



**REPUBLIKA E SHQIPËRISË**  
**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. 18 prot.

Tiranë, më 12.06.2026

**VENDIM**

**Nr. 18, datë 12.06.2026**

**PËR KONTROLLUESIN SHOQËRIA “PROGEEN” SHPK**

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 dhe provave të administruara në përfundim të hetimit administrativ në ngarkim të Kontrolluesit Shoqëria “Progeen” shpk (në vijim, “Kontrolluesi”),

**KONSTATOHET SE:**

Në zbatim të Urdhrit nr. 78, datë 10.04.2026 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim, “Komisioneri”), u krijua grupi i punës, i cili kreu hetimin administrativ pranë Kontrolluesit, me objekt:

- *Zbatimi i ligjit nr. 124/2024 “Për mbrojtjen e të dhënave personale” dhe akteve të miratuara nga Komisioneri në lidhje me mbledhjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale, gjatë kryerjes së aktivitetit nga Kontrolluesi.*

Komisioneri, pasi shqyrtoi relacionin e grupit të hetimit, procesverbalin e hetimit administrativ dhe provat e administruara gjatë ushtrimit të hetimit pranë Kontrolluesit, vëren se:

1. Kontrolluesi është person juridik i organizuar në formën e një shoqërie tregtare me përgjegjësi të kufizuar, i regjistruar në Qendrën Kombëtare të Biznesit me NUIS L32113001C me objekt aktiviteti: “*Import, eksport, tregtia me shumicë dhe pakicë e mallrave, sipërmarrja dhe shërbimi në fusha të ndryshme etj.,*”

“Progeen” shpk është një kompani e specializuar në ofrimin e shërbimeve në fushën e ndërtimit dhe çdo veprimtari në lidhje me të. Në kuadër të veprimtarisë që ushtron, Kontrolluesi mbledh dhe përpunon të dhëna personale për kategorinë e të dhënave “punonjës”, “klientë”, “vizitorë”, etj. Përpunimi i të dhënave personale kryhet në mënyrë manuale dhe elektronike.

2. Kontrolluesi ka publikuar rubrikën “*Politikat e Privatësisë*” në faqen zyrtare të internetit [www.progeen.com](http://www.progeen.com). Megjithatë, konstatohet se janë modele standarde të politikave të privatësisë.

Kontrolluesi nuk informon, në mënyrë të qartë dhe të kuptueshme, subjektet e të dhënave (klientë, vizitorë, punonjës, etj.), për fushën dhe qëllimin për të cilin do të përpunohen të dhënat personale, për mënyrën e përpunimit, personin që do t’i përpunojë të dhënat, të dhënat e kontaktit të nëpunësit të mbrojtjes së të dhënave të Kontrolluesit, afatin e mbajtjes së të dhënave, masat e sigurisë, të drejtat që subjektet e të dhënave gëzojnë (për akses, korrigjim dhe fshirje) etj., në kundërshtim me parashikimet e nenit 13 të Ligjit.

Zyra e Komisionerit vlerëson se, faqja zyrtare e internetit përbën zakonisht pikën e parë të kontaktit ndërmjet Kontrolluesit dhe subjektit të të dhënave, ndaj mungesa e një politike ose publikimi i saj në mënyrë jo të plotë kufizon informacionin e nevojshëm të subjekteve mbi qëllimin dhe mënyrën e përpunimit të të dhënave personale.

Gjithashtu, publikimi i “*Politikave të Privatësisë*” është thelbësor për ushtrimin efektiv të të drejtave të subjekteve të të dhënave. Vetëm përmes informimit të plotë sipas parashikimeve të nenit 13 të Ligjit, subjektet e të dhënave mund të njihen me të drejtat e tyre dhe me mënyrën për t’i ushtruar ato, duke shmangur situatat ku këto të drejta mbeten formale dhe të pazbatueshme në praktikë. Njëkohësisht, ato shërbejnë si mjet parandalues ndaj praktikave jo ligjore ose të njëanshme të Kontrolluesit gjatë përpunimit të të dhënave personale.

3. Rezulton se, Kontrolluesi nuk ka marrë masat e duhura teknike dhe organizative për të garantuar një nivel sigurie të përshtatshëm ndaj rrezikut, duke përfshirë, ndër të tjera, *pseudonimizimin dhe enkriptimin e të dhënave personale; aftësinë për të garantuar konfidencialitetin, integritetin, disponueshmërinë dhe qendrueshmërinë e sistemeve dhe të shërbimeve të përpunimit; aftësinë për të rivendosur disponueshmërinë dhe aksesin në të dhënat personale brenda një kohe të arsyeshme në rast incidenti fizik ose teknik; një proces për testimin, shqyrtimin dhe vlerësimin e rregullt të efikasitetit të masave teknike dhe organizative për të garantuar sigurinë e përpunimit etj.*, në kundërshtim me parashikimet e nenit 28 të Ligjit dhe Vendimit nr. 6, të Komisionerit.

Kontrolluesi, për shkak të 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 "*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*").

Gjithashtu, është konstatuar se, Kontrolluesi nuk mban dokumentacion mbi veprimtaritë e përpunimit, me qëllim demonstrimin e përputhshmërisë me ligjin, në formë të shkruar dhe në format elektronik, sipas parashikimeve të nenit 27 të Ligjit.

Referuar nenit 27 të Ligjit, Kontrolluesi ka detyrimin të mbajë dokumentacion, në format të shkruar dhe elektronik, për veprimtaritë e tij përpunuese në mënyrë që të jetë në gjendje të japë të dhëna lidhur me përputhshmërinë me këtë ligj. Referuar nenit 27 pika 4 e Ligjit, çmohet se Kontrolluesi nuk përfshihet në rrethin e subjekteve të përjashtuar nga detyrimet e nenit 27 pika 1 dhe 2 e Ligjit pasi, edhe pse ka më pak se 250 (dyqind e pesëdhjetë) persona të punësuar, gjatë ushtrimit të aktivitetit të tij të biznesit ai bën përpunim të rregullt e të shtrirë në kohë (pra jo rastësor) për kategorinë e të dhënave "*punonjës*", "*klientë*", etj. (*shih pika 4 e nenit 27 të Ligjit*).

Mungesa e këtij dokumentacioni dhe mosrespektimi i procedurave të brendshme rregullatore për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale, sipas kërkesave të nenit 27 dhe 28 të Ligjit, si dhe Vendimit nr. 6 të Komisionerit, demonstroi mungesë të rregullimit të brendshëm për pajtueshmëri dhe mungesë të kapaciteteve organizative për garantimin e një sistemi të integruar të mbrojtjes së të dhënave personale.

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 "*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 transponon dhe praktika më e mirë evropiane, e konsideron certifikimin si një mekanizëm përputhshmërie me Ligjin<sup>1</sup> 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

---

<sup>1</sup> Pika 3 e nenit 22, pika 3 e nenit 23 dhe pika 3 e nenit 28

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 Udhëzimin nr. 08 dhe nr. 09.

Në rastin konkret, Zyra e Komisionerit vlerëson se, për shkak të natyrës së veprimtarisë që ushtron, e cila kërkon masa të shtuara teknike dhe organizative për garantimin e sigurisë së të dhënave personale, Kontrolluesi duhet të krijojë, mirëmbajë dhe administrojë një sistem menaxhimi të të dhënave personale (PIMS) në përputhje me parashikimet e Udhëzimit nr. 09.

Bazuar në nenin 28 të Ligjit dhe nenin 13 të Udhëzimit nr. 09, Kontrolluesi duhet të marrë masa konkrete teknike dhe organizative, që garantojnë nivel të përshtatshëm për rrezikun, masa të cilat duhet të rishikohen në mënyrë periodike për të siguruar efektivitet të vazhdueshëm.

4. Nga verifikimi në vend, rezulton se Kontrolluesi e ka të organizuar rrjetin e brendshëm të intranetit me pajisje kompjuterike, të cilat nuk janë të qendëruara sipas modelit të domain controller-it apo ekuivalente, duke sjellë mungesën e një arkitekture të unifikuar për administrimin e përdoruesve, autorizimeve dhe politikave të sigurisë. Kjo mënyrë organizimi rrit rrezikun për akses të paautorizuar, mungesë gjurmueshmërie dhe dobësi në menaxhimin e privilegjeve, në kundërshtim me kërkesën e nenit 27 dhe 28 të Ligjit për garantimin e konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave personale përmes masave të përshtatshme teknike.

Në vijim, pajisja e sigurisë që përdor kontrolluesi për infrastrukturën e teknologjisë së informacionit nuk i përgjigjet standardeve më të mira ndërkombëtare, duke mos ofruar mekanizma të avancuar filtrimi, monitorimi dhe parandalimi të ndërhyrjeve (IPS/IDS, etj.), çka cenon kërkesën e nenit 28 të Ligjit për implementimin e masave teknike të përshtatshme në raport me rrezikun.

Zyra e Komisionerit vlerëson se, organizimi i infrastrukturës së teknologjisë së informacionit nga ana e Kontrolluesit, në mungesë të një sistemi të centralizuar për menaxhimin e përdoruesve, autentikimit dhe autorizimeve (si domain controller apo mekanizma ekuivalentë), nuk garanton një nivel të përshtatshëm sigurie në përputhje me kërkesat e nenit 28 të Ligjit nr. 124/2024. Kjo situatë krijon dobësi të konsiderueshme në administrimin e privilegjeve, kontrollin e aksesit dhe

gjurmueshmërinë e veprimeve, duke rritur rrezikun për akses të paautorizuar dhe cenim të konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave personale.

Gjithashtu, Zyra e Komisionerit vlerëson se, përdorimi i një infrastrukture rrjeti të përbashkët me një tjetër kontrollues, pa masa të dokumentuara për segmentim logjik apo fizik, nuk përmbush standardet minimale të sigurisë së përpunimit dhe bie ndesh me parimin e ndarjes së përgjegjësive dhe kontrollit të aksesit, siç kërkohet nga neni 28 i ligjit dhe Vendimit nr. 6, datë 05.08.2013 të Komisionerit “Për përcaktimin e rregullave të hollësishme për sigurimin e të dhënave personale” (në vijim, “Vendimi nr. 6”). Mungesa e këtyre masave rrit ndjeshëm ekspozimin ndaj incidenteve të sigurisë dhe ndërhyrjeve të paautorizuara ndërmjet sistemeve të ndryshme.

Në vijim, Zyra e Komisionerit vlerëson se, pajisjet dhe mekanizmat e sigurisë së përdorur nga Kontrolluesi nuk janë në përputhje me standardet bashkëkohore të sigurisë së informacionit, duke mos garantuar funksionalitete të avancuara për monitorimin, filtrimin dhe parandalimin e ndërhyrjeve (si IDS/IPS), në kundërshtim me parashikimin e nenit 28 të ligjit dhe detyrimet e përcaktuara në Vendimin nr. 6, për marrjen e masave teknike të përshtatshme në raport me nivelin e rrezikut. Për pasojë, niveli i mbrojtjes së të dhënave personale nuk konsiderohet i mjaftueshëm dhe proporcional me natyrën dhe rëndësinë e përpunimeve të kryera.

5. Nga verifikimi *on-site* i infrastrukturës së teknologjisë së informacionit, si dhe nga shqyrtimi i procedurave rregulluese që disponon Kontrolluesi, rezulton se:
  - Kontrolluesi nuk ka hartuar dhe miratuar plane të dokumentuara për menaxhimin e riskut, përfshirë identifikimin, analizimin dhe vlerësimin e rreziqeve që lidhen me përpunimin e të dhënave personale, si dhe nuk ka përcaktuar teknikat dhe mekanizmat përkatës të menaxhimit dhe monitorimit të performancës së masave të sigurisë, në kundërshtim me detyrimin për të garantuar një nivel sigurie të përshtatshëm sipas parimit të llogaridhënies;
  - Nuk ka të hartuar planin e politikave të vazhdueshmërisë së biznesit, dokumente këto që do të duhet të përmbanin politikat dhe objektivat që sigurojnë vijueshmërinë e punës;
  - Nuk ka të specifikuar/dokumentuar kohën maksimale në të cilën shërbimet dhe sistemet nuk mund të jenë funksionale. Nuk janë planifikuar masa që në rast dështimi të një/disa pajisjeve të mos ndikohet në funksionimin e sistemeve dhe shërbimeve të ofruara;
  - Nuk ka kryer auditime të brendshme me qëllim garantimin e mirëfunksionimit të këtyre teknikave për menaxhimin e riskut (ose në mungesë të teknikave, identifikim të riskut);
  - Politikat mbi gjurmët (log-et) për infrastrukturën mbështetëse TIK, nuk zbatohen sipas një procedure të rregulluar, me risk në qasje të paautorizuar në

të dhëna, kërcënim të sigurisë në fushën e teknologjisë së informacionit dhe mungesë transparence.

Gjithashtu, konstatohet se masat e ndërmarra në drejtim të *backup*-it janë të pamjaftueshme dhe nuk japin siguri në mbështetjen e planit të vazhdueshmërisë së biznesit (BCP) dhe planit të rimëkëmbjes nga katastrofa (DRP), në kundërshtim kjo me masat e sigurisë së informacionit. Nuk u gjetën procedurat e rikrijimit (*restore*) të *backup*-it të të dhënave me qëllim testimin e tyre për t'u siguruar që ato janë të efektshme dhe që mund të ekzekutohen brenda kohës së lejuar. Këto procedura duhet të testohen rregullisht, sistematikisht dhe vazhdimisht.

Për sa më sipër, konstatohet se Kontrolluesi nuk ka marrë masa organizative dhe teknike të përshtatshme për të mbrojtur të dhënat personale nga shkatërrime të paligjshme, aksidentale, humbje aksidentale, për të mbrojtur aksesin ose përhapjen nga persona të paautorizuar, veçanërisht në këtë rast kur përpunimi i të dhënave kryhet nëpërmjet komunikimeve elektronike, në kundërshtim me parashikimet e nenit 28 të Ligjit dhe Vendimit nr. 6.

Zyra e Komisionerit vlerëson se, mungesa e një plani të strukturuar për menaxhimin e riskut, e reflektuar në mos hartimin e procedurave për identifikimin, analizimin dhe vlerësimin e rreziqeve, si dhe në mungesën e auditimeve të brendshme dhe monitorimit të vazhdueshëm të masave të sigurisë, cenon drejtpërdrejt parimin e llogaridhënies sipas nenit 6 dhe detyrimet e nenit 28 të Ligjit. Pa një analizë të bazuar në risk, Kontrolluesi nuk është në gjendje të përcaktojë masa të përshtatshme teknike dhe organizative, duke krijuar ekspozim të lartë ndaj incidenteve të sigurisë, aksesit të paautorizuar dhe përpunimeve të paligjshme të të dhënave personale.

Në të njëjtën kohë, mungesa e planeve të vazhdueshmërisë së biznesit (BCP) dhe e planeve të rikuperimit nga katastrofat (DRP), si dhe mos përcaktimi i parametrave kritikë, si koha maksimale e ndërprerjes së shërbimeve (RTO/RPO), tregojnë një mungesë të planifikimit për garantimin e disponueshmërisë dhe integritetit të të dhënave. Këto mangësi rrisin ndjeshëm rrezikun që, në rast dështimi teknik apo incidenti kibernetik, të dhënat personale të mos rikuperohen brenda një afati të pranueshëm ose të humbasin në mënyrë të pakthyeshme, duke cenuar të drejtat dhe interesat e subjekteve të të dhënave.

Gjithashtu, mungesa e procedurave të rregulluara për administrimin e *log*-eve dhe pamjaftueshmëria e masave të *backup*-it, e shoqëruar me mungesën e testimit të rregullt të rikthimit të të dhënave (*restore*), tregon se masat e sigurisë janë të paplota dhe jo efektive në praktikë. Në këto kushte, Kontrolluesi nuk garanton gjurmueshmërinë e veprimeve mbi të dhënat, transparencën dhe aftësinë për të reaguar ndaj incidenteve, duke qenë në kundërshtim me kërkesat e nenit 28 të Ligjit dhe Vendimit nr. 6 të Komisionerit.

6. Konstatohet se, aktivitetet kryesore të Kontrolluesit janë procese përpunimi, të cilat, për shkak të natyrës, fushës së zbatimit ose qëllimeve të tyre, kërkojnë monitorim të rregullt e sistematik të subjekteve të të dhënave në një shkallë të gjerë. Megjithatë, Kontrolluesi nuk ka emëruar një nëpunës të mbrojtjes së të dhënave personale, në kundërshtim me nenin 33 të Ligjit.

Zyra e Komisionerit vlerëson se, aktivitetet e Kontrolluesit përfshijnë procese përpunimi të të dhënave personale që, për shkak të natyrës dhe mënyrës së realizimit të tyre, karakterizohen nga monitorim i vazhdueshëm i subjekteve të të dhënave. Konkretisht, përdorimi i sistemit të video-survejimit (CCTV) për mbikëqyrjen e ambienteve të punës dhe hapësirave përreth, sistemi i hyrje daljeve, numrit të punonjësve, të dhënat e klientëve, përbëjnë forma të përpunimit të cilat realizohen në mënyrë të strukturuar dhe të përsëritur në kohë.

Në këtë kuptim, këto procese përpunimi përbëjnë monitorim të rregullt dhe sistematik të subjekteve të të dhënave, pasi ato nuk janë të rastësishme apo sporadike, por pjesë integrale e ushtrimit të veprimtarisë së Kontrolluesit.

Në këto kushte, në përputhje me nenin 33 të Ligjit, Kontrolluesi ka detyrimin për caktimin e një nëpunësi për mbrojtjen e të dhënave personale, i cili do të sigurojë mbikëqyrjen e respektimit të legjislacionit në fuqi dhe përputhshmërinë e proceseve përpunuese me kërkesat ligjore.

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.

Nga kontrolli i ushtruar rezultoi se Kontrolluesi nuk i ka përmbushur këto detyrime. Në përfundim të hetimit administrativ, referuar provave dhe konstatimeve në vend si më sipër, grupi i inspektimit ka hartuar procesverbalin përkatës, një kopje e të cilit i është vendosur në dispozicion Kontrolluesit nëpërmjet rrugës postare.

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, gjatë seancës dëgjimore, të zhvilluar më datë 22.05.2026, shprehu bashkëpunimin dhe angazhimin e tij për të rikuperuar shkeljet e konstatuara nga grupi i hetimit dhe për të arritur përputhshmërinë me Ligjin.

Gjithashtu, nga ana e Kontrolluesit, protokolluar me tonën nr. 1024/6 prot., datë 20.05.2026, Kontrolluesi ka paraqitur pretendimet si vijon:

- Lidhur me pikën 2 të Procesverbalit, Kontrolluesi pretendon se: “Politikat e Privatësisë” së shoqërisë publikuar në faqen zyrtare nuk janë një model standard, pasi në vlerësim të Kontrolluesit, kjo rubrikë përmban element të personalizuar për veprimtarinë e shoqërisë në sektorin e ndërtimit dhe shitjes së apartamenteve, jo një model i përgjithshëm. “Politikat e Privatësisë” identifikojnë emrat dhe lokacionet e ofruesve/përpunuesve, përshkruhen kanalet konkrete të komunikimit me subjektet e të dhënave, formulari i kontaktit në faqen e internetit, fushatat reklamuese në Facebook dhe Instagram, sistemi CRM (Zoho). Politikat citojnë 11 nene specifike të ligjit 124/2024, specifikojnë bazat ligjore të diferencuara sipas kanalit dhe qëllimit të përpunimit, specifikojnë afatet konkrete të ruajtjes, të diferencuara sipas qëllimit. Këta element tregojnë se Politika e shoqërisë është dokument i përshtatur specifikisht për veprimtarinë e saj në sektorin e ndërtimit, e dallueshme nga modelet standarde që zakonisht përmbajnë fraza të përgjithshme. Sa i përket mungesës së kontaktit të nëpunësit të mbrojtjes së të dhënave personale në Politikën e Privatësisë, shoqëria sqaron se në shkurt 2026 dhe në datën e inspektimit 24.04.2026, DPO nuk ishte caktuar ende formalisht. Kjo mungesë u korrigjua menjëherë me caktimin e znj. Alketa Vushaj si DPO me vendimin e datës 28 prill 2026, si dhe politika e privatësisë është përditësuar me kontaktin zyrtar të DPO-së.

Zyra e Komisionerit vlerëson se ky pretendim nuk qëndron. Këto elemente, edhe pse tregojnë një përshtatje të pjesshme të dokumentit me aktivitetin e Kontrolluesit, nuk janë të mjaftueshme për të përmbushur kërkesat ligjore të transparencës dhe informimit të subjekteve të të dhënave personale, sipas nenit 13 të Ligjit. Në kuptim të këtij neni, Kontrolluesi ka detyrimin të sigurojë informacion të plotë, të qartë dhe të kuptueshëm për subjektet e të dhënave, duke përfshirë në mënyrë të detyrueshme qëllimin dhe bazën ligjore të përpunimit, identitetin dhe kontaktet e Kontrolluesit dhe përpunuesve, të dhënat e kontaktit të Nëpunësit për Mbrojtjen e të Dhënave (DPO), afatet e ruajtjes së të dhënave, masat e sigurisë të zbatuara, si dhe të drejtat që gëzojnë subjektet e të dhënave, përfshirë të drejtën e aksesit, korrigjimit, fshirjes dhe kufizimit të përpunimit.

Gjithashtu, pavarësisht përmbajtjes së deklaruar nga Kontrolluesi, informacioni i dhënë nuk paraqitet në mënyrë të plotë dhe të qartë për të gjitha kategoritë e subjekteve të të dhënave, duke mos garantuar nivelin e kërkuar të transparencës. Në veçanti, mungon një paraqitje e plotë dhe e kuptueshme e të drejtave të subjekteve të të dhënave, si dhe informacioni i detyrueshëm mbi kontaktin e DPO-së në momentin e mbledhjes dhe përpunimit të të dhënave.

Lidhur me mungesën e kontaktit të Nëpunësit për Mbrojtjen e të Dhënave Personale (DPO), argumenti i Kontrolluesit se ky funksion është caktuar më pas,

me vendim të datës 28 prill 2026, nuk e eliminon shkeljen e konstatuar. Detyrimi për caktimin dhe publikimin e kontaktit të DPO-së duhet të jetë i përmbushur në momentin e fillimit të përpunimit të të dhënave dhe gjatë gjithë periudhës së ushtrimit të veprimtarisë së përpunimit.

Sa më sipër, Zyra e Komisionerit vlerëson se “Politikat e Privatësisë” të publikuara nga Kontrolluesi, pavarësisht elementeve të personalizuar që përmbajnë, nuk përmbushin kërkesat e nenit 13 të Ligjit dhe nuk garantojnë nivelin e kërkuar ligjor të transparencës ndaj subjekteve të të dhënave personale.

- Lidhur me pikën 3 të Procesverbalit, Kontrolluesi pretendon se sipas vlerësimit të shoqërisë, lidhur me krijimin, zbatimin, mirëmbajtjen dhe përmirësimin në mënyrë të vazhdueshme të një Sistemi të Menaxhimit të të Dhënave Personale (PIMS) sipas Udhëzimit nr. 9/2025, si dhe nuk mban dokumentacion mbi veprimtaritë e përpunimit sipas nenit 27 të Ligjit, ky konstatim mbështetet në një interpretim të zgjeruar të Udhëzimit nr. 9, i cili nuk korrespondon me objektin dhe fushën e zbatimit të vet Udhëzimit. Udhëzimi rregullon procesin e certifikimit vullnetar të kontrolluesve që zgjedhin të certifikohen, jo detyrimet e përgjithshme të të gjithë shoqërive. Shoqëria “Progeen” shpk vlerëson se, nuk mund të trajtohet automatikisht si “subjekt përpunues i madh” vetëm për shkak të numrit të punonjësve, por pranon se, për shkak të përdorimit të sistemit biometrik dhe sistemit CCTV kërkohet një nivel i përforcuar masash teknike dhe organizative. Detyrimi për domain controller të dedikuar, IPS/IDS të avancuar dhe plane BCP/DRP të dokumentuara në standardin ISO/IEC 27001 është kërkesë e niveleve më të larta të menaxhimit të sigurisë, që duhet vlerësuar në raport me natyrën, fushën dhe rrezikun real të veprimtarisë.

Shoqëria zbaton aktualisht masa teknike dhe organizative të arsyeshme dhe proporcionale me rrezikun real të veprimtarisë së saj. Së pari, sistemi biometrik dhe HRBIS, që paraqesin rrezikun më të lartë për shkak të natyrës biometrike të të dhënave, menaxhohen nga përpunuesi i specializuar BIS Business Solutions shpk sipas Marrëveshjes së Përpunimit të nënshkruar më 12.09.2025 dhe Aneksit B të Kontratës së Shërbimeve, ku parashikohen masat e ruajtjes së vazhdueshmërisë (BCP/DR), backup me rotacion, sistem RAID, UPS dhe lidhje fibri të dyfishtë. Së dyti, sistemi CRM (Zoho Corporation) operon në infrastrukturën e tij të certifikuar sipas standardit ISO/IEC 27001 ndërkombëtar, me masa enkriptimi gjatë transmetimit dhe ruajtjes, të garantuara nga ofruesi. Së treti, rrjeti i brendshëm përdor segmentim me VLAN, kontroll aksesit me kredenciale individuale, antivirus dhe host firewall në të gjitha pajisjet, politikë fjalëkalimesh me kërkesa minimale të vendimeve të Komisionerit dhe akses i kufizuar fizik në serverin lokal. Këto masa, të kombinuara me delegimin e sistemeve kritike të përpunuesve të specializuar (BIS, Zoho), realizojnë një nivel sigurie proporcional me rrezikun e veprimtarisë. Shoqëria nuk konteston nevojën

për përmirësim të mëtejshëm të masave teknike dhe organizative dhe ka përgatitur tashmë një Plan Paraprak të Përmirësimit me afat 45 (dyzet e pesë) ditë.

Zyra e Komisionerit vlerëson se këto pretendime nuk qëndrojnë dhe nuk rrëzojnë konstatimet e bëra në procesverbal. *Së pari*, Kontrolluesi pranon se përpunon të dhëna biometrike përmes sistemit të aksesit dhe prezencës, si dhe të dhëna përmes sistemit CCTV. Këto kategori të dhënash konsiderohen me rrezik të lartë për të drejtat dhe liritë e subjekteve të të dhënave dhe kërkojnë jo vetëm masa teknike sigurie, por edhe një sistem të dokumentuar të menaxhimit të rrezikut, procedura të formalizuara dhe evidenca të vazhdueshme të përputhshmërisë ligjore.

*Së dyti*, fakti që disa nga sistemet kritike administrohen nga përpunues të jashtëm si BIS Business Solutions shpk. dhe Zoho Corporation nuk e transferon përgjegjësinë ligjore të Kontrolluesit. Në çdo rast, Kontrolluesi mbetet përgjegjës për të garantuar dhe për të provuar se përpunimi kryhet në përputhje me Ligjin, përfshirë vlerësimin e rrezikut, dokumentimin e masave të marra dhe mbajtjen e regjistrave përkatës të veprimtarive të përpunimit.

*Së treti*, masat e përshkruara nga Kontrolluesi, si përdorimi i VLAN-eve, firewall-eve, antivirusëve, backup-eve dhe kontrollit të aksesit, përbëjnë elemente të rëndësishme të sigurisë teknike, por nuk provojnë ekzistencën e një sistemi të strukturuar dhe të dokumentuar të menaxhimit të mbrojtjes së të dhënave personale, as përmbushjen e plotë të detyrimeve të parashikuara nga legjislacioni në fuqi, përfshirë mbajtjen e regjistrave të përpunimit sipas nenit 27 të Ligjit.

Megjithatë, fakti që Kontrolluesi ka hartuar një plan paraprak për përmirësimin e masave teknike dhe organizative brenda një afati 45 ditor, vlerësohet si një rrethanë lehtësuese dhe pozitive, por nuk ndikon në vlerësimin e gjendjes faktike të konstatuar gjatë inspektimit.

- Lidhur me konstatimin në pikën 6 të Procesverbalit, Kontrolluesi pretendon se Procesverballi konstaton se shoqëria nuk ka emëruar Nëpunësin e Mbrojtjes së të Dhënave Personale (DPO) në kohën e fillimit të hetimit administrativ. Komisioneri pranon shprehimisht në pikën 6 të Procesverbalit Nr. 1024/3 se: “Pas marrjes dijeni për Urdhrin e hetimit administrativ, Kontrolluesi ka emëruar me Vendimin e administratorit, datë 28.04.2026, nëpunësin për mbrojtjen e të dhënave personale.” Shoqëria thekson se caktimi i DPO-së është kryer brenda një afati prej 18 (tetëmbëdhjetë) ditësh nga lëshimi i Urdhrit Nr. 78, datë 10.04.2026, gjë që tregon vullnetin e plotë për përmbushjen e detyrimeve ligjore dhe bashkëpunimin aktiv me Komisionerin.

Zyra e Komisionerit vlerëson se, ky pretendim nuk qëndron. Nga aktet e administruara rezulton se, në datën e fillimit të hetimit administrativ Kontrolluesi nuk kishte emëruar Nëpunësin e Mbrojtjes së të Dhënave Personale (DPO),

ndonëse ushtronte veprimtari përpunimi që kërkonin një emërim të tillë sipas legjislacionit në fuqi. Emërimi i DPO-së me vendim të administratorit më 28.04.2026 është kryer vetëm pasi Kontrolluesi ka marrë dijeni për urdhrin e hetimit administrativ. Ky veprim tregon bashkëpunim dhe gatishmëri për përputhshmëri, por nuk ndryshon faktin se detyrimi ligjor nuk ishte përmbushur në kohën kur duhej të ishte përmbushur. Reagimi brenda një periudhe relativisht të shkurtër dhe emërimi i DPO-së mund të vlerësohen si elemente pozitive në përcaktimin e masave administrative apo të sanksionit, por nuk përbëjnë argument për të kundërshtuar ekzistencën e vetë shkeljes së konstatuar.

Kërkesa ligjore synon që Kontrolluesi të ketë një mekanizëm të brendshëm mbikëqyrjeje dhe këshillimi për mbrojtjen e të dhënave para dhe gjatë zhvillimit të veprimtarive të përpunimit, jo vetëm pas nisjes së një procedure kontrolli nga autoriteti mbikëqyrës. Për rrjedhojë, Zyra e Komisionerit vlerëson se emërimi i DPO-së pas fillimit të hetimit administrativ përbën një masë korrigjuese të ndërmarrë nga Kontrolluesi, por nuk përbën shkak për rrëzimin e konstatimit të procesverbalit lidhur me mosplotësimin në kohë të këtij detyrimi ligjor.

Në përfundim të analizës së rrethanave, fakteve dhe provave si më sipër, në frymën e Ligjit, Komisioneri konkludon se shkeljet e konstatuara gjatë ushtrimit të hetimit administrativ, të tilla si: mos dokumentimi për veprimtaritë përpunuese të Kontrolluesit në funksion të përputhshmërisë me Ligjin, mungesa e masave tekniko-organizative, mos zbatimi i detyrimit për caktimin e nëpunësit për mbrojtjen e të dhënave personale, në kuptim të shkronjës “a”, të pikës 1, të nenit 94 të Ligjit, si dhe shkelja e të drejtave të subjekteve të të dhënave në kuptim të shkronjës “b”, të pikës 2 të nenit 94 të Ligjit, përbëjnë kundërvajtje administrative dhe sanksionohen me gjobë, masa e të cilës llogaritet në bazë të rregullave të normuara në ligj si më poshtë:

*“1. Bazuar edhe në rrethanat e përcaktuara në pikën 2 të nenit 93 të këtij ligji, përbëjnë kundërvajtje administrative dhe dënohen me gjobë deri në 1 000 000 000 (një miliard) lekë, ose në rastin e një shoqërie tregtare deri në 2% të xhiros totale vjetore globale për vitin financiar paraardhës, cilado është më e lartë, shkeljet e detyrimeve:*

*a) të kontrolluesit dhe përpunuesit, sipas neneve 8, pika 6, e 11, të kapitullit III, të pjesës II të këtij ligji, me përjashtim të nenit 22 të këtij ligji;*

*2. Bazuar edhe në rrethanat e përcaktuara në pikën 2 të nenit 93, përbëjnë kundërvajtje administrative dhe dënohen me gjobë deri në 2 000 000 000 (dy miliardë) lekë, ose në rastin e një shoqërie tregtare, deri në 4% të xhiros totale vjetore globale për vitin financiar paraardhës, cilado që është më e lartë, shkeljet e mëposhtme:*

*b) shkeljet e të drejtave të subjekteve të të dhënave sipas neneve 12–20 të këtij ligji;*

Komisioneri vlerëson se, dokumentacioni i paraqitur nga Kontrolluesi nuk përmbush kërkesat e parashikuara nga Ligji dhe nuk mund të konsiderohet si provë e mjaftueshme

për të vërtetuar ekzistencën e masave të nevojshme organizative dhe teknike që Kontrolluesi ka detyrimin të zbatojë, në përputhje me legjislacionin në fuqi. Rrjedhimisht, aktet e referuara nuk prodhojnë efekt juridik në funksion të provueshmërisë së pretendimeve të Kontrolluesit, për qëllime të zbatimit të Ligjit.

Në rrethanat e shqyrtimit të kësaj çështje Komisioneri evidenton shkallën e bashkëpunimit nga ana e Kontrolluesit, si një nga kushtet e përgjithshme për caktimin e masës së sanksionit administrativ. Në këtë drejtim Komisioneri gjithashtu ka marrë në konsideratë xhiron vjetore të deklaruar nga Kontrolluesi sipas të dhënave zyrtare, si dhe rëndësinë e proceseve përpunuese dhe kohëzgjatjen e tyre.

Sa më sipër, mbështetur në dispozitat e Udhëzimit nr. 06, datë 16.07.2025, “*Për miratimin e metodologjisë për përllogaritjen e masës së sanksioneve administrative*”, veçanërisht në pikat 4 dhe 5 të Nënkapitullit 2.1 të Kapitullit 2, si dhe të Kapitullit 4, Komisioneri ka vlerësuar në mënyrë të drejtë dhe transparente masën e sanksionit administrativ ndaj Kontrolluesit, sipas përcaktimeve të neneve 93 dhe 94 të Ligjit, duke u bazuar në kufijtë minimal të përllogaritjes.

Komisioneri vlerësoi faktin se, shkeljet e konstatuara janë serioze në kuptim të Ligjit. Ato lidhen me garantimin e parimeve dhe përpunimin e ligjshëm të të dhënave, si dhe marrjen e masave të përshtatshme tekniko-organizative për sigurinë e të dhënave personale. Gjithashtu, vendimi i Komisionerit bazohet në mënyrën e reagimit të Kontrolluesit për korrigjimin e shkeljeve të konstatuara dhe zbutjen e efekteve të mundshme negative të tyre.

### **PËR KËTO ARSYE:**

Në zbatim të neneve 13, 27, 28, 33, 34, 81-84, pikës 1 të nenit 87, nenit 93, shkronjës “a” të pikës 1 dhe shkronjës “b” të pikës 2 të nenit 94, si dhe nenit 95 të Ligjit nr.124/2024 “*Për mbrojtjen e të dhënave personale*”, ligjit nr. 49/2012 “*Për gjykatat administrative dhe gjykimin e mosmarrëveshjeve administrative*”, i ndryshuar, si dhe ligjit nr. 10279, datë 20.05.2010 “*Për kundërvajtjet administrative*”, Komisioneri,

### **V E N D O S I:**

1. Dënimin e Kontrolluesit, Shoqëria “*Progeen*” shpk, me gjobë në masën **3,000,000** (tre milion) Lekë, për shkelje të nenit 13 të Ligjit;
2. Dënimin e Kontrolluesit, Shoqëria “*Progeen*” shpk, me gjobë në masën **18,000,000** (tetëmbëdhjetë milion) Lekë, për shkelje të neneve 27, 28 dhe 33 të Ligjit;
3. Kontrolluesi, Shoqëria “*Progeen*” shpk, urdhërohet të marrë masa për përditësimin e rubrikës “*Politikat e Privatësisë*” në faqen zyrtare të internetit, në lidhje me informimin e subjekteve të të dhënave, sipas parashikimeve të nenit 13 të Ligjit;

4. Kontrolluesi, Shoqëria “Progeen” shpk, në zbatim të neneve 27 dhe 28 të Ligjit, urdhërohet 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;
5. Kontrolluesi Shoqëria “Progeen” shpk, pas caktimit të nëpunësit për mbrojtjen e të dhënave personale sipas nenit 33, urdhërohet të marrë masa lidhur me trajnimin e punonjësve që kanë akses dhe përpunojnë të dhëna personale, sipas parashikimeve të nenit 34 të Ligjit;
6. Në zbatim të nenit 84 të Ligjit, Kontrolluesi, Shoqëria “Progeen” shpk, duhet të përmbushë detyrimet si më sipër, brenda afateve si vijon:
  - (i) brenda 15 (pesëmbëdhjetë) ditëve, detyrimin e përcaktuar në pikën 3 të dispozitivit të këtij vendimi;
  - (ii) brenda 30 (tridhjetë) ditëve, detyrimin e përcaktuar në pikën 4 të dispozitivit të këtij vendimi;
  - (iii) brenda 45 (dyzet e pesë) ditëve, detyrimet e përcaktuar në pikën 5 të dispozitivit të këtij vendimi.

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

7. Kontrolluesi, Shoqëria “Progeen” shpk, urdhërohet të njoftojë Komisionerin për masat e marra brenda 60 (gjashtëdhjetë) ditëve, duke filluar ky afat nga data e marrjes dijeni të këtij vendimi;
8. Vendimi për gjobë përbën “titull ekzekutiv” dhe zbatohet nga kundërvajtësi (Kontrolluesi), brenda 10 (dhjetë) ditëve nga data e njoftimit. Për ekzekutimin e gjobës ngarkohet shërbimi përbarimor gjyqësor;
9. Kundër këtij Vendimi mund të bëhet ankim në Gjykatën Administrative të Shkallës së Parë Tiranë, brenda 45 (dyzetë e pesë) ditëve nga data e njoftimit.

Ky Vendim u shpall sot, më datë 12.06.2026.

**KOMISIONERI**

**Besnik Dervishi**