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. 1027/6 prot. Tiranë, më 04.06.2026

REKOMANDIM

Nr. 30, datë 04.06.2026

PËR KONTROLLUESIN SHOQËRIA "KLENSI" 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, si dhe provave të administruara në përfundim të hetimit administrativ në ngarkim të Kontrolluesit Shoqëria "*Klensi*" shpk (në vijim, "*Kontrolluesi*"),

KONSTATOHET SE:

Në zbatim të Urdhrit nr. 81, datë 10.4.2026 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 K81513045H me objekt aktiviteti: "*Aktivitet në fushën e ndërtimit. Punime karpentieri. Import-Eksport, tregtim me shumicë e pakicë të mallrave, prodhimeve në fushën e ndërtimit*, etj."

"Klensi" 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. Rezulton se, Kontrolluesi nuk ka hartuar dhe publikuar "*Politikat e Privatësisë*" në faqen zyrtare të internetit www.klensishpk.com. Megjithatë, pas njoftimit për ushtrimin e hetimit administrativ, Kontrolluesi ka publikuar Politikat e Privatësisë, të cilat janë modele standarde (template) të politikave të privatësisë.

   Konstatohet se, Kontrolluesi nuk informon në gjuhën shqipe, 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 mbi privatësinë ose publikimi i saj në mënyrë jo të qartë dhe të plotë kufizon informacionin e nevojshëm ndaj subjekteve mbi qëllimin dhe mënyrën e përpunimit të të dhënave personale.

   Gjithashtu, publikimi i rubrikës "*Politikat e Privatësisë*" në mënyrë të kuptueshme dhe të aksesueshme për subjektet e të dhënave është thelbësor për ushtrimin efektiv të të drejtave të tyre. 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. Nga shqyrtimi i dokumentacionit të vendosur në dispozicion, rezulton se, Kontrolluesi disponon rregullore "*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*". Megjithatë, nga shqyrtimi i përmbajtjes së saj, si dhe nga analizimi në tërësi i provave të mbledhura gjatë hetimit administrativ, si procesverbalet e asgjësimit të mbajtura nga Kontrolluesi, rezulton se, rregullorja i referohet modelit tip të Zyrës së Komisionerit, si dhe nuk është e përditësuar në përputhje me legjislacionin e ri për mbrojtjen e të dhënave personale.

   Kontrolluesi nuk ka parashikuar rregulla specifike mbi kategoritë e të dhënave personale që përpunon, mënyrën e përpunimit, si mënyra e mbledhjes, regjistrimit,

ruajtjes dhe asgjësimit të tyre, sigurinë e të dhënave personale, aksesin në të dhënat personale, afatet e mbajtjes së të dhënave, etj., sipas parashikimeve të nenit 27 dhe 28 të Ligjit, me qëllim garantimin e përpunimit të ligjshëm dhe sigurisë së të dhënave, në përputhje me proceset përpunuese që kryen.

Zyra e Komisionerit vlerëson se, përshtatja dhe plotësimi i aktit të brendshëm/ rregullores "*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*", me të gjithë elementët ligjorë të përcaktuar në pikën 1 të nenit 27 të Ligjit, konsiderohet një detyrim shumë i rëndësishëm, në zbatim të nenit 27 dhe 28 të Ligjit, për të mundësuar shmangien e pasojave të rënda që mund të vijnë për subjektet e të dhënave.

Gjithashtu, në rregullore duhet të përcaktohen në mënyrë të detajuar rregulla dhe procedura organizative për të gjitha aspektet e përpunimit të të dhënave, duke përfshirë, mënyrën e përpunimit, masat e sigurisë fizike, teknike dhe administrative, ruajtjen dhe konfidencialitetin e të dhënave, aksesin, si dhe afatet e ruajtjes së të dhënave.

4. 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 qëndrueshmërinë 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, datë 05.08.2013 të Komisionerit "*Për përcaktimin e rregullave të hollësishme për sigurimin e të dhënave personale*" (në vijim, "*Vendimi nr. 6*").

   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, konstatohet 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.

   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[1] 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 zbatim të nenit 37 të Ligjit, 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, në zbatimin e Udhëzimit 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.

5. Nga verifikimi on-site i infrastrukturës së teknologjisë së informacionit, si dhe nga shqyrtimi i procedurave rregulluese të Kontrolluesit, 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;
   - Kontrolluesi 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;
   - Kontrolluesi nuk ka të specifikuar/dokumentuar kohën maksimale në të cilën shërbimet dhe sistemet nuk mund të jenë funksionale, si dhe nuk janë planifikuar masa që në rast dështimi të një/disa pajisjeve të mos ndikohet në funksionimin e sistemeve dhe shërbimeve të ofruara;

[1] *Pika 3 e nenit 22, pika 3 e nenit 28;*

- Kontrolluesi 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 të Komisionerit.

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 përcaktuara në nenin 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, Kontrolluesi ka caktuar personin e kontaktit nëpërmjet formularit të njoftimit referuar parashikimeve të ligjit të vjetër për mbrojtjen e të dhënave personale[2]. Megjithatë, Kontrolluesi nuk ka përmbushur detyrimin për informim, detyrim që buronte nga ligji i vjetër, si dhe aktualisht nga neni 34 i Ligjit, i cili normon se kontrolluesi publikon të dhënat e kontaktit të nëpunësit të mbrojtjes së të dhënave, me qëllim që subjektet e të dhënave të mund ta kontaktojnë për çështje që lidhen me proceset përpunuese, si dhe *ia njofton ato Komisionerit*.

   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 efektiv të 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 21.05.2026, të organizuar nga Zyra e Komisionerit, gjatë të 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 e datës 21.05.2026, protokolluar pranë Zyrës së Komisionerit me nr. 1027/5 prot., datë 21.05.2026, është përcjellë

[2] *Ligji nr. 9887/2008, shfuqizuar me hyrjen në fuqi të Ligjit nr. 124/2024, "Për mbrojtjen e të dhënave personale".*

dokumentacioni lidhur me masat e marra, në funksion të përputhshmërisë me legjislacionin për mbrojtjen e të dhënave personale, i cili përfshin aktet e mëposhtme:

- Dokumente bazë dhe dokumente orientuese të SMSI, si Dokumenti bazë i Sistemit të Menaxhimit të Sigurisë së Informacionit, Manuali i Sistemit të Menaxhimit të Sigurisë së Informacionit, Deklarata e Zbatueshmërisë – ISO/IEC 27001 Statement of Applicability, etj;
- Kodet dhe planet kryesore, si Kodi i Sjelljes, Kodi i Etikës së Biznesit, Plani i Evakuimit në Rast Emergjence (EEP), Plani i Vazhdimësisë së Biznesit (BCP);
- Politika të SMSI dhe politika mbështetëse si Politika e Sistemit të Menaxhimit të Sigurisë së Informacionit (SMSI/ISMS), Politika e Sigurisë së Informacionit, Politika për përdorimin e internetit, e-mailit dhe kompjuterëve, Politika e Fjalëkalimeve, Politika e Antivirusit dhe Antispamit, etj;
- Procedura të SMSI, duke përfshirë Procedurën e Dokumentacionit të Sistemit të Menaxhimit, Procedurën e Rekrutimit, Procedurën e Menaxhimit të Riskut, Procedurën e Menaxhimit të Incidenteve, Rolet dhe përgjegjësitë në SMSI, Menaxhimi i aksesit në Safety Box, Menaxhimi i Ndryshimeve në Rrjetin IT, Procedurë për auditimin e brendshëm të SMSI, etj;
- Raporte dhe regjistrime operative si Raporti i Auditit të Brendshëm, Raporti ditor i Kontrolleve Fizike, Raporti i Sistemeve, etj;
- Formularë dhe evidenca mbështetëse si Formular përshkrimi pune, Marrëveshja e Konfidencialitetit, Regjistri/evidenca e trajnimeve, Formular Hyrje-Dalje, Formular i Njohjes, etj.

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 13, 27, 28, 34, 81, 82, 83 dhe 84 të Ligjit, Komisioneri,

REKOMANDON:

1. Kontrolluesi, Shoqëria "*Klensi*" shpk, të ketë në vëmendje përditësimin e rubrikës "*Politikat e Privatësisë*", në faqen zyrtare www.klensishpk.com, me qëllim informimin e plotë të subjekteve të të dhënave, sipas parashikimeve të nenit 13 të Ligjit;

2. Kontrolluesi, Shoqëria "*Klensi*" shpk, në zbatim të nenit 27 dhe 28 të Ligjit, të ketë në vëmendje përditësimin e rregullores "*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 për çdo proces përpunimi, mënyrat e përpunimit të të dhënave, të drejtat e subjekteve të të dhënave, përcaktimin e niveleve të aksesit, afatet e ruajtjes së të dhënave, etj.;

3. Kontrolluesi, Shoqëria "*Klensi*" shpk, të marrë masa lidhur me trajnimin e punonjësve që kanë akses dhe përpunojnë të dhëna personale, sipas parashikimeve të nenit 34 të Ligjit;

4. 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 dhe 2 më sipër;
   (ii) brenda 45 (dyzet e pesë) ditëve, detyrimin e përcaktuar në pikën 3 më sipër.

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

5. Kontrolluesi, të njoftojë Komisionerin për masat e marra brenda 60 (gjashtëdhjetë) ditëve;

6. 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 mos zbatimit 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 04.06.2026.

KOMISIONERI

Besnik Dervishi