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. 2793/5 prot. Tiranë, më 13.11.2026

REKOMANDIM

Nr. 73, datë 13.11.2026

PËR KONTROLLUESIN, SHOQËRIA "UJËSJELLËS KANALIZIME GJIROKASTËR" 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 ngarkim të Kontrolluesit "Ujësjellës Kanalizime Gjirokastër sh.a." (në vijim "Kontrolluesi"),

KONSTATOHET SE:

Në zbatim të Urdhrit nr. 202, 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 M23329601L, 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", "konsumatorë/abonentë", "vizitorë" etj. Përpunimi i të dhënave personale kryhet në mënyrë manuale dhe elektronike.

2. Kontrolluesi administron në arkivin fizik dosjet e personelit aktual dhe të larguar. Nga verifikimi i dokumentacionit të administruar konstatohet se në dosjet e personelit aktual, ndër të tjera, disponohet "certifikatë familjare" e punonjësve.

   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 administron në arkivin fizik dosje të personelit të larguar të cilat, ndër të tjera, përmbajnë "fotokopje e dokumentit të identitetit", "diplomë", "listë notash", "akti i emërimit", "raport mjekoligjor" etj.

   Nga shqyrtimi i akteve të vendosura në dispozicion grupit të hetimit rezulton se Kontrolluesi nuk ka parashikuar afate të ruajtes si dhe procedura për fshirjen/asgjësimin e dokumentacionit pas përmbushjes së qëllimit për të cilin janë mbledhur, në kundërshtim kjo me parimin e kufizimit të ruajtes në kohë sipas parashikimit të pikës 5 të nenit 6 të Ligjit, që nënkupton që të dhënat mbahen në një formë që lejon identifikimin e subjekteve të të dhënave për një periudhë jo më të gjatë sesa është e nevojshme për qëllimin për të cilin ato përpunohen.

   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 pikën 2 të nenit 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").

   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.

   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 pikën 2 të nenit 6 dhe nenin 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 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, që në momentin e mbledhjes së të dhënave personale.

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 "Flare Billing", i cili përdoret për administrimin e abonentëve të shërbimit të ujësjellës kanalizimeve, kontratave të shërbimit, matësve, leximeve të konsumit, faturimit, arkëtimit, detyrimeve financiare, marrëveshjeve të pagesës me këste, taksave dhe tarifave vendore, si dhe kërkesave, ankesave dhe verifikimeve të abonentëve. Sistemi përmban module funksionale të ndërlidhura, nëpërmjet të cilave realizohet regjistrimi, konsultimi, përditësimi, korrigjimi, ruajtja, gjenerimi dhe eksportimi i informacionit që lidhet me abonentët dhe marrëdhënien e tyre me Kontrolluesin.

   Nga verifikimi i ndërfaqes së sistemit rezulton se në modulin e administrimit të abonentëve përpunohen të dhëna identifikuese dhe të kontaktit, përfshirë numrin e kontratës, numrin e serisë, numrin e abonentit, emrin, mbiemrin, datëlindjen, llojin dhe numrin e dokumentit të identifikimit, numrin personal, adresën e banimit, rrugën, pallatin, shkallën, apartamentin, qytetin, numrin e telefonit dhe adresën e postës elektronike. Gjithashtu administrohen të dhëna mbi kategorinë dhe statusin e kontratës, njësinë administrative, zonën, bllokun, planin tarifor, mënyrën e faturimit dhe numrin e familjarëve në rastet e faturimit aforfe.

   Nëpërmjet këtij moduli realizohet krijimi i kartelës elektronike të abonentit, në të cilën informacioni identifikues dhe i kontaktit lidhet me të dhënat kontraktore, teknike dhe financiare. Sistemi përmban fusha për regjistrimin e komenteve dhe shënimeve, si dhe funksionalitete për ngarkimin e dokumenteve elektronike që lidhen me abonentin. Fushat e shënimeve mundësojnë regjistrimin e informacionit në tekst të lirë, ndërsa funksionaliteti i ngarkimit të dokumenteve krijon mundësinë e administrimit të dokumentacionit shtesë në format elektronik.

   Gjithashtu, sistemi mundëson administrimin e historikut të ndryshimeve për çdo abonent, duke pasqyruar ndryshimet në të dhënat identifikuese, adresën, informacionin kontraktor, të dhënat e faturimit dhe të dhënat për matësit. Ky funksionalitet krijon mundësinë e evidentimit të ndryshimeve në kartelën e abonentit, por kërkon kontrolle të dokumentuara për gjurmueshmërinë, integritetin dhe mbrojtjen e regjistrimeve të aktivitetit.

   Nëpërmjet modulit të matësve dhe leximeve realizohet regjistrimi i matësve të ujit, lidhja e tyre me kontratat dhe abonentët, administrimi i numrave identifikues dhe

karakteristikave teknike, datave të instalimit, ndërrimit dhe historikut të matësve. Gjithashtu regjistrohen leximet e konsumit sipas periudhave përkatëse, duke mundësuar përllogaritjen e sasisë së konsumuar dhe lidhjen e saj me faturimin. Sistemi përmban funksionalitete për gjenerimin e raporteve të leximeve dhe evidentimin e abonentëve për të cilët nuk janë regjistruar lexime.

Nëpërmjet moduleve të faturimit, planeve tarifore dhe artikujve realizohet administrimi i kategorive të shërbimeve, çmimeve, tarifave, periudhave të faturimit dhe përllogaritja e detyrimeve të abonentëve. Sistemi mundëson krijimin dhe administrimin e faturave, konsultimin e historikut të faturimit, evidentimin e detyrimeve të papaguara, kamatëvonesave dhe balancave kreditore. Gjithashtu përmban funksionalitete për krijimin e faturave zbritëse dhe korrigjimin e elementeve të faturave të mëparshme, duke mundësuar ndryshime në informacionin financiar të lidhur me abonentin.

Nëpërmjet modulit të marrëveshjeve për pagesë me këste (AKM) realizohet administrimi i marrëveshjeve për shlyerjen e detyrimeve, përcaktimi i planeve të pagesës, regjistrimi i kësteve, përllogaritja e vlerave financiare dhe kamatëvonesave, si dhe anulimi i marrëveshjeve. Në këtë proces përpunohen të dhëna identifikuese, kontraktore dhe financiare, të lidhura me historikun e detyrimeve dhe mënyrën e shlyerjes së tyre.

Nëpërmjet modulit të arkëtimit realizohet administrimi i arkave, caktimi i tyre për operatorët, regjistrimi i pagesave dhe krijimi i mandateve të arkëtimit. Sistemi mundëson regjistrimin e pagesave të plota dhe të pjesshme, shpërndarjen e shumave të arkëtuara ndërmjet detyrimeve dhe evidentimin e gjendjes financiare të abonentëve. Gjithashtu përmban funksionalitete për anulimin dhe korrigjimin e mandateve të arkëtimit, si dhe regjistra të veçantë për mandatet e anuluara dhe mandatet me data të modifikuara.

Nga verifikimi i funksionaliteteve të arkëtimit rezulton se sistemi parashikon nivele të ndryshme autorizimi për operatorët, përfshirë përdorues me të drejta të zgjeruara për kryerjen e veprimeve në arka të tjera dhe regjistrimin e mandateve me data të mëparshme. Këto funksionalitete mundësojnë ndërhyrje në informacionin financiar dhe historikun e transaksioneve të abonentëve, për të cilat nevojiten kontrolle të dokumentuara mbi autorizimin, ndarjen e detyrave dhe gjurmueshmërinë e veprimeve.

Nëpërmjet modulit të konsultimit dhe raportimit realizohet aksesimi i informacionit të detajuar mbi abonentët, faturat, pagesat, transaksionet, detyrimet dhe balancat. Sistemi mundëson filtrimin e informacionit sipas parametrave të ndryshëm, gjenerimin e raporteve, printimin dhe shkarkimin e faturave në format PDF, si dhe eksportimin e të dhënave në format Excel. Për rrjedhojë, të dhënat personale dhe financiare mund të nxirren nga mjedisi i aplikacionit dhe të ruhen në skedarë elektronikë jashtë tij.

Nëpërmjet modulit të ankesave dhe verifikimit të abonentëve realizohet regjistrimi, administrimi dhe trajtimi i kërkesave dhe ankesave, si dhe dokumentimi i verifikimeve të kryera. Në këto procese përpunohen të dhëna identifikuese, të kontaktit, të dhëna kontraktore, përmbajtja e ankesave, rezultatet e verifikimeve dhe dokumentacioni shoqërues. Sistemi parashikon gjithashtu regjistrimin e numrit personal, ngarkimin e

fotografive ose kopjeve të dokumenteve të identifikimit, fotografive të matësve dhe imazheve të nënshkrimeve të abonentëve.

Nëpërmjet modulit të sigurisë realizohet administrimi i përdoruesve dhe roleve të sistemit. Nga verifikimi i ndërfaqes rezulton se për përdoruesit administrohen të dhëna mbi emrin, mbiemrin, emrin e përdoruesit, adresën elektronike, rolin, statusin dhe datën e krijimit. Sistemi mundëson krijimin, ndryshimin dhe administrimin e roleve, si dhe caktimin e privilegjeve për funksionalitetet përkatëse. Në ndërfaqen e përdoruesve evidentohen llogari me role dhe të drejta të ndryshme, përfshirë përdorues aktivë dhe privilegje të lidhura me administrimin e abonentëve, faturimin dhe funksione të tjera të aplikacionit.

Aksesi në sistem realizohet nëpërmjet një ndërfaqeje autentikimi me emër përdoruesi dhe fjalëkalim. Sistemi përmban opsionin "Më mbaj mend", si dhe funksionalitete për ndryshimin dhe rivendosjen e fjalëkalimit, përfshirë verifikimin nëpërmjet një kodi të dërguar në adresën elektronike të përdoruesit.

Për rrjedhojë, nëpërmjet sistemit "Flare Billing" realizohet përpunimi i kombinuar i të dhënave identifikuese, të kontaktit, kontraktore, familjare, teknike, financiare, dokumenteve elektronike, fotografive dhe imazheve të nënshkrimeve, duke mundësuar lidhjen e tyre me një abonent dhe kontratë konkrete. Funksionalitetet e sistemit lejojnë aksesimin, ndryshimin, korrigjimin, anulimin, raportimin dhe eksportimin e informacionit, përfshirë veprime që ndikojnë drejtpërdrejt në konfidencialitetin dhe integritetin e të dhënave personale.

Nga verifikimi i sistemit elektronik dhe dokumentacionit të administruar, në lidhje me masat teknike dhe organizative të sigurisë, konstatohet se Ujësjellës Kanalizime Gjirokastër nuk paraqiti dokumentacion dhe evidenca. Konkretisht, Kontrolluesi:

- nuk disponon politika dhe procedura të dokumentuara për administrimin, përdorimin dhe sigurinë e sistemit elektronik "Flare Billing", nëpërmjet të cilit realizohet përpunimi i të dhënave personale të abonentëve;
- nuk disponon procedurë të dokumentuar që të përcaktojë qëllimet, mënyrën dhe rregullat e përdorimit të sistemit, kategoritë e përdoruesve, përgjegjësitë e tyre dhe kufizimet përkatëse gjatë përpunimit të të dhënave personale;
- nuk rezulton i dokumentuar një proces periodik për identifikimin, analizimin dhe vlerësimin e rreziqeve që lidhen me përpunimin elektronik të të dhënave personale nëpërmjet sistemit, përfshirë rreziqet e aksesit të paautorizuar, ndryshimit, humbjes, zbulimit ose shkatërrimit të të dhënave;
- nuk disponon procedurë të dokumentuar për krijimin, miratimin, ndryshimin, pezullimin dhe çaktivizimin e llogarive të përdoruesve, përfshirë rastet e ndryshimit të detyrës ose përfundimit të marrëdhënies së punës;
- nuk disponon një matricë të miratuar të roleve dhe privilegjeve, ku të përcaktohen të drejtat e aksesit për secilin funksion, modul dhe kategori të të dhënave personale;
- nuk disponon procedurë të dokumentuar për rishikimin periodik të të drejtave të aksesit, në raport me detyrat dhe përgjegjësitë konkrete të përdoruesve, si dhe për identifikimin dhe heqjen e privilegjeve të panevojshme;

- nuk disponon procedurë të dokumentuar për administrimin dhe kontrollin e llogarive me privilegje administrative, përfshirë identifikimin e administratorëve, autorizimin e veprimeve të tyre dhe monitorimin e ndryshimeve të kryera në konfigurimet e sistemit;
- nuk rezulton i dokumentuar procesi i miratimit dhe gjurmueshmërisë së ndryshimeve të roleve dhe privilegjeve, përfshirë përdoruesin që ka kryer ndryshimin, datën, arsyen dhe autorizimin përkatës;
- nuk disponon procedurë të dokumentuar për ndarjen e detyrave ndërmjet përdoruesve që administrojnë abonentët, regjistrojnë leximet, gjenerojnë faturat, arkëtojnë pagesat, korrigjojnë detyrimet dhe administrojnë të drejtat e aksesit;
- nuk disponon procedurë të dokumentuar për administrimin e privilegjeve të operatorëve të arkëtimit, veçanërisht për përdoruesit që mund të kryejnë veprime në arka të tjera, të anulojnë mandate ose të regjistrojnë transaksione me data të mëparshme;
- nuk disponon politikë të dokumentuar për menaxhimin e kredencialeve dhe fjalëkalimeve, përfshirë kërkesat e sigurisë, ruajtjen, rivendosjen, kufizimin e tentativave të pasuksesshme dhe bllokimin e llogarive;
- nuk rezulton i dokumentuar një vlerësim i rrezikut mbi mekanizmin e autentikimit të përdorur, përfshirë nevojën për autentikim me shumë faktorë (MFA/2FA), veçanërisht për llogaritë me privilegje administrative dhe përdoruesit që kryejnë operacione kritike;
- nuk rezulton e dokumentuar mënyra e mbrojtjes së *cookies* dhe sesioneve të autentikimit, përfshirë përdorimin e parametrave të sigurisë Secure, HttpOnly dhe SameSite, si dhe masat për parandalimin e rrëmbimit ose ripërdorimit të sesioneve;
- nuk disponon procedurë të dokumentuar për administrimin e kodeve të verifikimit që dërgohen me *email* gjatë rivendosjes së fjalëkalimit, përfshirë vlefshmërinë kohore, kufizimin e tentativave dhe përdorimin vetëm një herë të kodit;
- nuk disponon procedurë të dokumentuar për regjistrimin, ruajtjen, mbrojtjen, monitorimin dhe analizimin e *log*-eve të aktivitetit të përdoruesve;
- nuk rezulton e dokumentuar në mënyrë të plotë gjurmueshmëria e aksesimit të kartelave të abonentëve, konsultimit të dokumenteve të identifikimit, ndryshimit të të dhënave kontraktore, shkarkimit të dokumenteve dhe eksportimit të raporteve;
- nuk rezulton e dokumentuar mënyra e mbrojtjes së historikut të ndryshimeve të abonentëve nga ndërhyrja, ndryshimi ose fshirja e paautorizuar, si dhe afati i ruajtjes së regjistrimeve përkatëse;
- nuk disponon procedurë për auditimin periodik të operacioneve që ndikojnë në informacionin financiar, përfshirë korrigjimin e faturave, krijimin e faturave zbritëse, anulimin e marrëveshjeve me këste dhe anulimin ose ndryshimin e mandateve të arkëtimit;
- nuk rezulton i dokumentuar një mekanizëm i plotë kontrolli për operacionet e anulimit dhe korrigjimit të mandateve, përfshirë autorizimin, regjistrimin e arsyes së veprimit, ruajtjen e vlerave përpara dhe pas ndryshimit dhe lidhjen ndërmjet mandatit të anuluar dhe mandatit të ri;

- nuk disponon procedurë të dokumentuar për kontrollin e ndryshimeve të datave të transaksioneve dhe regjistrimin e mandateve me data të mëparshme, përfshirë autorizimin, monitorimin dhe verifikimin periodik të këtyre veprimeve;
- nuk rezulton i dokumentuar një proces periodik për rakordimin dhe kontrollin e integritetit të informacionit ndërmjet leximeve, faturave, pagesave, mandateve të arkëtimit, balancave kreditore dhe marrëveshjeve me këste;
- nuk disponon procedurë të dokumentuar për administrimin e komenteve dhe shënimeve në tekst të lirë mbi abonentët, përfshirë përcaktimin e kategorive të informacionit që lejohen të regjistrohen, kufizimin e të dhënave të panevojshme dhe kontrollin e aksesit;
- nuk disponon procedurë të dokumentuar për administrimin e dokumenteve elektronike të ngarkuara në sistem, përfshirë kategoritë e dokumenteve, qëllimin e mbledhjes, personat e autorizuar për akses, afatet e ruajtjes dhe fshirjen e tyre;
- nuk disponon procedurë të dokumentuar për mbrojtjen e kopjeve ose fotografive të dokumenteve të identifikimit dhe imazheve të nënshkrimeve të abonentëve, përfshirë kufizimin e konsultimit, shkarkimit, transmetimit dhe përdorimit të tyre;
- nuk rezulton i dokumentuar mekanizmi i kontrollit të skedarëve të ngarkuar në sistem, përfshirë kufizimin e formateve të lejuara, kontrollin ndaj përmbajtjeve keqdashëse dhe parandalimin e ekzekutimit të skedarëve të paautorizuar;
- nuk rezulton e dokumentuar mënyra se si kontrollohet lidhja ndërmjet dokumenteve të identifikimit, fotografive të matësve, imazheve të nënshkrimeve, numrit të kontratës dhe abonentit përkatës, për të parandaluar regjistrimin ose aksesimin e gabuar të informacionit;
- nuk disponon procedurë të dokumentuar për administrimin e të dhënave të mbledhura gjatë verifikimeve të abonentëve, përfshirë procesverbalet, konstatimet, fotografitë, dokumentet shoqëruese dhe përgjegjësitë e përdoruesve që kryejnë verifikimet;
- nuk disponon procedurë të dokumentuar për eksportimin, shkarkimin, printimin dhe transferimin e të dhënave personale nga sistemi, përfshirë përcaktimin e përdoruesve të autorizuar, qëllimin e eksportimit dhe kufizimet mbi volumin e informacionit;
- nuk rezulton i dokumentuar një mekanizëm për regjistrimin dhe monitorimin e eksportimeve të raporteve në format Excel ose PDF, përfshirë identitetin e përdoruesit, kohën e veprimit dhe kategorinë e informacionit të eksportuar;
- nuk disponon procedurë të dokumentuar për mbrojtjen e skedarëve elektronikë të eksportuar, përfshirë ruajtjen në pajisjet fundore, transmetimin, kufizimin e aksesit dhe fshirjen e kopjeve lokale;
- nuk disponohet dokumentacion i plotë mbi arkitekturën teknike të sistemit, përfshirë serverët ku hostohet aplikacioni, teknologjinë dhe konfigurimin e bazës së të dhënave, komponentët e rrjetit dhe mënyrën e komunikimit ndërmjet 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 personale dhe kopjeve rezervë;
- nuk rezulton i dokumentuar inventari i aseteve TIK që marrin pjesë në mbledhjen, transmetimin, ruajtjen dhe përpunimin e të dhënave personale nëpërmjet sistemit;

- nuk disponon 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 dhe mbrojtja e komponentëve të aplikacionit dhe bazës së të dhënave, përfshirë segmentimin e rrjetit, rregullat e *firewall*-it dhe kufizimin e komunikimeve ndërmjet sistemeve;
- nuk rezulton e dokumentuar mënyra e mbrojtjes së të dhënave gjatë transmetimit ndërmjet pajisjeve të përdoruesve, aplikacionit, bazës së të dhënave dhe sistemeve të integruara, 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 dokumentet identifikuese dhe informacionin financiar;
- nuk disponon procedurë të dokumentuar për administrimin e privilegjeve të aksesit në bazën e të dhënave, përfshirë llogaritë teknike, llogaritë administrative, kufizimin e aksesit të drejtpërdrejtë dhe auditimin e operacioneve kritike;
- nuk disponon procedurë të dokumentuar për menaxhimin e cenueshmërive teknike të aplikacionit *web*, serverëve, bazës së të dhënave dhe komponentëve të tjerë të infrastrukturës;
- nuk disponon procedurë të dokumentuar për menaxhimin e përditësimeve dhe *patch*-eve të sigurisë, përfshirë identifikimin, vlerësimin, planifikimin, instalimin dhe verifikimin e përditësimeve;
- nuk disponon evidenca të mjaftueshme 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 aplikacioni dhe serveri, për të verifikuar se ndryshimi i identifikuesve të abonentëve, kontratave, faturave ose mandateve nuk mundëson akses ose ndërhyrje të paautorizuar;
- nuk disponon 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 disponon dokumentacion mbi integrimet e sistemit me shërbimet e tjera dhe sistemet e palëve të treta, përfshirë kategoritë e të dhënave që shkëmbehen, protokollet e komunikimit, autentikimin dhe autorizimin e sistemeve;
- nuk rezulton e dokumentuar marrëdhënia ndërmjet Kontrolluesit dhe zhvilluesit, mirëmbajtësit apo ofruesit të sistemit, përfshirë përgjegjësitë për sigurinë, kushtet e aksesit dhe përpunimin e të dhënave personale;
- nuk disponon 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 disponon procedurë të dokumentuar për krijimin dhe administrimin e kopjeve rezervë të bazës së të dhënave, dokumenteve elektronike dhe komponentëve të

aplikacionit, ku të përcaktohen periodiciteti, përgjegjësitë, vendndodhja dhe afatet e ruajtjes;

- nuk disponon evidenca të mjaftueshme 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 disponon 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 disponon 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 dhe përgjegjësitë për rikuperimin;
- nuk disponon procedurë të dokumentuar për identifikimin, raportimin, regjistrimin, klasifikimin, analizimin dhe trajtimin e incidenteve të sigurisë së informacionit;
- nuk disponon 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 disponon 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 dokumenteve të identifikimit, fotografive të matësve, imazheve të nënshkrimeve, shënimeve, ankesave, verifikimeve dhe regjistrave të aktivitetit;
- nuk rezulton e dokumentuar rrjedha e të dhënave personale (*data flow*), nga momenti i mbledhjes dhe regjistrimit, lidhja me kontratën dhe abonentin, përpunimi në modulet e faturimit dhe arkëtimit, shkëmbimi me sisteme të tjera, eksportimi dhe deri në arkivimin ose fshirjen e tyre;
- nuk disponon 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 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 "Flare-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 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 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, 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.

6. Rezulton se Kontrolluesi ka nënshkruar disa kontrata, konkretisht:

   - Kontratë shërbimi nr. 3339 prot., datë 05.12.2024, me subjektin, shoqëria "KREATX" sh.p.k., me objekt "Mirëmbajtje e programit të faturimit dhe fiskalizimit";
   - Kontratë shërbimi nr. 312 prot., datë 09.02.2023, me subjektin, shoqëria "Ak Invest" sh.a., me objekt "Pagesa e faturave të ujit nëpërmjet "Ak Invest" sh.a.".

   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 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, pavarësisht sasisë së të dhënave personale që përpunon, nuk disponon rregullore të posaçme "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale", në të cilën të parashikohen rregulla specifike mbi kategoritë e të dhënave personale që përpunohen, 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 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. Rezulton 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 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 së 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, si dhe 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.

   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, me shkresën nr. 2304/1 prot., datë 29.10.2026, administruar me tonën me nr. 2304/1 prot., datë 29.10.2026, gjatë seancës dëgjimore janë dorëzuar pretendimet me shkrim lidhur me konstatimet e procesverbalit të hetimit, si dhe është dorëzuar dokumentacioni, si vijon:

- Urdhër nr. 271, datë 26.10.2026 dhe shkresë nr. 2269 prot., datë 26.10.2026 "Për detyrë shtesë", për emërimin e nëpunësit për mbrojtjen e të dhënave personale;
- Shkresë nr. 2311 prot., datë 28.10.2026 "Matrica e përdoruesve të sistemit të faturimit";
- Shkresë nr. 2288 prot., datë 27.10.2026 "Për thirrjen e Këshillit Mbikëqyrës të shoqërisë rajonale Ujësjellës Kanalizime Gjirokastër sh.a.";
- Deklarata konfidencialiteti (11 fletë);
- Memo nr. 2287 prot., datë 27.10.2026 "Për plotësimin dhe nënshkrimin e deklaratave të konfidencialitetit";
- Format Formular nr. 1 për hapje kontrate me abonent.

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 Gjirokastër" 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 Gjirokastër" 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.

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

4. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Gjirokastër" 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 Gjirokastër" 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 Gjirokastër" 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 Gjirokastër" 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 Gjirokastër" 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 Gjirokastër" 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 Gjirokastër" 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/gjirokastër.

11. Kontrolluesi, shoqëria "Ujësjellës Kanalizime Gjirokastër" 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 8 dhe 10 më sipër;
    iii) brenda 30 (tridhjetë) ditëve, detyrimet e përcaktuara në pikat 4, 5 dhe 6 më sipër;
    iv) brenda 45 (dyzet e pesë) ditëve, detyrimin e përcaktuar në pikat 7, 9 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