



**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. 548/6 prot.

Tiranë, më 17.04.2026

**REKOMANDIM**

**Nr. 23, datë 17.04.2026**

**PËR KONTROLLUESIN “KONTAKT” 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”), si dhe provave të administruara në ngarkim të Kontrolluesit “Kontakt” shpk (në vijim, “Kontrolluesi”),

**KONSTATOHET SE:**

Në zbatim të Urdhrit nr. 42, datë 19.02.2026 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 NIPT J92108006V me objekt aktiviteti: “Në fushën e ndërtimit, punime, projekte, prodhim materiale ndërtimi, mbikëqyrje, kolaudim, ndërtime civile etj.”

“Kontakt” shpk është një kompani e specializuar në ofrimin e shërbimeve të ndërtimit, projektimit, mbikëqyrje, kolaudim, ndërtime civile etj. 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 kryen procedurat e rekrutimit për pozicionet vakante të punës, nëpërmjet aplikimit në website zyrtar të kompanisë [www.kontakt.al](http://www.kontakt.al) në rubrikën “Kërko punë”. Publikimet e pozicioneve të punës bëhen në web nga Departamenti i Burimeve Njerëzore. Pas klikimit në këtë rubrikë shfaqet një faqe ku janë të listuara të gjithë pozicionet vakante. Në krahë të djathtë të secilit prej pozicioneve të shpallura është ikona “Apliko”. Me klikimin në këtë ikonë, automatikisht shfaqen dritaret që duhet të plotësojë aplikanti me kategoritë e të dhënave “emër”; “mbiemër”; “e-mail”; “Tel”; “CV”. Pas plotësimit me të dhënat përkatëse, me klikimin e ikonës “Dërgo”, aplikimi dërgohet automatikisht në emailin e Burimeve Njerëzore.

Konstatohet se, Kontrolluesi ruan në adresat elektronike të administruara nga punonjësi i Burimeve Njerëzore, dokumentacion që përmban të dhëna personale të aplikantëve për punë, si jetëshkrim (CV) të dorëzuara në kuadër të procedurës së rekrutimit, edhe në rastet kur pozicioni i punës është plotësuar dhe procedura përkatëse ka përfunduar.

Gjithashtu, nga verifikimi i dokumentit “Procedurë Rekrutimi” të vendosur në dispozicion të grupit të hetimit administrativ, rezulton se, Kontrolluesi, nuk ka parashikuar afate konkrete lidhur me kohën e ruajtjes së të dhënave personale, për dokumentacionin e dorëzuar nga aplikantët, pas përfundimit të procedurës së rekrutimit dhe plotësimit të pozicionit të punës.

Rezulton se, të dhënat e mbledhura nga Kontrolluesi ruhen pa përcaktuar një afat konkret të ruajtjes së tyre, në kundërshtim me pikën 5, të nenit 6 të Ligjit, që nënkupton se të dhënat personale mbahen në një formë që lejon identifikimin e subjekteve të të dhënave për një periudhë jo më të gjatë se sa është e nevojshme për qëllimin për të cilin ato përpunohen, si dhe Udhëzimin nr. 11, datë 08.09.2011 të Komisionerit “Për përpunimin e të dhënave të punonjësve në sektorin privat”, i ndryshuar (në vijim, “Udhëzimi nr. 11”).

Zyra e Komisionerit vlerëson se, 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. Koha e ruajtjes së të dhënave

personale duhet të përcaktohet nga Kontrolluesi, në përputhje me parashikimin e pikës 5, të nenit 6 të Ligjit.

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 kërkimi i vërtetimit të gjendjes gjyqësore është i justifikuar në çdo rast, pasi jo në të gjitha pozicionet e punës një e tillë është e nevojshme dhe proporcionale.

3. Kontrolluesi ka krijuar në platformën “Facebook” dhe “Instagram” profile zyrtare, në të cilën pasqyron veprimtari të ndryshme, duke ilustruar nëpërmjet fotografive dhe videove, të dhënat e subjekteve, punonjës, pjesëmarrës, etj.

Konstatohet se, subjektet e të dhënave nuk informohen mbi qëllimin dhe mënyrën e përpunimit të të dhënave personale, personin që do t’i përpunojë të dhënat, 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 8 dhe 13 të Ligjit.

Zyra e Komisionerit vlerëson se, informimi i subjekteve të të dhënave personale është një nga detyrimet bazë të Kontrolluesit, pasi u jep mundësinë subjekteve të të dhënave personale të njihen me të drejtat që gëzojnë dhe mundësinë e ushtrimit të tyre në praktikë. Mospërbushja e këtij detyrimi nga ana e Kontrolluesit mund të sjellë pasoja sa i përket privatësisë dhe përpunimit të të dhënave personale të subjekteve të të dhënave.

Gjithashtu, Zyra e Komisionerit vlerëson se kur përpunimi kryhet mbi bazën e pëlqimit, Kontrolluesi duhet të jetë në gjendje të provojë që subjekti i të dhënave ka dhënë pëlqimin për përpunimin e të dhënave personale të tij.

“Pëlqim” është çdo element tregues i vullnetit të subjektit të të dhënave, i dhënë lirisht, i informuar dhe i qartë, nëpërmjet të cilit ai, me anë të një deklaratë ose me çdo lloj shfaqjeje tjetër të padyshimtë pohuese të vullnetit, shpreh dakordësinë për përpunimin e të dhënave personale, që lidhen me të për një ose më shumë qëllime specifike.

4. Nga shqyrtimi i dokumentacionit të vendosur në dispozicion, rezulton se, Kontrolluesi nuk disponon rregullorë 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, mënyrën e përpunimit të të dhënave, sigurinë e të dhënave personale, konfidencialitetin, aksesin në të dhënat personale, afatet e mbajtjes së të dhënave, të drejtat e subjekteve të 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.

Referuar nenit 27 të Ligjit, 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 këtë ligj. Në këtë kuadër, mosdisponimi 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, datë 05.08.2013 të Komisionerit “*Për përcaktimin e rregullave të hollësishme për sigurimin e të dhënave personale*”, 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.

Gjithashtu, Zyra e Komisionerit vlerëson se, hartimi dhe zbatimi i rregullores është një detyrim kryesor për Kontrolluesin në përputhje me nenin 27 dhe 28 të Ligjit. Në të, 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.

5. 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 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 zbatim të nenit 37 të Ligjit, Komisioneri ka miratuar Udhëzimin nr. 8 datë 20.11.2025 “Për kriteret shitesë për akreditimin e organizmave certifikues” (në vijim, “Udhëzimi nr. 8”) dhe Udhëzimin nr. 9.

Udhëzimi nr. 9 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. 8 dhe nr. 9.

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. 9.

Bazuar në nenin 28 të Ligjit nenin 13 të Udhëzimit nr. 9, 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. Konstatohet se, Kontrolluesi e ka deleguar shërbimin e mirëmbajtjes së faqes zyrtare [www.kontakt.al](http://www.kontakt.al) tek palë të treta. Megjithatë, Kontrolluesi nuk ka lidhur një marrëveshje në të cilën të specifikohen masat konkrete tekniko-organizative të detyrueshme për t’u zbatuar nga ana e përpunuesit, me qëllim garantimin e sigurisë dhe përpunimit të ligjshëm të të dhënave personale, sipas parashikimeve të nenit 26 të Ligjit dhe Udhëzimit nr. 19, datë 03.08.2012 të Komisionerit “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”, i ndryshuar (në vijim, “Udhëzimi nr. 19”).

Nga analizimi i përmbajtjes së marrëveshjes, rezulton se, nuk janë reflektuar detyrimet dhe përgjegjësitë mes kontrolluesit dhe përpunuesit, sipas parashikimeve të nenit 26 të Ligjit dhe përcaktimeve të Udhëzimit nr. 19, datë 03.08.2012 të Komisionerit “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”, i ndryshuar (në vijim, “Udhëzimi nr. 19”). Zyra e Komisionerit vlerëson se, në rastet e delegimit të përpunimit të të dhënave

---

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

Kontrolluesi duhet të miratojë një akt/kontratë, që palët duhet të përdorin në rast të këtij delegimi, me anë të së cilës të garantojë përcaktimin e rregullave në marrëdhënien e tij me përpunuesin, me qëllim që delegimi i përpunimit të këtyre të dhënave të përpunuesit të jetë në përputhje me nenin 26 të Ligjit dhe me Udhëzimin nr. 19 të Komisionerit. Në rastet e delegimit të përpunimit të të dhënave dhe/ose shërbimit, Kontrolluesi duhet të sigurohet që përpunuesi të garantojë përpunim të ligjshëm dhe të sigurt të të dhënave.

7. 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.

Gjithashtu, pajisja e sigurisë së Kontrolluesit 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 Ligji. 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 Vendimi 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.

8. Nga verifikimi on-site i infrastrukturës së teknologjisë së informacionit, si dhe nga shqyrtimi i procedurave rregulluese që disponon Kontrolluesi, rezulton se:

- Nuk ka plane të dokumentuara për menaxhimin e riskut, teknikat e menaxhimit dhe të performancës;
- 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/disë 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 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 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.

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.

Kontrolluesi nuk ka emëruar një nëpunës të mbrojtjes së të dhënave personale, në kundërshtim me nenin 33 të Ligjit.

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 26.03.2026, 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 me nr. 1943 prot., datë 17.03.2026, protokolluar pranë Zyrës së Komisionerit me nr. 548/5 prot., datë 31.03.2026, është përcjellë dokumentacioni mbi masat e marra në funksion të përmbushjes së detyrimeve ligjore dhe konstatimeve të grupit të kontrollit, si më poshtë:

- Formular për marrjen e pëlqimit për realizimin dhe publikimin e fotografive dhe videove në rrjetet sociale dhe faqet e internetit, duke përcaktuar në këtë akt të dhënat e Kontrolluesit, qëllimin e përpunimit, kategoritë e të dhënave personale që përpunohen, bazën ligjore, afatin, transferimin e të dhënave personale dhe të drejtat e subjektit të të dhënave personale;
- Urdhër i brendshëm “Për caktimin e nëpunësit për mbrojtjen e të dhënave personale”;
- Dokumentacioni mbi sistemin e menaxhimit të sigurisë së informacionit, duke përfshirë: Kodin e sjelljes, Planin e brendshëm dhe planin e evakuimit në rast emergjence (EEP), Kodin e etikës së biznesit, planin e vazhdimësisë së biznesit (BCP), Politikën e sistemit të menaxhimit të sigurisë së informacionit (SMSI/ISMS), Politikën e sigurisë së informacionit, politikën e rekrutimit, politikën e komunikimit të jashtëm, politikën e kontrollit të aksesit, politikën e menaxhimit të incidenteve të sigurisë së informacionit, politikën për përdorimit e internetit, e-mailit dhe kompjuterëve, politikën për pajisjet portative, politikën për skanimin e cenueshmërive, etj.;
- Marrëveshje konfidencialiteti;
- Procedura e dokumentacionit të sistemit të menaxhimit të integruar, Procedura e të drejtave të aksesit, Procedura e menaxhimit të incidenteve, Procedurë për monitorimin e rrjetit, Procedurë për menaxhimin dhe asgjësimin e mediave, etj.;
- Politikën e fjalëkalimeve për llogaritë e përdoruesve, Politikën e menaxhimit të kapaciteteve të sistemeve IT, Politikën e menaxhimit të trajnimeve dhe eventeve;
- Menaxhimi i aksesit në safety box, menaxhimi i ndryshimeve në rrjetin IT, menaxhimi i çelësave të enkriptimit, etj.;
- ISMS rolet dhe përgjegjësitë;

- Procedurë për auditimin e brendshëm të sistemit të menaxhimit të sigurisë së informacionit (SMSI);
- Raporte auditimi, 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 6, 13, 27, 28, 34, 81, 82, 83 dhe 84 të Ligjit, Komisioneri,

### **REKOMANDON:**

1. Kontrolluesi, të ketë në vëmendje përcaktimin e afateve kohore për ruajtjen e të dhënave, për të gjithë 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, të ketë në vëmendje marrjen e “Pëlqimit” të subjekteve të të dhënave në përputhje me parimet dhe kriteret ligjore të sanksionuara në nenet 6 dhe 7 të Ligjit;
3. Kontrolluesi, në zbatim të nenit 27 dhe 28 të Ligjit, të marrë masa për 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 etj.;
4. Kontrolluesi, të marrë masa për të hartuar marrëveshjen me përpunuesin, duke specifikuar detyrimet midis palëve, sipas detyrimeve të parashikuara në nenin 26 të Ligjit dhe Udhëzimin nr. 19;
5. Kontrolluesi, të ketë në vëmendje caktimin e nëpunësit për mbrojtjen e të dhënave personale, sipas parashikimeve të neneve 33 dhe 34 të Ligjit, si dhe të njoftojë Zyrën e Komisionerit për caktimin e tij;
6. Në zbatim të nenit 84 të Ligjit, të përmbushen detyrimet, sipas këtij akti brenda afateve, si vijon:
  - (i) vazhdimisht, detyrimin e përcaktuar në pikat 1, 2 dhe 5 më sipër;
  - (ii) brenda 30 (tridhjetë) ditëve, detyrimet e përcaktuara në pikat 3 dhe 4 më sipër;

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

7. Kontrolluesi të njoftojë Komisionerin për masat e marra brenda 60 (gjashtëdhjetë) ditëve;
8. 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 17.04.2026.

**KOMISIONERI**

**Besnik Dervishi**