



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. 2406/6 prot.

Tiranë, më 03.12.2025

REKOMANDIM

Nr. 55, datë 03.12.2025

PËR KONTROLLUESIN “PRISMA” SH.P.K

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 të Republikës së Shqipërisë” (në vijim, “Kodi i Procedurave Administrative”), si dhe provave të administruara në ngarkim të Kontrolluesit “Prisma” shpk (në vijim, “Kontrolluesi”),

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 188, datë 23.09.2025 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”, me fokus masat teknike-organizative për përpunimin e tyre, veçanërisht sistemet e menaxhimit të sigurisë së informacionit (SMSI)”.*

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 shoqëri tregtare me përgjegjësi të kufizuar, e regjistruar me numër identifikimi M22121029F, në Tiranë, i cili ka si objekt aktiviteti: “Krijimin, zbatimin, integrimin e sistemeve të informacionit dhe programeve kompjuterike në pajisje lokale ose server, etj.”

Kontrolluesi në kuadër të veprimtarisë që ushtron, përpunon të dhëna personale për kategoritë “klientë”, “punëmarrës”, etj. Përpunimi i të dhënave kryhet në mënyrë manuale dhe elektronike.

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

Konstatohet se të dhënat personale të subjekteve janë përpunuar dhe/ose publikuar në rrjetin social “Facebook” dhe “Instagram”, pa marrë paraprakisht pëlqimin e tyre, në kundërshtim me parimet e mbrojtjes së të dhënave personale dhe me kriteret për përpunimin e tyre, të parashikuara në nenet 6 dhe 7 të Ligjit, si dhe në mungesë të pëlqimit të kërkuar sipas nenit 8 të po këtij Ligji.

Zyra e Komisionerit vlerëson se, përpunimi i të dhënave personale të subjekteve të të dhënave, përmes publikimit të fotografive të subjekteve të të dhënave në platforma si “Facebook” dhe “Instagram”, pa marrë paraprakisht “Pëlqimin”, bie në kundërshtim me nenet 6 dhe 7 të Ligjit.

“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.

3. Kontrolluesi disponon një sistem të video-survejjimit (CCTV) për mbikëqyrjen e ambienteve të brendshme dhe të jashtme të ambienteve ku ushtron aktivitetin. Nga verifikimi i kryer në vend konstatohet se, kontrolluesi disponon tabelë informimi për mbikëqyrjen e ambienteve me sistemin CCTV, por nuk është sipas modelit standard të miratuar nga Komisioneri, në kundërshtim me parashikimin e nenit 13 të Ligjit dhe Udhëzimin nr. 3, datë 30.04.2025 të Komisionerit “Mbi përpunimin e të dhënave personale nga sistemet e video-survejjimit” (në vijim, “Udhëzimi nr. 3”).

Zyra e Komisionerit vlerëson se, informimi i subjekteve të të dhënave personale mbi prezencën e sistemit të video survejjimit CCTV 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. Mospërmbyshja e këtij detyrimi nga ana e Kontrolluesit mund të sjellë pasoja të rënda sa i përket privatësisë dhe përpunimit të të dhënave personale të subjekteve të të dhënave.

4. Kontrolluesi ka vendosur në dispozicion të grupit të hetimit Udhëzim “Regjistri i përpunimit të të dhënave personale të kompanisë”, por nga shqyrtimi i saj, konstatohet se, në të nuk parashikohen rregulla specifike mbi kategoritë e të dhënave personale, mënyrën e përpunimit të të dhënave, sigurinë e të dhënave, konfidencialitetin, të drejtat e subjekteve, etj., sipas parashikimeve të nenit 28 të Ligjit, me qëllim garantimin e përpunimit të ligjshëm dhe sigurisë së të dhënave, në përputhje me proceset përpunuese të tij.

Zyra e Komisionerit vlerëson se është i nevojshëm rishikimi i aktit “Regjistri i përpunimit të të dhënave personale të kompanisë” dhe përshtatja e dispozitave të tij, në mënyrë të tillë që, të parashikohen në mënyrë të detajuar rregulla dhe procedura mbi kategoritë e të dhënave personale që përpunohen, mënyrën e përpunimit, masat e sigurisë dhe konfidencialitetit, afatet e ruajtjes, të drejtat e subjekteve të të dhënave, si dhe përcaktimin e niveleve të aksesit, me qëllim garantimin e përpunimit të ligjshëm dhe sigurisë së të dhënave, në përputhje me proceset përpunuese të Kontrolluesit dhe në zbatim të nenit 28 të Ligjit.

5. Kontrolluesi disponon politika lidhur me sigurinë e informacionit, konkretisht:

- Politikat e privatësisë;
- Politikat e sigurisë së informacionit;
- Politika e brendshme për menaxhimin e incidenteve të sigurisë së të dhënave;
- Politikat e sigurisë për sistemin e kamerave.

Konstatohet se, mungojnë elementë të tjerë të sigurisë së të dhënave si: “Analiza e sigurisë së sistemit të arkivimit” për të gjitha llojet e proceseve përpunuese gjatë ushtrimit të aktivitetit, “Raport vlerësimi mbi sigurinë në sistemin e arkivimit elektronik dhe fizik”, “Kontrolli i sigurisë së sistemit të përpunimit të të dhënave”, etj., në kundërshtim me parashikimet e nenit 28 të Ligjit, 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”) dhe Udhëzimit nr. 47, datë 14.09.2018 të Komisionerit “Për përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga subjektet përpunuese të mëdha” (në vijim, “Udhëzimi nr. 47”).

Kontrolluesi gjatë hetimit administrativ, ka vendosur në dispozicion të grupit të kontrollit, kopje të Certifikatës së Konformitetit “Për sistemin e menaxhimit të sigurisë së informacionit” ISO 27001:2013. Megjithatë, konstatohet se, Kontrolluesi nuk dokumenton masat organizative dhe teknike të ndërmarra në kuadër të sigurisë së informacionit, gjatë ushtrimit të aktivitetit, veçanërisht nëpërmjet sistemeve elektronike sipas këtij standardi.

Gjithashtu, Kontrolluesi nuk ka ndërmarrë masa konkrete në kuadër të trajnimit të punonjësve që kanë akses dhe përpunojnë të dhëna personale, lidhur me legjislacionin në fuqi për mbrojtjen e të dhënave personale, në kundërshtim me nenin 34 të Ligjit dhe Udhëzimin nr. 47 të Komisionerit.

Për sa më sipër, grupi i kontrollit konstaton mosplotësim të detyrimeve në lidhje me ngritjen, administrimin dhe mirëmbajtjen e Sistemit të Menaxhimit të Sigurisë së Informacionit (SMSI), për sa i takon mbrojtjes së të dhënave personale, të parashikuar në Udhëzimin nr. 47, si dhe në zbatim të nenit 28 të Ligjit, për shkak të cilësisë si subjekt përpunues i madh, si dhe për shkak të natyrës së veçantë të veprimtarisë që Kontrolluesi ushtron.

Zyra e Komisionerit vlerëson se, për shkak të cilësisë si subjekt përpunues i madh, si dhe 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, është i detyruar të krijojë, mirëmbajë dhe administrojë SMSI në përputhje me parashikimet e Udhëzimit nr. 47.

SMSI për mbrojtjen e të dhënave personale duhet të bazohet në standardin ISO 27001:2022, siç parashikohet në nenin 5 të Udhëzimit nr. 48, datë 14.09.2018, të Komisionerit “*Për certifikimin e sistemeve të sigurisë së informacionit, të dhënave personale dhe mbrojtjes së tyre*” (në vijim, “*Udhëzimit nr. 48*”) i cili është një sistem i certifikueshëm, për qëllime përputhshmërie me standardin e sipërpërmendur, vetëm me organizma të akredituar dhe autorizuar sipas parashikimeve të Udhëzimit nr. 48.

Zyra e Komisionerit vlerëson se, bazuar në Kreun IV, të Udhëzimit nr. 47 dhe nenin 34 të Ligjit, Kontrolluesi duhet të marrë masa konkrete në kuadër të trajnimit të punonjësve që kanë akses dhe përpunojnë të dhëna personale, bazuar në legjislacionin në fuqi për mbrojtjen e të dhënave personale. Trajnimet në lidhje me mbrojtjen e të dhënave personale, duhet të jenë të vazhdueshme dhe të përshtatura sipas nevojave dhe proceseve të punës së Kontrolluesit dhe legjislacionit në fuqi për mbrojtjen e të dhënave personale, me qëllim ndërgjegjësimin e punonjësve, të cilët për shkak të proceseve të punës, janë të ngarkuar për përpunimin e të dhënave personale.

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.

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 03.10.2025, gjatë të cilës ka deklaruar angazhimin për rikuperimin e shkeljeve të konstatuara gjatë hetimit administrativ. Gjithashtu, përfaqësuesi i Kontrolluesit, para seancës dëgjimore ka depozituar nëpërmjet shkresës administruar me tonën nr. 2406/5 prot., datë 30.10.2025, pretendimet me shkrim lidhur me gjetjet e Procesverbalit të Hetimit Administrativ nr. 2406/2 prot., datë 24.10.2025, konkretisht si më poshtë vijon:

- Lidhur me konstatimin sa i takon tabelës së informimit mbi sistemin e survejimit CCTV, Kontrolluesi ka vendosur gjatë seancës dëgjimore tabelën sipas Udhëzimit nr. 3 të Komisionerit.
- Lidhur me konstatimin për marrjen e pëlqimit të përpunimit të të dhënave personale, Kontrolluesi ka vendosur në dispozicion formularët e dhënies së pëlqimit për punonjës dhe klientë.

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, 8, 13, 28, 34, 81, 82, 83 dhe 84 të Ligjit,

REKOMANDOJ:

1. 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;
2. Kontrolluesi, në zbatim të nenit 28 të Ligjit, të marrë masa për rishikimin e rregullores “*Regjistri i përpunimit të të dhënave personale të kompanisë*”, 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.;
3. Kontrolluesi, të marrë masa 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, sipas parashikimeve të përcaktuara në germet “c” dhe “ç”, të pikës 1 të nenit 34 të Ligjit;
4. Kontrolluesi, me qëllim garantimin e sigurisë së të dhënave personale duhet të zbatojë detyrimet e përcaktuara në Udhëzimin nr. 47, lidhur me trajnimin e punonjësve që kanë akses dhe përpunojnë të dhëna personale si dhe për krijimin, mirëmbajtjen dhe administrimin e Sistemit të Menaxhimit të Sigurisë së Informacionit (SMSI) për mbrojtjen e të dhënave personale;¹
5. Kontrolluesi, për shkak të natyrës së veçantë të aktivitetit që ushtron, duhet të marrë masat e nevojshme për të vlerësuar mbi certifikimin e sistemeve të menaxhimit të sigurisë së informacionit, të të dhënave personale dhe mbrojtjes së tyre, sipas parashikimeve të Udhëzimit nr. 48;²
6. Në zbatim të nenit 84 të Ligjit, të përmbushen detyrimet, sipas këtij akti brenda afateve, si vijon:
 - (i) vazhdimisht, detyrimin e përcaktuar në pikën 1 më sipër;
 - (ii) brenda 30 (tridhjetë) ditëve, detyrimet e përcaktuara në pikat 2 dhe 3 më sipër;
 - (iii) brenda 45 (dyzet e pesë) ditëve, detyrimin e përcaktuar në pikën 4 më sipër.

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

7. Kontrolluesi të njoftojë Komisionerin për masat e marra;
8. Komisioneri, bazuar në germën “a”, pika 2, e 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 03.12.2025.

KOMISIONERI

Besnik Dervishi

1. Udhëzimi nr. 47 dhe Udhëzimi nr. 48 janë shfuqizuar me Udhëzimin nr. 08, datë 20.11.2025 “Për kriteret shitesë për akreditimin e organizmave certifikues”.

2. Detyrimet e parashikuara në Udhëzimin nr. 47 dhe nenin 5 të udhëzimit nr. 48, vijojnë sipas përcaktimeve të Udhëzimit nr. 9, datë 20.11.2025 “Për kriteret e përgjithshme për certifikimin dhe për dhënien e vulave dhe të shenjave të mbrojtjes së të dhënave personale”.