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. 2486/5 prot. Tiranë, më 05.11.2026

REKOMANDIM

Nr. 72, datë 05.11.2026

PËR KONTROLLUESIN, SHOQËRIA "UJËSJELLËS KANALIZIME FIER" 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 Fier sh.a." (në vijim "Kontrolluesi"),

KONSTATOHET SE:

Në zbatim të Urdhrit nr. 172, 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 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 J63423411D, 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 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", rezulton se 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.

   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. Veprimtaria e Kontrolluesit për përpunimin e të dhënave personale realizohet, ndër të tjera, nëpërmjet sistemit elektronik "UKF Web System", i cili përdoret për administrimin e abonentëve, kontratave, matësve dhe të dhënave që lidhen me konsumin e shërbimit. Sistemi përmban gjithashtu komponentin "UK Reader", nëpërmjet të cilit realizohet aksesimi i funksionaliteteve përkatëse nga përdoruesit e autorizuar.

Nga verifikimi i ndërfaqes së sistemit rezulton se në të administrohen të dhëna të lidhura me kontratën dhe abonentin, përfshirë numrin e kontratës së vjetër, numrin e kontratës, numrin e abonentit/subjektit, emrin, atësinë, mbiemrin, rrugën, pallatin, shkallën/apartamentin, qytetin, telefonin, adresën e postës elektronike, të dhëna identifikuese, të dhëna mbi kategorinë e kontratës, statusin e kontratës dhe informacione të tjera të lidhura me marrëdhënien e abonentit me Kontrolluesin.

Sistemi përpunon gjithashtu të dhëna që lidhen me matësin dhe konsumin, duke mundësuar lidhjen e informacionit teknik të matësit me kontratën dhe abonentin përkatës. Nëpërmjet kësaj strukture krijohet një profil elektronik i abonentit, ku të dhënat identifikuese dhe të kontaktit ndërthuren me të dhënat kontraktore dhe ato të lidhura me shërbimin.

Nga verifikimi i sistemit rezulton gjithashtu funksionaliteti për administrimin e informacionit të lidhur me vendndodhjen e matësit dhe abonentit, i cili paraqitet nëpërmjet një harte elektronike. Në ndërfaqen e sistemit shfaqen të dhëna të vendndodhjes dhe një paraqitje hartografike e pozicionit përkatës, si dhe fotografia e matësit.

Për rrjedhojë, nëpërmjet sistemit realizohet përpunimi i kombinuar i të dhënave identifikuese, të dhënave të kontaktit, adresës, të dhënave kontraktore, të dhënave mbi matësin dhe konsumin, të dhënave të vendndodhjes dhe imazheve të lidhura me matësin, duke mundësuar lidhjen e këtyre informacioneve me një abonent dhe kontratë konkrete.

Aksesi në komponentin "UK Reader" realizohet nëpërmjet një ndërfaqeje autentikimi me kod/verifikim të përdoruesit dhe fjalëkalim, siç evidentohet nga pamjet e administruara gjatë kontrollit.

Nga verifikimi i sistemit elektronik dhe dokumentacionit të administruar konstatohet se Kontrolluesi:

- nuk disponon politika dhe procedura të dokumentuara për administrimin, përdorimin dhe sigurinë e sistemit "UKF Web System/UK Reader", nëpërmjet të cilit përpunohen të dhëna personale të abonentëve;
- nuk disponon 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 disponon procedurë të dokumentuar për krijimin, miratimin, ndryshimin, pezullimin dhe çaktivizimin e llogarive të përdoruesve;
- nuk disponon procedurë të dokumentuar për përcaktimin dhe rishikimin periodik të të drejtave të aksesit, në raport me funksionet dhe përgjegjësitë konkrete të secilit përdorues;
- nuk disponon procedurë të dokumentuar për administrimin dhe kontrollin e llogarive me privilegje administrative, përfshirë përcaktimin e personave që disponojnë këto privilegje dhe monitorimin e veprimeve të tyre;
- nuk disponon procedurë të dokumentuar për menaxhimin e kredencialeve dhe fjalëkalimeve, përfshirë kompleksitetin, periodicitetin e ndryshimit, rivendosjen dhe mbrojtjen e tyre;

- nga verifikimi i ndërfaqes së autentikimit nuk evidentohet përdorimi i një mekanizmi të autentikimit me shumë faktorë (MFA/2FA), ndërsa nuk disponohet dokumentacion që të provojë një vlerësim të rrezikut mbi mekanizmin e autentikimit të përdorur;
- nuk disponon procedurë të dokumentuar për regjistrimin, ruajtjen, mbrojtjen, monitorimin dhe analizimin e *log*-eve të aktivitetit të përdoruesve;
- nuk rezulton e dokumentuar mënyra se si evidentohet identiteti i përdoruesit që ka aksesuar të dhënat e një abonenti, koha e aksesit dhe veprimet e kryera mbi të dhënat;
- nuk disponon procedurë për auditimin periodik të veprimeve të përdoruesve, përfshirë konsultimin, regjistrimin, ndryshimin, korrigjimin, eksportimin ose fshirjen e të dhënave;
- nuk disponon procedurë të dokumentuar për menaxhimin e të dhënave të vendndodhjes që administrohen në sistem, duke përfshirë përcaktimin e përdoruesve që mund t'i aksesojnë, qëllimin e përdorimit dhe afatin e ruajtjes së tyre;
- nuk disponon procedurë të dokumentuar për administrimin e fotografive të matësve, përfshirë mënyrën e realizimit, transmetimit, ruajtjes, aksesimit dhe fshirjes së tyre;
- nuk rezulton i dokumentuar mekanizmi nëpërmjet të cilit fotografia, vendndodhja, të dhënat e matësit dhe të dhënat e abonentit lidhen ndërmjet tyre, si dhe kontrollet e aplikuara për të parandaluar lidhjen ose aksesimin e gabuar të informacionit;
- nuk disponon procedurë të dokumentuar për pajisjet mobile ose pajisjet e tjera fundore, nëse këto përdoren nga punonjësit për leximin e matësve, regjistrimin e informacionit, fotografimin ose transmetimin e të dhënave drejt sistemit qendror;
- nuk rezulton e dokumentuar mënyra e mbrojtjes së të dhënave gjatë transmetimit nga pajisja e përdoruesit drejt sistemit qendror, përfshirë mekanizmat e enkriptimit dhe sigurimin e komunikimit;
- nuk disponon procedurë të dokumentuar për ruajtjen dhe fshirjen e të dhënave personale, të diferencuar sipas kategorive të informacionit të administruar në sistem;
- nuk rezultojnë të përcaktuara dhe të dokumentuara afatet e ruajtjes së të dhënave të vendndodhjes dhe fotografive të matësve;
- nuk disponon procedurë të dokumentuar për eksportimin, shkarkimin ose transferimin e të dhënave personale nga sistemi, përfshirë përcaktimin e përdoruesve të autorizuar dhe kushtet në të cilat këto veprime lejohen;
- nuk disponon procedurë të dokumentuar për *backup*-in e databazës dhe të të dhënave personale, ku të përcaktohen periodiciteti, përgjegjësitë, afati dhe vendndodhja e ruajtjes së kopjeve rezervë;
- nuk disponon procedurë të dokumentuar për testimin periodik të rikthimit të të dhënave nga *backup*-et;
- nuk disponon procedurë të dokumentuar për vazhdimësinë e funksionimit dhe rikuperimin e sistemit pas incidenteve fizike ose teknike (*Business Continuity/Disaster Recovery*);
- nuk disponon procedurë të dokumentuar për menaxhimin e incidenteve të sigurisë dhe cenimeve të të dhënave personale, përfshirë identifikimin, raportimin, dokumentimin, klasifikimin, përshkallëzimin dhe trajtimin e tyre;
- nuk disponon procedurë të dokumentuar për menaxhimin e cenueshmërive teknike të aplikacionit, serverëve, databazës dhe komponentëve të tjerë të infrastrukturës;

- nuk disponon procedurë të dokumentuar për menaxhimin e përditësimeve dhe *patch*-eve të sigurisë;
- nuk disponon procedurë të dokumentuar për testimin periodik të sigurisë së aplikacionit, përfshirë skanimin e cenueshmërive dhe testimet e sigurisë së aplikacionit *web*;
- nuk rezulton i dokumentuar një proces për testimin, vlerësimin dhe analizimin periodik të efektivitetit të masave teknike dhe organizative të zbatuara për sistemin;
- nuk disponohet dokumentacion i plotë mbi arkitekturën teknike të sistemit, përfshirë serverët ku hostohet aplikacioni, databazën, ndarjen ndërmjet shtresës së aplikacionit dhe databazës, konfigurimin e rrjetit dhe mekanizmat e mbrojtjes së tyre;
- nuk rezulton e dokumentuar nëse sistemi hostohet në infrastrukturën e vetë Kontrolluesit apo nga një ofrues i jashtëm, si dhe vendndodhja fizike/logjike e të dhënave dhe kopjeve rezervë;
- nuk rezulton e dokumentuar marrëdhënia ndërmjet kontrolluesit dhe zhvilluesit, mirëmbajtësit apo ofruesit të sistemit, nëse ky i fundit ka mundësi aksesi në sistem ose në databazën që përmban të dhënat personale;
- nuk disponon procedurë të dokumentuar për aksesin në distancë të administratorëve, mirëmbajtësve ose palëve të treta në sistem;
- nuk rezulton i dokumentuar inventari i aseteve TIK që marrin pjesë në mbledhjen, transmetimin, ruajtjen dhe përpunimin e të dhënave nëpërmjet sistemit;
- nuk rezulton e dokumentuar rrjedha e të dhënave personale (*data flow*) nga momenti i mbledhjes së informacionit në terren, transmetimi drejt sistemit, ruajtja në databazë, konsultimi nga përdoruesit dhe deri në fshirjen ose arkivimin e tij;
- nuk rezulton i dokumentuar një proces periodik për identifikimin, analizimin dhe vlerësimin e rreziqeve që lidhen me përpunimin elektronik të të dhënave personale nëpërmjet këtij sistemi.

Për sa më sipër, konstatohet se Kontrolluesi përdor sistemin elektronik "UKF Web System/UK Reader" për përpunimin e një numri të konsiderueshëm kategorish të të dhënave personale të abonentëve, ku të dhënat identifikuese dhe të kontaktit ndërthuren me të dhënat kontraktore, të dhënat mbi matësin, konsumin, vendndodhjen dhe imazhin e matësit. Megjithatë, mungojnë masat e ndërmarra për garantimin dhe demonstrimin e përputhshmërisë së veprimtarive të përpunimit, në kuptim të nenit 27 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 "UKF Web System/UK Reader" 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.

4. 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 verifikimi në vend rezulton se të dhënat imazhe/video ruhen përtej afatit ligjor 30-ditor, në kundërshtim me parimin e ruajtjes në kohë, sipas pikës 5 të nenit 6 të Ligjit dhe Udhëzimit nr. 03, datë 30.04.2025 "Për përpunimin e të dhënave personale nga sistemet e video-survejimit" (në vijim "Udhëzimi nr. 03"). Nga ana e Kontrolluesit nuk janë ndërmarrë masa për fshirjen/shkatërrimin e këtyre të dhënave pas përfundimit të periudhës së ligjshme të ruajtjes së këtyre regjistrimeve, në kundërshtim me nenin 3 të Udhëzimit nr. 03 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. 03 të Komisionerit.

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 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.

5. Nga shqyrtimi i dokumentacionit të vënë në dispozicion nga Kontrolluesi rezulton se ka nënshkruar kontratë shërbimi me nr. 2138/24 prot., datë 26.12.2025, me subjektin "JEHONA SOFT" sh.p.k., me objekt "Shërbim mirëmbajtje AL-Billing".

   Nga analizimi i përmbajtjes së kontratës konstatohet se në të nuk specifikohet shprehimisht roli ligjor i palëve në lidhje me përpunimin e të dhënave personale të abonentëve/klientëve të Kontrolluesit, kategoritë e të dhënave personale që shkëmbehen ndërmjet palëve, qëllimin e përpunimit, afatin e ruajtjes, si dhe masat konkrete tekniko-organizative të detyrueshme për t'u zbatuar, me qëllim garantimin e sigurisë dhe përpunimit të ligjshëm të të dhënave personale.

   Gjithashtu, nuk janë reflektuar detyrimet sipas parashikimeve të 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.

6. Nga shqyrtimi i dokumentacionit të administruar rezulton se Kontrolluesi disponon aktin e brendshëm "Rregullore për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale". Megjithatë, nga shqyrtimi i përmbajtjes së saj rezulton se në të nuk janë parashikuar 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, siguria e të dhënave personale, aksesi në të dhënat personale, afatet e mbajtjes së të dhënave, që nuk janë pjesë e sistemit CCTV 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" 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. 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, "Deklarata e Konfidencialitetit", në përmbushje të detyrimit ligjor që buron nga neni 30 i Ligjit, si dhe Vendimi nr. 6, datë 05.08.2013, i 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.

8. 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.

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 22.10.2026, 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, Kontrolluesi ka dorëzuar gjatë seancës dëgjimore dokumentacionin, si vijon:

- Urdhër i brendshëm për caktimin e personit përgjegjës për mbrojtjen e të dhënave personale nr. 3723 prot., datë 21.10.2026;
- Kontratë me objekt "Shërbim, mirëmbajtje AL-Billing", nr. 2138/24 prot., datë 26.12.2025;
- Kontratë Kolektive 2023 – 2026.

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, 26, 27, 28, 30, 33 dhe 81 - 84 të Ligjit, Komisioneri,

REKOMANDON:

1. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Fier" 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 Fier" 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 Fier" sh.a., të marrë masa për të hartuar marrëveshjen me përpunuesin, duke specifikuar marrëdhëniet midis palëve, sipas detyrimeve të parashikuara në nenin 26 të Ligjit.

4. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Fier" sh.a., në zbatim të neneve 27 dhe 28 të Ligjit, të marrë masa për përditësimin e aktit të brendshëm rregullator "Politika e mbrojtjes së 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.

5. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Fier" 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 Fier" sh.a., të ketë në vëmendje 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 Fier" sh.a., në zbatim të nenit 30 të Ligjit, të marrë masa mbi hartimin dhe aplikimin e "Deklaratës së Konfidencialitetit" për punëmarrësit, të cilët kanë akses në mbledhjen, përpunimin dhe ruajtjen e të dhënave personale.

8. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Fier" 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 shuk.al/fier.

9. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Fier" 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.

10. 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 6 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 3 dhe 7 më sipër;
iv) brenda 45 (dyzet e pesë) ditëve, detyrimin e përcaktuar në pikat 5 dhe 9 më sipër.

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

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

12. 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