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. 2484/6 prot. Tiranë, më 05.11.2026

REKOMANDIM

Nr. 70, datë 05.11.2026

PËR KONTROLLUESIN, SHOQËRIA "UJËSJELLËS KANALIZIME ELBASAN", 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 Elbasan sh.a." (në vijim "Kontrolluesi"),

KONSTATOHET SE:

Në zbatim të Urdhrit nr. 170, 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 M23322201V, 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. Kontrolluesi mban në arkivin fizik dosjet e personelit aktual dhe të larguar të cilat, ndër të tjera, përmbajnë kopje të: "vërtetim i gjendjes gjyqësore"; "certifikatë personale"; "certifikata trajnimesh"; "dëftesë pjekurie"; "librezë shëndetësore"; "jetëshkrim"; "letërnjoftim" etj.

   Nga shqyrtimi i "Rregullores për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale" (e pamiratuar nga strukturat përkatëse) 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, si dhe si dhe Udhëzimin nr. 11, datë 08.09.2011, të Komisionerit "Mbi përpunimin e të dhënave të punonjësve në sektorin privat", i ndryshuar (në vijim "Udhëzimi nr. 11").

   Zyra e Komisionerit vlerëson se 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, në përputhje me Udhëzimin nr. 11.

3. Veprimtaria e Kontrolluesit për përpunimin e të dhënave personale realizohet, ndër të tjera, nëpërmjet një sistemi elektronik për administrimin e abonentëve, kontratave, konsumit dhe faturimit, i cili përdoret për administrimin e marrëdhënies së Kontrolluesit me abonentët dhe realizimin e proceseve që lidhen me ofrimin dhe faturimin e shërbimit.

   Nga verifikimi i ndërfaqes së sistemit elektronik rezulton se ky sistem përmban funksionalitete të ndryshme për administrimin e abonentëve, matësve, konsumit dhe faturimit. Në menunë kryesore të aplikacionit evidentohen module, të tilla si "Administrimi", "Konsumi", "Matësi", "AKM", "Krijo Faturë Zbritëse", "Faturat Zbritëse", "Faturimi", "Faturat Afati Shtesë", "Lista e Kontratave" dhe "Kontrata Debi".

   Nëpërmjet modulit "Administrim Abonenti" realizohet regjistrimi, konsultimi dhe administrimi i informacionit të lidhur me abonentin dhe kontratën përkatëse. Nga ndërfaqja e sistemit rezulton se të dhënat organizohen në seksione të ndryshme, përfshirë informacionin mbi kontratën, abonentin, informacionin e pagesës dhe informacionin mbi matësin.

Në sistem përpunohen kategori të ndryshme të të dhënave personale, përfshirë emrin, mbiemrin, atësinë, adresën, të dhënat e kontaktit, numrin e kontratës, numrin e abonentit, të dhëna identifikuese, të dhëna mbi kategorinë e abonentit, zonën/njësinë përkatëse, informacionin mbi matësin, të dhënat mbi konsumin, faturimin, pagesat dhe detyrimet, si dhe informacione të tjera të lidhura me marrëdhënien ndërmjet Kontrolluesit dhe abonentit.

Nga ndërfaqja e sistemit rezulton gjithashtu se për çdo abonent mund të administrohen të dhëna të lidhura me kontratën e shërbimit, statusin e saj, të dhënat e matësit, kategorinë përkatëse të abonentit dhe informacionin financiar të krijuar gjatë marrëdhënies kontraktore. Në këtë mënyrë, sistemi elektronik përbën një nga burimet kryesore të informacionit të Kontrolluesit dhe mundëson përpunimin e centralizuar të të dhënave personale të abonentëve.

Nëpërmjet moduleve të faturimit dhe konsumit realizohet gjithashtu lidhja e të dhënave identifikuese të abonentit me informacionin mbi konsumin e regjistruar, periudhën e faturimit, faturat e lëshuara, detyrimet dhe pagesat, duke krijuar një historik elektronik të marrëdhënies së abonentit me Kontrolluesin.

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 elektronik, nëpërmjet të cilit përpunohen të dhënat personale të abonentëve;
- nuk disponon një procedurë të dokumentuar që të përcaktojë rolet dhe përgjegjësitë e personave që administrojnë sistemin, si dhe ndarjen e përgjegjësive ndërmjet përdoruesve të zakonshëm dhe përdoruesve me privilegje administrative;
- nuk disponon procedurë të dokumentuar për krijimin, miratimin, ndryshimin, pezullimin dhe çaktivizimin e llogarive të përdoruesve të sistemit;
- nuk disponon procedurë të dokumentuar për përcaktimin dhe rishikimin periodik të të drejtave të aksesit, sipas funksionit, pozicionit dhe nevojës konkrete të përdoruesit për akses në të dhënat personale;
- nuk disponon procedurë të dokumentuar për administrimin e privilegjeve të përdoruesve dhe llogarive administrative, përfshirë autorizimin, monitorimin dhe rishikimin periodik të tyre;
- nuk disponon procedurë të dokumentuar për menaxhimin e kredencialeve dhe fjalëkalimeve të përdoruesve, duke përfshirë kërkesat minimale të sigurisë, ndryshimin, rivendosjen dhe mbrojtjen e tyre;
- nga dokumentacioni i administruar nuk evidentohet një procedurë që përcakton përdorimin e mekanizmave shtesë të autentikimit për aksesin në sistem, në varësi të privilegjeve dhe nivelit të rrezikut;
- nuk disponon procedurë të dokumentuar për gjenerimin, administrimin, ruajtjen dhe analizimin e *log*-eve të sistemit;

- nuk rezulton e dokumentuar mënyra se si evidentohet dhe kontrollohet, kush ka aksesuar profilin e një abonenti, kur është realizuar aksesi dhe çfarë veprimi është kryer mbi të dhënat e tij;
- nuk disponon procedurë të dokumentuar për auditimin periodik të veprimeve të përdoruesve, përfshirë konsultimin, regjistrimin, ndryshimin, korrigjimin, eksportimin apo fshirjen e të dhënave personale;
- nuk disponon procedurë të dokumentuar për menaxhimin e incidenteve të sigurisë së informacionit dhe cenimeve të të dhënave personale, duke përfshirë identifikimin, raportimin e brendshëm, klasifikimin, dokumentimin, përshkallëzimin dhe trajtimin e tyre;
- nuk disponon procedurë të dokumentuar për vlerësimin e incidenteve të sigurisë nga këndvështrimi i cenimit të të dhënave personale dhe përcaktimin e përgjegjësive për trajtimin e tyre;
- nuk disponon procedurë të dokumentuar për identifikimin, vlerësimin dhe menaxhimin e cenueshmërive teknike të sistemit elektronik dhe infrastrukturës mbështetëse;
- nuk disponon procedurë të dokumentuar për menaxhimin e përditësimeve dhe *patch*-eve të sigurisë të aplikacionit, sistemit operativ, serverëve dhe komponentëve të tjerë mbështetës;
- nuk disponon procedurë të dokumentuar për testimin periodik të sigurisë së sistemit, përfshirë skanimin e cenueshmërive, testimin e konfigurimeve dhe testimet e tjera të sigurisë;
- nuk disponon procedurë të dokumentuar për *backup*-in e databazës dhe të dhënave personale të administruara në sistem, ku të përcaktohen periodiciteti, përgjegjësitë, afatet e ruajtjes dhe masat e sigurisë për kopjet rezervë;
- nuk disponon procedurë të dokumentuar për testimin periodik të rikthimit të të dhënave nga *backup*-et, me qëllim verifikimin e mundësisë së rikthimit të disponueshmërisë dhe aksesit në të dhënat personale pas një incidenti fizik ose teknik;
- nuk disponon procedurë të dokumentuar për vazhdimësinë e funksionimit dhe rikuperimin e sistemit pas incidenteve apo fatkeqësive (*Business Continuity/Disaster Recovery*);
- nuk disponon procedurë të dokumentuar për ruajtjen dhe fshirjen e të dhënave personale të abonentëve, ku të përcaktohen afatet konkrete të ruajtjes sipas kategorisë dhe qëllimit të përpunimit;
- nuk rezulton e dokumentuar mënyra e trajtimit të të dhënave të abonentëve pas përfundimit të marrëdhënies kontraktore, përfshirë kriteret për ruajtjen, arkivimin, anonimizimin ose fshirjen e tyre;
- nuk disponon procedurë të dokumentuar për eksportimin, shkarkimin dhe transferimin e të dhënave personale nga sistemi, duke mos qenë të përcaktuar personat që mund të kryejnë këto veprime dhe kushtet në të cilat ato lejohen;
- nuk disponon procedurë të dokumentuar për administrimin e pajisjeve fundore nga të cilat aksesohet sistemi elektronik;
- nuk disponon procedurë të dokumentuar për menaxhimin e ndryshimeve (*change management*) në aplikacion, databazë dhe infrastrukturën mbështetëse;

- nuk disponon procedurë të dokumentuar për aksesin e ofruesve të jashtëm të shërbimeve TIK në sistem dhe databazën e abonentëve, përfshirë autorizimin, kufizimin, monitorimin dhe ndërprerjen e aksesit të tyre;
- nuk rezulton i dokumentuar një proces periodik për identifikimin, analizimin dhe vlerësimin e rreziqeve që lidhen me përpunimin elektronik të të dhënave personale të abonentëve;
- nuk rezulton i dokumentuar një proces për testimin, vlerësimin dhe analizimin periodik të efektivitetit të masave teknike dhe organizative të zbatuara për mbrojtjen e sistemit dhe të dhënave personale që administrohen në të;
- nuk rezulton e dokumentuar në mënyrë të plotë infrastruktura teknike mbi të cilën hostohet sistemi, arkitektura e tij, serverët dhe databazat e përdorura, segmentimi i rrjetit, mekanizmat e mbrojtjes së komunikimit dhe ndërveprimi i sistemit me sisteme të tjera;
- nuk rezulton i dokumentuar inventari i sistemeve, pajisjeve dhe aseteve TIK që marrin pjesë në përpunimin e të dhënave personale;
- nuk rezulton e dokumentuar një skemë e rrjedhës së të dhënave personale (*data flow*), e cila të evidentojë burimin e të dhënave, sistemet ku regjistrohen, përdoruesit që i aksesojnë, marrësit e mundshëm dhe destinacionin e tyre gjatë gjithë ciklit të përpunimit.

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, në përputhje me nenet 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 elektronik "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 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.

   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.

   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. 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.

6. Rezulton se Kontrolluesi ka nënshkruar kontratë shërbimi nr. 24 prot., datë 10.01.2023, me subjektin Unioni Financiar Tiranë, me objekt "Pagesën e faturave të ujit nëpërmjet Union Financiar Tiranë sh.a.".

   Nga shqyrtimi i përmbajtjes së kontratës së mësipërme konstatohet se në asnjërën prej tyre 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. Nga shqyrtimi i dokumentacionit të vendosur në dispozicion rezulton se Kontrolluesi disponon rregulloren (e cila nuk rezulton të jetë e miratuar) "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale". Megjithatë, nga shqyrtimi i përmbajtjes së saj rezulton se në të nuk janë të parashikuara rregulla specifike mbi mënyrën e përpunimit të të dhënave personale, si mënyra e mbledhjes dhe regjistrimit, si dhe masat konkrete tekniko-organizative që aplikohen nga Kontrolluesi në funksion të ruajtjes dhe konfidencialitetit të të dhënave, 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 Kontrolluesi duhet të rishikojë dhe të plotësojë rregulloren "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale", duke e miratuar atë nga strukturat përkatëse dhe duke përfshirë në të rregulla specifike që të pasqyrojnë në mënyrë të plotë proceset aktuale të përpunimit të të dhënave personale.

   Në këtë kuadër, rregullorja duhet të parashikojë mënyrën e mbledhjes dhe regjistrimit të të dhënave personale, kategoritë e të dhënave që përpunohen, qëllimet dhe bazat ligjore të përpunimit, nivelet e aksesit të personelit në të dhëna, si dhe masat konkrete teknike dhe organizative të zbatuara për garantimin e sigurisë dhe konfidencialitetit të të dhënave, në përputhje me parashikimet e neneve 27 dhe 28 të Ligjit.

   Zyra e Komisionerit vlerëson se dispozita e nenit 27 të Ligjit i detyron kontrolluesit të mbajnë dokumentacion të detajuar për veprimtaritë e tyre të përpunimit, në mënyrë që të jenë në gjendje të demonstrojnë përputhshmërinë me Ligjin në çdo kohë. Mosdisponimi i një rregulloreje të miratuar dhe të plotë, që të pasqyrojë masat teknike dhe organizative të zbatuara, sipas kërkesave të Vendimit nr. 6, datë 05.08.2013, të Komisionerit "Për përcaktimin e rregullave të hollësishme për sigurimin e të dhënave personale", demonstron mungesë të kapaciteteve organizative për garantimin e një sistemi të integruar të mbrojtjes së të dhënave personale.

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:

- Rregullore "Për administrimin, aksesin, ruajtjen dhe fshirjen e të dhënave imazh/video të sistemit të video-survejimit";
- Procedura e menaxhimit të aksesit, privilegjeve dhe fjalëkalimeve;
- Politika e sigurisë së informacionit;
- Procedura e *log*-eve dhe auditimit të veprimeve;
- Procedura e menaxhimit të cenueshmërive, përditësimeve dhe testimit të sigurisë;
- Procedura e *backup*-it, rikthimit dhe vazhdimësisë së funksionimit (BC/DR);
- Procedura e ruajtjes, fshirjes dhe eksportimit të të dhënave të abonentëve;
- Pajisjet fundore, menaxhimi i ndryshimeve dhe aksesi i ofruesve të jashtëm;
- Vlerësimi i rrezikut dhe testimi i efektivitetit të masave;
- Dokumentacioni teknik, inventari i aseteve TIK dhe rrjedhjes së të dhënave.

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, 30, 33 dhe 81- 84 të Ligjit, Komisioneri,

REKOMANDON:

1. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Elbasan" 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 Elbasan" 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, si dhe të drejtat e subjektit të të dhënave.

3. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Elbasan" 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 Elbasan" sh.a., në zbatim të neneve 27 dhe 28 të Ligjit, të ketë në vëmendje 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 Elbasan" 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 Elbasan" 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 Elbasan" 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/elbasan.

8. Kontrolluesi shoqëria "Ujësjellës Kanalizime Elbasan" 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 pikën 1 më sipër;
   ii) brenda 15 (pesëmbëdhjetë) ditëve, detyrimin e përcaktuar në pikat 2 dhe 6 më sipër;
   iii) brenda 30 (tridhjetë) ditëve, detyrimet e përcaktuara në pikat 3, 4 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