënave personale, sipas kërkesave të nenit 28 të Ligjit.

Zyra e Komisionerit vlerëson se ndërthurja në sistemin "SMI Al-Billing/UKTSMI" e të dhënave identifikuese, të kontaktit dhe kontraktore me të dhënat mbi konsumin, vendndodhjen dhe fotografitë e matësve, kërkon masa teknike dhe organizative të përshtatura me rreziqet e këtij përpunimi. Lidhja e këtyre informacioneve me një abonent konkret mundëson krijimin e një pasqyre të detajuar mbi marrëdhënien e tij me shërbimin, ndërsa aksesimi, ndryshimi ose përhapja e paautorizuar e tyre mund të cenojë privatësinë dhe të sjellë pasoja në administrimin e kontratës, saktësinë e faturimit dhe trajtimin e pretendimeve të abonentit. Për këtë arsye, përcaktimi i rregullave për përdorimin e sistemit, kufizimi i aksesit sipas detyrave funksionale dhe kontrolli i veprimeve të përdoruesve janë të nevojshme për të parandaluar përdorimin e të dhënave përtej qëllimeve të autorizuara dhe për të mundësuar identifikimin e përgjegjësive në rast parregullsish.

Gjithashtu, siguria e përpunimit duhet të mbulojë të gjithë rrjedhën e të dhënave, nga mbledhja në terren dhe transmetimi drejt sistemit qendror, deri te ruajtja, konsultimi, eksportimi dhe fshirja e tyre. Dokumentimi i arkitekturës teknike, pajisjeve të përdorura, vendndodhjes së të dhënave dhe akseseve të ofruesve të jashtëm është i nevojshëm për të identifikuar pikat e ekspozimit dhe për të përcaktuar masat mbrojtëse përkatëse. Në të njëjtën kohë, menaxhimi i cenueshmërive dhe përditësimeve, mbrojtja e komunikimit, krijimi dhe testimi i kopjeve rezervë, si dhe procedurat për trajtimin e incidenteve dhe rikuperimin e sistemit shërbejnë për të zvogëluar rrezikun e zbulimit, ndryshimit, humbjes ose pamundësisë së aksesimit të të dhënave. Përshtatshmëria e këtyre masave duhet të mbështetet në një vlerësim të dokumentuar të rrezikut, përfshirë nevojën për mekanizma shtesë autentikimi dhe mbrojtjeje.

Në këtë kuadër, Zyra e Komisionerit vlerëson se mungesat e evidentuara në dokumentacion kufizojnë mundësinë e Kontrolluesit për të provuar se administrimi dhe siguria e sistemit realizohen në mënyrë të qëndrueshme, të kontrollueshme dhe të verifikueshme. Politikat dhe procedurat duhet të përcaktojnë përgjegjësi konkrete, rregulla veprimi dhe mekanizma kontrolli, ndërsa zbatimi i tyre duhet të provohet

nëpërmjet evidencave përkatëse dhe të vlerësohet periodikisht. Mungesa e dokumentimit nuk provon vetvetiu mungesën e çdo mekanizmi teknik mbrojtës, por nuk mundëson verifikimin e zbatimit, vazhdimësisë dhe efektivitetit të tij. Për rrjedhojë, formalizimi, zbatimi dhe rishikimi i këtyre masave janë të nevojshme për të adresuar mangësitë e konstatuara dhe për të garantuar e demonstruar përputhshmërinë e përpunimit me kërkesat e neneve 27 dhe 28 të Ligjit.

Gjithashtu, 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, të Komisionerit "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 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 nevojshme 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 Udhëzimet nr. 08 dhe nr. 09. Në rastin konkret, Zyra e Komisionerit vlerëson 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, të mirëmbajë dhe të 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.

5. Kontrolluesi ka nënshkruar një kontratë shërbimi me shoqërinë "Union Financiar Tiranë" sh.a., datë 04.05.2016, me objekt "*Kryerja nga ofruesi i shërbimit për llogari të UKT e shërbimit të arkëtimit të faturave të ujit të klientëve familjarë dhe jofamiljarë, duke përfshirë kamatëvonesat* ".

   Nga analizimi i përmbajtjes së kontratës së mësipërme konstatohet se nuk specifikohen masat konkrete tekniko-organizative të detyrueshme për t'u zbatuar nga ana e

përpunuesit, me qëllim garantimin e sigurisë dhe përpunimit të ligjshëm të të dhënave personale, si dhe nuk janë reflektuar detyrimet sipas parashikimeve në nenin 26 të Ligjit dhe Udhëzimin nr. 19 të Komisionerit, datë 03.08.2012 "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", të ndryshuar (në vijim "Udhëzimi nr. 19").

Zyra e Komisionerit vlerëson se çdo delegim i përpunimit të të dhënave personale duhet të realizohet përmes një kontrate të shkruar dhe të detajuar, e cila përcakton qëllimin e përpunimit, kategoritë e të dhënave, masat e sigurisë që do të zbatojë përpunuesi, përgjegjësitë ligjore dhe procedurat për kontrollin dhe raportimin. Kjo siguron që delegimi të jetë në përputhje me legjislacionin në fuqi, në mënyrë që të sigurohet që përpunuesi të garantojë përpunim të ligjshëm dhe të sigurt të të dhënave, sipas parashikimeve të nenit 26 të Ligjit.

6. Kontrolluesi ka vënë në dispozicion të grupit të hetimit administrativ "*Rregulloren për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale në Shoqërinë Ujësjellës Kanalizime Tiranë sh.a.*". Megjithatë, nga shqyrtimi i përmbajtjes së këtyre akteve konstatohet se në to nuk janë të parashikuara rregulla specifike mbi kategoritë e të dhënave personale që përpunon Kontrolluesi gjatë ushtrimit të veprimtarisë dhe procedura organizative mbi mënyrën e përpunimit të tyre, si mënyra e mbledhjes, regjistrimit, ruajtjes dhe asgjësimit të tyre, sigurinë e të dhënave personale, aksesin në të dhënat personale etj., sipas parashikimeve të neneve 27 dhe 28 të Ligjit, me qëllim garantimin e përpunimit të ligjshëm dhe sigurisë së të dhënave, në përputhje me proceset përpunuese që kryen.

   Zyra e Komisionerit vlerëson se përshtatja dhe plotësimi i dokumentit "*Rregullore për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale në Shoqërinë Ujësjellës Kanalizime Tiranë sh.a.*", me të gjitha elementet ligjore të përcaktuara në pikën 1 të nenit 27 të Ligjit, konsiderohet një detyrim shumë i rëndësishëm, në zbatim të neneve 27 dhe 28 të Ligjit, për të mundësuar shmangien e pasojave të rënda që mund të vijnë për subjektet e të dhënave.

   Gjithashtu, në aktet e brendshme 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.

7. 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 caktimi i një nëpunësi për mbrojtjen e të dhënave personale është një detyrim i rëndësishëm, që ka për qëllim garantimin e sigurisë së të

dhënave personale gjatë proceseve përpunuese, që realizohen nga ana e Kontrolluesit gjatë ushtrimit të veprimtarisë së tij.

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 28.10.2026, të organizuar nga Zyra e Komisionerit, gjatë së 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, gjatë seancës dëgjimore është dorëzuar dokumenti "*Oracle database backup and recovery configuration document*".

Me shkresën nr. 17096/3 prot., datë 28.10.2026, administruar me tonën me nr. 2482/5 prot., datë 28.10.2026, Kontrolluesi ka paraqitur pretendimet ndaj procesverbalit të hetimit administrativ, si vijon:

- Lidhur me konstatimin në pikën 2 të procesverbalit, Kontrolluesi pretendon se: *"Nuk ka vendosur si praktikë të përgjithshme kërkimin e certifikatës familjare për të gjithë punonjësit dhe nuk e aplikon një kërkesë të tillë në mënyrë sistematike. Prania e këtij dokumenti në disa dosje të personelit lidhet me dokumentacionin e administruar në raste të veçanta, përfshirë rastet kur dokumenti është paraqitur nga vetë punonjësi dhe nuk dëshmon në vetvete ekzistencën e një detyrimi të përgjithshëm për paraqitjen e tij. Administrimi i certifikatës familjare ka pasur për qëllim ndihmën dhe saktësimin dhe verifikimin e të dhënave identifikuese të punonjësi, përfshirë atësinë dhe adresën e banimit, kur këto të dhëna janë të nevojshme për komunikimin dhe dërgimin e njoftimeve zyrtare, si dhe bashkëpunimin e institucionit në rastet e proceseve gjyqësore".*

Zyra e Komisionerit vlerëson se ky pretendim nuk qëndron. *Së pari*, pretendimi i Kontrolluesit se administrimi i certifikatës familjare nuk përbën një praktikë të përgjithshme apo sistematike nuk e përjashton atë nga detyrimi për të garantuar përputhshmërinë e çdo veprimtarie përpunimi me kërkesat e Ligjit. Në këtë kuptim, pavarësisht numrit të dosjeve në të cilin është konstatuar prezenca e këtij dokumenti apo mënyrës së sigurimit të tij, Kontrolluesi ka detyrimin të identifikojë dhe të justifikojë qëllimin konkret të përpunimit, bazën ligjore përkatëse, domosdoshmërinë e administrimit dhe afatin e ruajtjes së të dhënave personale.

Së dyti, lidhur me argumentin se certifikata familjare është administruar për verifikimin e të dhënave identifikuese, atësisë dhe adresës së banimit të punonjësve, Zyra e Komisionerit vlerëson se ky dokument përmban një kategori më të gjerë të dhënash personale sesa ato që rezultojnë të nevojshme për realizimin e qëllimeve të deklaruara. Konkretisht, certifikata familjare përmban edhe të dhëna personale të anëtarëve të tjerë të familjes, të cilët nuk janë pjesë e marrëdhënies së punës me Kontrolluesin. Për rrjedhojë, administrimi i këtij dokumenti, në mungesë të një nevoje konkrete dhe të ligjshme, nuk përputhet me parimin e minimizimit të të dhënave personale, i parashikuar në pikën 3 të nenit 6 të Ligjit, sipas të cilit të dhënat e përpunuara duhet të jenë të përshtatshme, të lidhura me qëllimin dhe të kufizuara në atë që është e nevojshme për realizimin e tij.

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, 13, 14, 26, 27, 28, 33 dhe 81-84 të Ligjit, Komisioneri,

REKOMANDON:

1. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Tiranë" sh.a., të ketë në vëmendje proceset e përpunimit të të dhënave personale, në mënyrë që përpunimi të mos jetë në tejkalim të parimit të minimizimit së të dhënave, në përputhje me parashikimin e pikës 3 të nenit 6 të Ligjit.
2. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Tiranë" sh.a., të ketë në vëmendje rishikimin dhe përditësimin e formularit të aplikimit për lidhjen e kontratës me abonentët, duke përfshirë një klauzolë informuese të qartë, të plotë, transparente dhe të kuptueshme, në përputhje me nenet 13 dhe 14 të Ligjit.
3. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Tiranë" sh.a., të marrë masa për të hartuar marrëveshjen me përpunuesin, duke specifikuar detyrimet midis palëve, sipas detyrimeve të parashikuara në nenin 26 të Ligjit.
4. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Tiranë" sh.a., në zbatim të neneve 27 dhe 28 të Ligjit, të ketë në vëmendje përditësimin e aktit të brendshëm rregullator "*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale në Shoqërinë Ujësjellës Kanalizime Tiranë sh.a.*", duke parashikuar në të masa konkrete teknike dhe organizative për mbrojtjen e të dhënave personale për çdo kategori të dhënash dhe proces përpunimi, mënyrat e përpunimit të të dhënave, të drejtat e subjekteve të të dhënave, përcaktimin e niveleve të aksesit etj.
5. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Tiranë" sh.a., në zbatim të neneve 27 dhe 28 të Ligjit të marrë masa për dokumentimin e proceseve përpunuese, si dhe masa konkrete teknike dhe organizative për mbrojtjen e të dhënave personale, në funksion të aktivitetit të tij, për çdo proces përpunimi.

6. Kontrolluesi, shoqëria “Ujësjellës Kanalizime Tiranë” sh.a., të marrë masa për zbatimin e rregullave të brendshme mbi trajtimin, aksesin dhe shpërndarjen e të dhënave personale, me qëllim parandalimin e përpunimeve të paautorizuara dhe rritjen e nivelit të sigurisë dhe konfidencialitetit të të dhënave, sipas parashikimeve të nenit 28 të Ligjit.
7. Kontrolluesi, shoqëria “Ujësjellës Kanalizime Tiranë” sh.a., të marrë masa për caktimin e nëpunësit për mbrojtjen e të dhënave personale sipas parashikimeve të nenit 33 të Ligjit, si dhe për publikimin e të dhënave të kontaktit të nëpunësit për mbrojtjen e të dhënave personale në faqen zyrtare të internetit ukt.al.
8. Kontrolluesi, shoqëria “Ujësjellës Kanalizime Tiranë” sh.a., të marrë masa me qëllim garantimin e sigurisë së të dhënave personale dhe të zbatojë detyrimet e përcaktuara në nenet 33 dhe 34 të Ligjit, lidhur me trajnimin e punonjësve që kanë akses dhe përpunojnë të dhëna personale, në përputhje me proceset përpunuese që ata kryejnë gjatë veprimtarisë së tyre.
9. Në zbatim të nenit 84 të Ligjit, të përmbushen detyrimet sipas këtij akti, brenda afateve, si vijon:

   i) vazhdimisht, detyrimin e përcaktuar në pikat 1, 2 dhe 4 më sipër;
   ii) brenda 15 (pesëmbëdhjetë) ditëve, detyrimin e përcaktuar në pikën 6 më sipër;
   iii) brenda 30 (tridhjetë) ditëve, detyrimet e përcaktuara në pikat 3, 5 dhe 7 më sipër;
   iv) brenda 45 (dyzet e pesë) ditëve, detyrimin e përcaktuar në pikat 5 dhe 8 më sipër.

   Afatet e sipërpërmendura fillojnë nga data e marrjes dijeni të këtij akti.
10. Kontrolluesi të njoftojë Komisionerin për masat e marra brenda 60 (gjashtëdhjetë) ditëve.
11. Komisioneri, bazuar në shkronjën “a” të pikës 2 të 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 të moszbatimit të tyre, 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 05.11.2026.

KOMISIONERI

Besnik Dervishi