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. 2795/7 prot. Tiranë, më 13.11.2026

REKOMANDIM

Nr. 75, datë 13.11.2026

PËR KONTROLLUESIN, SHOQËRIA "UJËSJELLËS KANALIZIME SHKODËR" 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"), procesverbalit të hetimit, si dhe provave të administruara në përfundim të hetimit administrativ në ngarkim të Kontrolluesit "Ujësjellës Kanalizime Shkodër sh.a." (në vijim "Kontrolluesi"),

KONSTATOHET SE:

Në zbatim të Urdhrit nr. 204, datë 05.10.2026, 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 hetimit administrativ, 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 M37819701O, me objekt aktiviteti "*Shërbimi i furnizimit me ujë të pijshëm i konsumatorëve dhe shitja e tij; Mirëmbajtja e sistemit/sistemeve të furnizimit me ujë të pijshëm; Prodhimi dhe/ose blerja e ujit për plotësimin e kërkesës së konsumatorëve etj.*".

   Kontrolluesi mbledh dhe përpunon të dhëna personale për kategorinë e të dhënave "punonjës", "klientë/abonentë", "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, ndër të tjera, rezulton se disponohet edhe "certifikatë familjare" e nëpunësit. Nga shqyrtimi i dokumentit të vendosur në dispozicion të grupit të hetimit administrativ "Rregullore e Brendshme e Organizimit dhe e Funksionimit të Shoqërisë" 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 edhe 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.

   Rezulton se Kontrolluesi ruan dokumentacionin e personelit të larguar pa përcaktuar afate konkrete ruajtjeje dhe pa ndërmarrë masa për asgjësimin e tij pas përfundimit të qëllimit të përpunimit, në kundërshtim me pikën 5 të nenit 6 të Ligjit.

   Zyra e Komisionerit vlerëson se Kontrolluesi duhet të përcaktojë në mënyrë të qartë dhe të dokumentuar afatet e ruajtjes për çdo kategori të dhënash personale, duke marrë në konsideratë qëllimin e përpunimit, bazën ligjore përkatëse, detyrimet që rrjedhin nga legjislacioni sektorial, si dhe nevojën për ruajtje për qëllime të mbrojtjes së të drejtave ligjore apo për përmbushjen e detyrimeve kontraktore. Afatet duhet të jenë proporcionale dhe të justifikuara, duke shmangur ruajtjen e të dhënave për një kohë të pacaktuar, në përputhje me parashikimin e pikës 5 të nenit 6 të Ligjit.

   Gjithashtu, Kontrolluesi duhet të hartojë procedura të qarta për fshirjen, asgjësimin ose anonimizimin e të dhënave personale pas përfundimit të afatit të ruajtjes, si dhe mekanizma monitorimi dhe auditimi të brendshëm për të garantuar zbatimin efektiv të këtyre afateve. Në rastet kur të dhënat ruhen për periudha më të gjata për qëllime arkivore në interes publik, për qëllime kërkimore apo statistikore, duhet të aplikohen masa të përshtatshme teknike dhe organizative për të garantuar minimizimin e të dhënave dhe kufizimin e aksesit.

3. Kontrolluesi ka të instaluar sistemin e video-survejimit (CCTV), përmes të 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 të orientuara në mënyrë të tillë që monitorojnë ambientet e jashtme të ndërtesës, duke përfshirë edhe ambiente të tjera, rrugë kalimi dhe qytetarë, në kundërshtim me nenet 6 dhe nenin 7 të Ligjit dhe Udhëzimin nr. 03, datë 30.04.2025 "Për përpunimin e të dhënave personale nga sistemet e video-survejimit" (në vijim "Udhëzimi nr. 03").

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

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 vendosja e kamerave duhet të kufizohet vetëm në ambientet e nevojshme për qëllimin e deklaruar të survejimit, pa përfshirë hapësira publike, rrugë kalimi apo ambiente të palëve të treta. Zyra e Komisionerit vlerëson se Kontrolluesi duhet të rishikojë planvendosjen e kamerave të sistemit të video-survejimit (CCTV), duke siguruar që orientimi dhe mbulimi i tyre të jetë proporcional me qëllimin e survejimit, në përputhje me nenet 6 dhe 7 të Ligjit, si dhe Udhëzimin nr. 03 të Komisionerit.

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. 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 Kontrolluesi duhet të sigurojë që, në momentin e mbledhjes së të dhënave personale, abonenti të informohet në mënyrë të qartë, transparente dhe të plotë për përpunimin e të dhënave të tij personale, në përputhje me parashikimet e neneve 13 dhe 14 të Ligjit.

   Në këtë kuadër, Kontrolluesi duhet të përfshijë në formularin e aplikimit një klauzolë informuese, e cila të përmbajë: qëllimin dhe bazën ligjore të përpunimit; kategoritë e të dhënave personale që mblidhen; afatet e ruajtjes së të dhënave; të drejtat e subjektit të të dhënave, duke përfshirë të drejtën e aksesit, korrigjimit, fshirjes dhe kundërshtimit të përpunimit; si dhe të drejtën për të paraqitur ankesë pranë Zyrës së Komisionerit.

   Zyra e Komisionerit vlerëson se transparenca në përpunimin e të dhënave personale është një parim themelor i Ligjit, zbatimi i të cilit kërkon që subjekti i të dhënave të jetë i

informuar plotësisht para ose në momentin e mbledhjes së të dhënave të tij, në mënyrë që të ushtrojë në mënyrë efektive të drejtat e tij, në përputhje me parashikimet e neneve 13 dhe 14 të Ligjit.

5. Veprimtaria e Kontrolluesit për përpunimin e të dhënave personale realizohet, ndër të tjera, nëpërmjet sistemit elektronik "AL-Billing" të administrimit të abonentëve dhe faturimit, i cili përdoret për administrimin e abonentëve të shërbimit të ujësjellës-kanalizimeve, kontratave, konsumit të ujit, faturimit, leximeve, arkëtimit, marrëveshjeve për shlyerjen e detyrimeve, ankesave, raportimit dhe administrimit të përdoruesve. Sistemi paraqitet si një aplikacion me ndërfaqe *web*, nëpërmjet të cilit përdoruesit aksesojnë modulet funksionale përkatëse, në varësi të të drejtave të caktuara.

   Nga verifikimi i ndërfaqes së sistemit rezulton se aplikacioni përmban modulet "Abonenti", "Faturim", "Leximet", "Arkëtim", "Ankesat", "Aktmarrëveshje", "Raporte" dhe "Administrim", të cilat mundësojnë regjistrimin, konsultimin, përditësimin dhe administrimin e informacionit që lidhet me abonentët dhe marrëdhënien e tyre kontraktore dhe financiare me Kontrolluesin.

   Nëpërmjet modulit të administrimit të abonentëve realizohet kërkimi dhe konsultimi i regjistrimeve të abonentëve, duke përdorur si parametra numrin e klientit, numrin e kontratës, kodin e abonentit, njësinë dhe bllokun përkatës. Sistemi paraqet një strukturë tabelare, ku informacioni i abonentëve organizohet sipas numrit të klientit, numrit të kontratës, identifikimit të abonentit, zonës/nënzonës, adresës, kategorisë së faturimit dhe statusit të regjistrimit.

   Nëpërmjet kësaj strukture krijohet lidhja ndërmjet identifikuesve të abonentit, kontratës, vendndodhjes së shërbimit dhe kategorisë së faturimit, duke mundësuar kërkimin dhe konsultimin e informacionit të një abonenti konkret, si dhe administrimin e regjistrimeve sipas ndarjes territoriale dhe organizative të shërbimit.

   Nga verifikimi i sistemit rezulton gjithashtu funksionaliteti për administrimin e zonave dhe nënzonave, nëpërmjet të cilit abonentët klasifikohen sipas njësive territoriale të shërbimit. Kjo strukturë mundëson organizimin e informacionit mbi abonentët dhe kontratat sipas vendndodhjes, duke krijuar lidhje ndërmjet identifikimit të abonentit, adresës dhe zonës së shërbimit.

   Moduli i faturimit realizon administrimin e proceseve që lidhen me konsumin dhe përllogaritjen e detyrimeve. Nga verifikimi i ndërfaqes evidentohet funksionaliteti "Regjistro Konsum", në të cilin përdoruesi mund të regjistrojë numrin e klientit, zonën, nënzonën dhe numrin e kontratës, si dhe të zgjedhë kategorinë përkatëse të konsumit, përfshirë konsumin aforfe. Sistemi përmban gjithashtu fushë për datën e faturimit, duke mundësuar lidhjen e informacionit mbi konsumin me periudhën përkatëse të faturimit.

   Nëpërmjet këtij procesi, të dhënat identifikuese të abonentit dhe kontratës ndërthuren me informacionin mbi konsumin, zonën e shërbimit dhe periudhën e faturimit, duke mundësuar krijimin dhe administrimin e regjistrimeve që përdoren për përllogaritjen e detyrimeve financiare të abonentëve.

Nga verifikimi i strukturës së aplikacionit rezulton se sistemi përmban gjithashtu module për leximet, arkëtimin dhe aktmarrëveshjet, të cilat lidhen funksionalisht me administrimin e konsumit, pagesave dhe detyrimeve të abonentëve. Nëpërmjet këtyre moduleve parashikohet administrimi i informacionit që lidhet me marrëdhënien financiare të abonentëve me Kontrolluesin.

Moduli i ankesave realizon regjistrimin dhe administrimin e kërkesave dhe ankesave të abonentëve. Nga verifikimi i ndërfaqes "Regjistro Ankesë" rezulton se sistemi përmban fusha për numrin e klientit, numrin e regjistrit, numrin e dokumentit dhe përmbajtjen e ankesës. Gjithashtu, në ndërfaqen përkatëse paraqitet një regjistër elektronik, ku informacioni organizohet sipas numrit të regjistrit, numrit të klientit, përmbajtjes së ankesës, numrit të dokumentit, objektit, datës, kontaktit dhe përgjigjes së dhënë.

Në këtë mënyrë, sistemi mundëson lidhjen e përmbajtjes së ankesës me identifikuesit e abonentit, dokumentacionin administrativ, të dhënat e kontaktit dhe përgjigjen përkatëse. Përmbajtja e ankesave mund të përfshijë informacione personale shtesë, në varësi të objektit dhe rrethanave të paraqitura nga abonenti.

Nëpërmjet modulit të raportimit realizohet kërkimi, filtrimi dhe konsultimi i informacionit mbi abonentët, kontratat dhe detyrimet. Nga verifikimi i ndërfaqes "Raporte mbi Abonentët" rezulton se sistemi mundëson filtrimin e të dhënave sipas zonës/nënzonës, tipit ose kategorisë së abonentit, tipit të faturimit, kategorisë dhe statusit.

Moduli i administrimit të përdoruesve realizon menaxhimin e llogarive që aksesojnë sistemin. Nga verifikimi i ndërfaqes "Administrimi i Përdoruesve" rezulton se aplikacioni përmban një listë të përdoruesve të regjistruar, ku paraqiten emri i plotë, emri i përdoruesit dhe roli përkatës. Në listë evidentohen role të ndryshme, përfshirë administratorë, specialistë, arkëtarë dhe përdorues të lidhur me funksione të tjera administrative.

Në ndërfaqen e administrimit paraqiten funksionalitete për krijimin e përdoruesve të rinj, administrimin e përdoruesve ekzistues dhe ndryshimin e elementeve të llogarive të tyre. Kjo strukturë mundëson administrimin e aksesit sipas përdoruesve dhe roleve, ndërsa mënyra konkrete e kufizimit të privilegjeve, miratimit të autorizimeve dhe kontrollit periodik të tyre nuk verifikohet nga dokumenti dhe verifikim teknik i konfigurimeve përkatëse.

Në lidhje me autentikimin e përdoruesve, nga verifikimi i ndërfaqes rezulton se aksesi në sistem realizohet nëpërmjet emrit të përdoruesit dhe fjalëkalimit. Gjithashtu, sistemi përmban një mekanizëm të dytë verifikimi, nëpërmjet të cilit përdoruesit i dërgohet një kod në adresën elektronike, i cili duhet të vendoset në ndërfaqen përkatëse për të përfunduar procesin e hyrjes.

Për rrjedhojë, sistemi paraqet një mekanizëm autentikimi me dy hapa, duke kombinuar kredencialet e përdoruesit me verifikimin nëpërmjet një kodi të dërguar me *email*. Megjithatë, nga ndërfaqja e administruar nuk mund të përcaktohet mënyra teknike e gjenerimit dhe ruajtjes së kodit, numri i tentativave të lejuara, mekanizmi i çaktivizimit të kodeve të përdorura, mbrojtja e sesioneve dhe zbatimi i këtij mekanizmi për të gjitha kategoritë e përdoruesve.

Sistemi elektronik (Al-Billing) mundëson administrimin e integruar të të dhënave identifikuese dhe të kontaktit, të dhënave kontraktore, adresave, informacionit mbi konsumin, faturimin, detyrimet, pagesat, ankesat dhe aktivitetin e përdoruesve. Përpunimi realizohet nëpërmjet moduleve funksionale të ndërlidhura, ku të dhënat mund të regjistrohen, konsultohen, ndryshohen, filtrohen dhe përdoren për realizimin e veprimtarisë së shërbimit.

Nga verifikimi i sistemit elektronik dhe dokumentacionit të administruar, në lidhje me masat teknike dhe organizative të sigurisë, evidentohen çështjet e mëposhtme, për të cilat nuk rezultojnë të paraqitura evidenca të mjaftueshme mbi konfigurimin, zbatimin dhe efektivitetin e kontrolleve përkatëse. Konkretisht, Kontrolluesi:

- nuk paraqiti politika dhe procedura të dokumentuara për administrimin, përdorimin dhe sigurinë e sistemit elektronik të abonentëve dhe faturimit;
- nuk paraqiti procedurë të dokumentuar që të përcaktojë qëllimet, mënyrën dhe rregullat e përdorimit të sistemit, kategoritë e përdoruesve dhe përgjegjësitë e tyre gjatë përpunimit të të dhënave personale;
- nuk paraqiti një vlerësim të dokumentuar të rreziqeve që lidhen me përpunimin e të dhënave identifikuese, kontraktore, financiare dhe të ankesave nëpërmjet sistemit elektronik;
- nuk paraqiti procedurë të dokumentuar për krijimin, miratimin, ndryshimin, pezullimin dhe çaktivizimin e llogarive të përdoruesve;
- nuk paraqiti matricë të miratuar të roleve dhe privilegjeve, ku të përcaktohen të drejtat e aksesit për administratorët, specialistët, arkëtarët dhe kategoritë e tjera të përdoruesve;
- nuk paraqiti procedurë të dokumentuar për rishikimin periodik të të drejtave të aksesit, në raport me detyrat dhe përgjegjësitë konkrete të secilit përdorues;
- nuk paraqiti procedurë të dokumentuar për administrimin dhe kontrollin e llogarive me privilegje administrative, përfshirë autorizimin, kufizimin dhe monitorimin e veprimeve të administratorëve;
- nuk rezulton i dokumentuar procesi i miratimit dhe gjurmueshmërisë së ndryshimeve të roleve dhe privilegjeve të përdoruesve;
- nuk paraqiti procedurë të dokumentuar për ndarjen e detyrave ndërmjet përdoruesve që administrojnë abonentët, regjistrojnë konsumin, përpunojnë faturat, kryejnë arkëtime dhe administrojnë llogaritë e sistemit;
- nuk paraqiti politikë të dokumentuar për administrimin e kredencialeve dhe fjalëkalimeve, përfshirë kërkesat e sigurisë, ruajtjen, rivendosjen dhe kufizimin e tentativave të pasuksesshme të autentikimit;
- nuk rezulton e dokumentuar mënyra teknike e funksionimit të mekanizmit të autentikimit me kod të dërguar në *email*, përfshirë gjenerimin e sigurt të kodit, vlefshmërinë kohore, kufizimin e tentativave dhe çaktivizimin pas përdorimit;
- nuk rezulton e dokumentuar nëse mekanizmi i autentikimit me dy hapa zbatohet në mënyrë të detyrueshme për të gjithë përdoruesit, përfshirë administratorët dhe llogaritë me privilegje të larta;

- nuk paraqiti procedurë të dokumentuar për administrimin e sesioneve të përdoruesve, përfshirë kohëzgjatjen, përfundimin automatik pas joaktivitetit, revokimin e sesioneve dhe mbrojtjen e identifikuesve të autentikimit;
- nuk rezulton e dokumentuar mënyra e mbrojtjes së *cookies* dhe tokenëve të sesioneve, përfshirë përdorimin e parametrave të sigurisë Secure, HttpOnly dhe SameSite, sipas mekanizmit teknik të përdorur;
- nuk paraqiti procedurë të dokumentuar për regjistrimin, ruajtjen, mbrojtjen, monitorimin dhe analizimin e *log*-eve të aktivitetit të përdoruesve;
- megjithëse sistemi përmban funksionalitetin "Aktiviteti i Përdoruesve", nga ndërfaqja e verifikuar evidentohet regjistrimi i hyrjeve në sistem, aktivitetit të fundit dhe kohëzgjatjes së sesioneve, ndërsa nuk evidentohet gjurmueshmëria e plotë e veprimeve konkrete mbi të dhënat personale;
- nuk rezulton e dokumentuar mënyra sesi identifikohet përdoruesi që ka konsultuar, regjistruar, ndryshuar, korrigjuar ose fshirë të dhënat e një abonenti, përfshirë datën, orën dhe vlerat përpara dhe pas ndryshimit;
- nuk paraqiti evidenca mbi mbrojtjen e regjistrave të aktivitetit nga ndryshimi ose fshirja e paautorizuar, afatet e ruajtjes dhe kontrollin periodik të tyre;
- nuk paraqiti procedurë për auditimin periodik të veprimeve të përdoruesve në modulet e abonentëve, faturimit, leximeve, arkëtimit, ankesave dhe aktmarrëveshjeve;
- nuk rezulton i dokumentuar një mekanizëm i plotë kontrolli mbi regjistrimin dhe korrigjimin e konsumit, përfshirë autorizimin e ndryshimeve dhe ruajtjen e historikut të leximeve ose të dhënave të faturimit;
- nuk paraqiti procedurë të dokumentuar për kontrollin e integritetit të informacionit kontraktor dhe financiar, përfshirë lidhjen ndërmjet numrit të klientit, numrit të kontratës, zonës, konsumit, faturimit dhe detyrimeve;
- nuk rezulton i dokumentuar procesi i kontrollit dhe verifikimit të regjistrimeve të konsumit aforfe, përfshirë përdoruesit e autorizuar, kriteret e regjistrimit dhe gjurmueshmërinë e ndryshimeve;
- nuk paraqiti procedurë të dokumentuar për administrimin e të dhënave personale të përfshira në ankesat e abonentëve, përfshirë kategoritë e informacionit, aksesin, ruajtjen dhe fshirjen e tyre;
- nuk rezulton e dokumentuar mënyra e kufizimit të aksesit në përmbajtjen e ankesave, dokumentet shoqëruese dhe përgjigjet, në raport me përgjegjësitë e përdoruesve;
- nuk paraqiti procedurë të dokumentuar për administrimin e raporteve mbi abonentët, përfshirë kufizimin e aksesit sipas kategorisë së raportit, qëllimit të përdorimit dhe kategorive të të dhënave;
- nuk rezulton i dokumentuar një mekanizëm për kontrollin dhe regjistrimin e eksportimit, printimit ose shkarkimit të informacionit nga sistemi, nëse këto funksionalitete janë të aktivizuara;
- nuk paraqiti procedurë të dokumentuar për mbrojtjen e raporteve dhe skedarëve elektronikë të nxjerrë nga sistemi, përfshirë ruajtjen në pajisjet fundore, transmetimin dhe fshirjen e tyre;
- nuk paraqiti dokumentacion të plotë mbi arkitekturën teknike të sistemit, përfshirë serverët ku hostohet aplikacioni, teknologjinë dhe konfigurimin e bazës së të dhënave, komponentët e rrjetit dhe mekanizmat e mbrojtjes së tyre;

- nuk rezulton e dokumentuar nëse sistemi hostohet në infrastrukturën e vetë Kontrolluesit apo në infrastrukturë të një ofruesi të jashtëm, si dhe vendndodhja fizike dhe logjike e të dhënave dhe kopjeve rezervë;
- nuk paraqiti inventar të dokumentuar të aseteve TIK që marrin pjesë në mbledhjen, transmetimin, ruajtjen dhe përpunimin e të dhënave personale;
- nuk paraqiti procedurë të dokumentuar për konfigurimin e sigurt të serverëve, aplikacionit, bazës së të dhënave dhe pajisjeve të rrjetit, përfshirë kufizimin e shërbimeve, porteve, protokolleve dhe aksesit administrativ;
- nuk rezulton e dokumentuar ndarja ndërmjet shtresës së aplikacionit dhe bazës së të dhënave, segmentimi i rrjetit dhe kufizimi i komunikimeve ndërmjet komponentëve;
- nuk rezulton e dokumentuar mënyra e mbrojtjes së të dhënave gjatë transmetimit ndërmjet pajisjeve të përdoruesve, aplikacionit dhe bazës së të dhënave, përfshirë përdorimin e protokolleve të sigurta dhe mekanizmave të enkriptimit;
- nuk rezulton i dokumentuar vlerësimi i nevojës dhe zbatimi i masave të mbrojtjes së të dhënave gjatë ruajtjes, përfshirë enkriptimin ose kontrolle të tjera të përshtatshme për informacionin identifikues dhe financiar;
- nuk paraqiti procedurë të dokumentuar për administrimin e privilegjeve të aksesit në bazën e të dhënave, përfshirë llogaritë teknike, llogaritë administrative dhe kufizimin e aksesit të drejtpërdrejtë;
- nuk paraqiti procedurë të dokumentuar për menaxhimin e cenueshmërive teknike të aplikacionit *web*, serverëve, bazës së të dhënave dhe komponentëve të tjerë të infrastrukturës;
- nuk paraqiti procedurë të dokumentuar për menaxhimin e përditësimeve dhe *patch*-eve të sigurisë, përfshirë identifikimin, planifikimin, instalimin dhe verifikimin e tyre;
- nuk paraqiti evidenca mbi testimin periodik të sigurisë së aplikacionit, përfshirë skanimin e cenueshmërive, testimet e penetrimit dhe verifikimin e dobësive të autentikimit, autorizimit dhe administrimit të sesioneve;
- nuk rezulton i dokumentuar testimi i kontrolleve të autorizimit në nivel serveri, për të verifikuar se ndryshimi i identifikuesve të klientëve, kontratave ose regjistrimeve nuk mundëson akses ose ndërhyrje të paautorizuar në informacion;
- nuk paraqiti procedurë të dokumentuar për menaxhimin e ndryshimeve të aplikacionit, përfshirë zhvillimin, testimin, miratimin dhe kalimin e ndryshimeve në mjedisin e prodhimit;
- nuk rezulton e dokumentuar ndarja ndërmjet mjediseve të zhvillimit, testimit dhe prodhimit, si dhe masat për kufizimin e përdorimit të të dhënave reale personale në mjediset ku nuk zhvillohet prodhimi;
- nuk rezulton e dokumentuar marrëdhënia ndërmjet Kontrolluesit dhe zhvilluesit, mirëmbajtësit ose ofruesit të sistemit, përfshirë përgjegjësitë për sigurinë, kushtet e aksesit dhe përpunimin e të dhënave personale;
- nuk paraqiti procedurë të dokumentuar për aksesin në distancë të administratorëve, mirëmbajtësve dhe palëve të treta, përfshirë autorizimin, autentikimin, kufizimin e privilegjeve dhe monitorimin e sesioneve;

- nuk paraqiti procedurë të dokumentuar për krijimin dhe administrimin e kopjeve rezervë të bazës së të dhënave dhe komponentëve të sistemit, ku të përcaktohen periodiciteti, përgjegjësitë, vendndodhja dhe afatet e ruajtjes;
- nuk paraqiti evidenca mbi ekzekutimin dhe kontrollin e kopjeve rezervë, përfshirë regjistrimin e proceseve të suksesshme ose të dështuara, mbrojtjen e kopjeve dhe kontrollin e integritetit të tyre;
- nuk paraqiti procedurë të dokumentuar për testimin periodik të rikthimit të të dhënave nga kopjet rezervë, të shoqëruar me rezultate testimi dhe verifikim të plotësisë së informacionit të rikuperuar;
- nuk paraqiti plan të dokumentuar për vazhdimësinë e funksionimit dhe rikuperimin e sistemit pas incidenteve fizike ose teknike (*Business Continuity/Disaster Recovery*), përfshirë objektivat RTO dhe RPO;
- nuk paraqiti procedurë të dokumentuar për identifikimin, raportimin, regjistrimin, klasifikimin, analizimin dhe trajtimin e incidenteve të sigurisë së informacionit;
- nuk paraqiti procedurë të dokumentuar për menaxhimin e cenimeve të të dhënave personale, përfshirë vlerësimin e rrezikut, dokumentimin e cenimit, marrjen e masave korrigjuese dhe njoftimet përkatëse sipas kërkesave ligjore;
- nuk paraqiti procedurë të dokumentuar për ruajtjen, arkivimin, fshirjen ose anonimizimin e të dhënave personale, të diferencuar sipas kategorive të informacionit që administrohet në sistem;
- nuk rezultojnë të përcaktuara dhe dokumentuara afatet e ruajtjes së të dhënave të abonentëve, kontratave, konsumit, faturimit, arkëtimit, ankesave dhe regjistrave të aktivitetit;
- nuk rezulton e dokumentuar rrjedha e të dhënave personale (*data flow*), nga momenti i regjistrimit të abonentit, lidhja me kontratën dhe zonën e shërbimit, përpunimi në modulet e konsumit dhe faturimit, konsultimi nga përdoruesit dhe deri në arkivimin ose fshirjen e informacionit;
- nuk paraqiti procedurë të dokumentuar për trajnimin dhe ndërgjegjësimin e përdoruesve mbi sigurinë e informacionit, konfidencialitetin dhe përdorimin e autorizuar të të dhënave personale;

- nuk rezulton i dokumentuar një proces periodik për testimin, vlerësimin dhe analizimin e efektivitetit të masave teknike dhe organizative të sigurisë, përfshirë raportimin e gjetjeve, përcaktimin e masave korrigjuese dhe verifikimin e zbatimit të tyre.

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 e 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 "Al-Billing" 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 Ligjin1 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 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, 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 ka nënshkruar disa kontrata shërbimi, konkretisht:

   - Kontratë shërbimi nr. 2041 prot., datë 11.07.2024, me subjektin Posta Shqiptare sh.a., me objekt "Kontratë shërbimi për pagesën e faturave të ujit nëpërmjet Posta Shqiptare sh.a.";
   - Kontratë nr. 1831 prot., datë 01.08.2025, me subjektin "Jehona Soft" sh.p.k., me objekt "Mirëmbajtje e sistemit të faturimit dhe arkëtimit".

   Nga shqyrtimi i përmbajtjes së kontratave të mësipërme konstatohet se në to nuk janë përcaktuar në mënyrë të shprehur dhe të dokumentuar rolet, përgjegjësitë dhe detyrimet e palëve në raport me përpunimin e të dhënave personale të klientëve të Kontrolluesit, përfshirë përcaktimin e marrëdhënies kontrollues - përpunues. Gjithashtu, kontratat nuk përmbajnë përcaktime të posaçme lidhur me objektin, natyrën, qëllimin dhe kohëzgjatjen e përpunimit, kategoritë e të dhënave personale dhe të subjekteve të të dhënave, si dhe masat teknike dhe organizative për garantimin e sigurisë së përpunimit, në përputhje me kërkesat e nenit 26 të Ligjit dhe Udhëzimit 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.

7. Konstatohet se Kontrolluesi nuk disponon rregullore "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale", në të cilën të parashikohen rregulla specifike mbi kategoritë e të dhënave personale, mënyrën e përpunimit të të dhënave, sigurinë e të dhënave personale, konfidencialitetin, afatet e mbajtjes së të dhënave, të drejtat e subjekteve etj., me qëllim garantimin e përpunimit të ligjshëm dhe sigurisë së të dhënave, në përputhje me proceset përpunuese që kryen, sipas parashikimeve të neneve 27 dhe 28 të Ligjit.

   Zyra e Komisionerit vlerëson se Kontrolluesi ka detyrimin të mbajë dokumentacion për veprimtaritë e tij përpunuese, në mënyrë që të jetë në gjendje të japë të dhëna lidhur me përputhshmërinë me Ligjin. Në këtë kuadër, mospasja e një akti të brendshëm rregullator për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale, si dhe të proceseve përpunuese, është në kundërshtim me kërkesat e neneve 27 dhe 28 të Ligjit, si dhe Vendimit nr. 6, datë 05.08.2013, të Komisionerit "Për përcaktimin e rregullave të hollësishme për sigurimin e të dhënave personale".

   Gjithashtu, Zyra e Komisionerit vlerëson se hartimi i rregullores "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale", ku të parashikohen elemente të domosdoshme, si përcaktimi i rregullave dhe procedurave organizative specifike mbi mënyrën e përpunimit të të dhënave personale, sigurinë e të dhënave, konfidencialitetin, aksesin në të dhënat personale, afatet e ruajtjes së të dhënave personale etj., 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.

8. Në vijim të hetimit rezultoi se Kontrolluesi nuk aplikon për punëmarrësit/personat që, për shkak të funksionit apo detyrave të tyre, kanë akses në informacionin e mbajtur nga ana e tij "Deklaratën e Konfidencialitetit", në përmbushje të detyrimit ligjor që buron nga neni 30 i Ligjit, si 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").

   Mungesa e një deklarate të tillë nuk siguron dokumentimin formal të detyrimit të personave të autorizuar për të ruajtur konfidencialitetin e të dhënave personale dhe për të mos i përdorur ato për qëllime të ndryshme nga ato për të cilat kanë marrë akses.

   Zyra e Komisionerit vlerëson se qëllimi i nënshkrimit të "Deklaratës së Konfidencialitetit" është garantimi i ndërgjegjësimit dhe përgjegjësisë të çdo nëpunësi që ka akses në të dhëna personale, duke përcaktuar në mënyrë të qartë kufijtë e përpunimit të lejuar, ndalimin e përdorimit të të dhënave për qëllime personale apo të paautorizuara,

detyrimin për ruajtjen e konfidencialitetit edhe pas përfundimit të marrëdhënies së punës. Ky instrument përbën një masë thelbësore organizative në kuadër të parimit të përgjegjshmërisë, duke dokumentuar faktin se Kontrolluesi ka marrë masa konkrete për të garantuar përpunimin e ligjshëm dhe të sigurt të të dhënave personale, sipas parashikimeve të nenit 30 të Ligjit.

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.

   Nga verifikimi i dokumentacionit të vendosur në dispozicion rezulton se Kontrolluesi nuk ka emëruar një nëpunës të mbrojtjes së të dhënave personale, në kundërshtim me nenin 33 të Ligjit, si dhe nuk është dokumentuar përcaktimi i një personi përgjegjës për monitorimin dhe koordinimin e përmbushjes së detyrimeve në fushën e mbrojtjes së të dhënave.

   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. Në këtë drejtim, vihet re se Kontrolluesi, pas njoftimit të urdhrit të hetimit administrativ, ka ndërmarrë masa duke caktuar nëpunësin për mbrojtjen e të dhënave personale.

   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 02.11.2026, 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, me shkresën nr. 3939 prot., datë 30.10.2026, administruar me tonën me nr. 2795/6 prot., datë 2.11.2026, është dorëzuar dokumentacioni, si vijon:

   - "Marrëveshje për krijimin e subjektit të kompetencave të përbashkëta të ujësjellës kanalizimeve";

- Statuti i shoqërisë aksionare “Shoqëria rajonale Ujësjellës Kanalizime qarku Shkodër sh.a.”;
- Vendim nr. 3, datë 10.07.2023, nr. 3 prot., datë 10.07.2023 “Për zmadhimin e kapitalit dhe pranimin e aksionarit të ri të shoqërisë rajonale Ujësjellës Kanalizime qarku Shkodër sh.a.”;
- Aktmarrëveshje (kontratë) për transferim aktiviteti ndërmjet Shoqërisë Rajonale Ujësjellës Kanalizime Qarku Shkodër sh.a. dhe Shoqërisë Ujësjellës Kanalizime Shkodër;
- Urdhër nr. 06, datë 08.01.2026, nr. 60 prot., datë 08.01.2026 “Për ngritjen e komisionit të ekspertizës së protokoll/arkivës”;
- Vendim nr. 15, datë 09.06.2014 “Për zbatimin e kontratës model të miratuar nga KKRR për të gjithë klientët e sektorit të furnizimit me ujë dhe largimit e përpunimit të ujërave të ndotura”;
- Rregullore nr. 1907 prot., datë 08.08.2025 “Politika e përdorimit të rrjetit kompjuterik si dhe sistemeve”;
- Rregullore nr. 1906 prot., datë 08.08.2025 “Politikat e përdorimit të shërbimit të internetit dhe postës elektronike”;
- Kontratë shërbimi nr. 3430 prot., datë 24.12.2025 “Për pagesën e faturave të ujit nëpërmjet Rubicon sh.a. ose PAGO”;
- Kontratë shërbimi nr. 496 prot., datë 15.02.2024 “Për pagesën e faturave të ujit nëpërmjet RAEA Financial Services sh.p.k.”;
- Kontratë shërbimi nr. 496/2 prot., datë 15.02.2024 “Për pagesën e faturave të ujit nëpërmjet AK-Invest sh.a.”;
- Kontratë shërbimi nr. 496/1 prot., datë 15.02.2024 “Për pagesën e faturave të ujit nëpërmjet EasyPay sh.p.k”;
- Urdhër i brendshëm nr. 638, datë 15.10.2026 “Për caktimin e punonjësit si person kontakti me komisionerin për mbrojtjen e të dhënave personale”;
- Shkresë nr. 3812 prot., datë 22.10.2026 “Raporti i performancës SHRUK Shkodër për 9-mujorin e 2026-ës”;
- Shkresë nr. 23137 prot., datë 22.09.2026 “Akt-rekomandimi mes Bashkisë Shkodër dhe SHRUKSH për vitet 2023 - 2026”;
- Vendim nr. 2, datë 04.04.2024 “Për prioritizimin për menaxhimin e likuiditetit dhe pagesave të shoqërisë rajonale Ujësjellës Kanalizime Shkodër sh.a., për vitin 2024”;
- Deklarata Konfidencialiteti (9 fletë);
- Urdhër i Brendshëm nr. 584, datë 25.09.2026 “Për likuidimin e shpenzimeve të trajnimit”.

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, 7, 13, 14, 26, 27, 28, 30, 33, 34 dhe 81- 84 të Ligjit, Komisioneri,

REKOMANDON:

1. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Shkodër" sh.a., të ketë në vëmendje përcaktimin e afateve kohore për ruajtjen e të dhënave, për të gjitha 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.

2. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Shkodër" sh.a., të ketë në vëmendje proceset e përpunimit të të dhënave personale, në mënyrë që përpunimi mos të jetë në tejkalim të parimit të minimizimit së të dhënave, në përputhje me parashikimin e të pikës 3 të nenit 6 të Ligjit.

3. Kontrolluesi shoqëria "Ujësjellës Kanalizime Shkodër" sh.a., të ketë në vëmendje përcaktimin e planeve të kamerave përmes sistemit të video-survejimit (CCTV), në përputhje me parashikimet e neneve 6 dhe 7 të Ligjit.

4. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Shkodër" sh.a., në zbatim të neneve 13 dhe 14 të Ligjit, të parashikojë në formularin e aplikimit të abonentit një klauzolë informuese për mbledhjen dhe përpunimin e të dhënave personale, e cila të përmbajë qëllimin dhe bazën ligjore të përpunimit, kategoritë e të dhënave personale që mblidhen, afatet e ruajtjes, të drejtat e subjektit të të dhënave, si dhe të drejtën për të paraqitur ankesë pranë Zyrës së Komisionerit.

5. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Shkodër" sh.a., të marrë masa për të rishikuar kontratat me përpunuesit, duke specifikuar detyrimet midis palëve dhe masat tekniko-organizative, sipas dispozitave të parashikuara në nenin 26 të Ligjit.

6. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Shkodër" sh.a., në zbatim të neneve 27 dhe 28 të Ligjit, të marrë masa për hartimin e një akti të brendshëm rregullator 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 proces përpunimi, mënyrat e përpunimit të të dhënave, të drejtat e subjekteve të të dhënave, përcaktimin e niveleve të aksesit etj.

7. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Shkodër" 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;

8. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Shkodër" 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.

9. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Shkodër" sh.a., në zbatim të nenit 30 të Ligjit, të marrë masa për hartimin dhe aplikimin e "Deklaratës së

Konfidencialitetit" për punëmarrësit, të cilët kanë akses në mbledhjen, përpunimin dhe ruajtjen e të dhënave personale.

10. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Shkodër" sh.a., të marrë masa për caktimin e nëpunësit për mbrojtjen e të dhënave personale sipas parashikimit 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 shuk.al/shkodër.

11. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Shkodër" 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.

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

    i) vazhdimisht, detyrimet e përcaktuara në pikat 1, 2 dhe 3 më sipër;
    ii) brenda 15 (pesëmbëdhjetë) ditëve, detyrimin e përcaktuar në pikat 4 dhe 8 më sipër;
    iii) brenda 30 (tridhjetë) ditëve, detyrimet e përcaktuara në pikat 5, 6, 9 dhe 10 më sipër.
    iv) brenda 45 (dyzet e pesë) ditëve, detyrimin e përcaktuar në pikat 7 dhe 11 më sipër.

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

13. Kontrolluesi të njoftojë Komisionerin për masat e marra brenda 60 (gjashtëdhjetë) ditëve.

14. 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 13.11.2026.

KOMISIONERI

Besnik Dervishi