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. 822/6 prot. Tiranë, më 05.08.2026

REKOMANDIM

Nr. 51, datë 05.08.2026

PËR KONTROLLUESIN, SHOQËRIA "DELTA PHARMA-AL" 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 përfundim të hetimit administrativ në ngarkim të kontrolluesit, shoqëria "DELTA PHARMA-AL" sh.p.k. (në vijim "Kontrolluesi"),

KONSTATOHET SE:

Në zbatim të Urdhrit nr. 59, datë 19.03.2026, 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 grupit të hetimit, procesverbalin e konstatimit 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 K62202046U, me objekt aktiviteti "*Distributor dhe shpërndarës i barnave dhe medikamenteve mjekësore. Import, eksport, tregti me shumicë dhe pakicë të barnave dhe medikamenteve mjekësore, barnave popullore, pajisjeve dhe aparaturave mjekësore etj.*".

Kontrolluesi mbledh dhe përpunon të dhëna personale për kategoritë e të dhënave "punonjës", "klientë", "vizitorë" etj. Përpunimi i të dhënave personale kryhet në mënyrë manuale dhe elektronike.

2. Kontrolluesi, ndër të tjera, përpunon të dhëna personale të subjekteve të të dhënave punonjës, vizitorë, nëpërmjet dosjeve fizike dhe në mënyrë elektronike (faqe e internetit, sistemi CCTV etj.). Megjithatë, Kontrolluesi nuk ka vendosur në dispozicion dokumentacion provues lidhur me asgjësimin e të dhënave personale të subjekteve të të dhënave, për të cilat ka përfunduar qëllimi i përpunimit të tyre, në kundërshtim me nenin 27 të Ligjit.

   Nga verifikimi i dokumentacionit të vendosur në dispozicion të grupit të hetimit administrativ, rezulton se Kontrolluesi nuk ka hartuar 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.

   Gjithashtu, 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 sesa është e nevojshme për qëllimin për të cilin ato përpunohen, 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 brendshme 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.

   Gjithashtu, 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 dhe mosdokumentimi i procedurave të brendshme rregullatore për asgjësimin e të dhënave personale të subjekteve të të dhënave, për të cilat ka përfunduar qëllimi i përpunimit të tyre, sipas kërkesave të nenit 27 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" (në vijim "Vendimi nr. 6"), demonstron 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.

3. Kontrolluesi ka të instaluar sistemin e video-survejimit (CCTV), përmes të cilit kryen mbikëqyrjen e ambienteve të brendshme dhe të jashtme ku ushtron veprimtarinë e tij. Nga analizimi i planvendosjes së kamerave konstatohet se disa prej tyre janë të instaluara dhe orientuara në mënyrë të tillë që monitorojnë ambientet e jashtme të ndërtesës, duke përfshirë edhe ambiente të tjera, rrugë kalimi me mundësi fokusimi të kalimtarëve, si dhe ambientet e posteve të punës, në kundërshtim me pikat 2 dhe 3 të nenit 6 dhe nenin 7 të Ligjit, Udhëzimin nr. 03, datë 30.04.2025, të Komisionerit "Për përpunimin e të dhënave personale nga sistemet e video-survejimit" (në vijim "Udhëzimi nr. 03") dhe Udhëzimin nr. 11.

   Nga dokumenti "*Rregullore për Mbrojtjen, Përpunimin, Ruajtjen dhe Sigurinë e të Dhënave Personale në Përdorimin e Sistemit të Video-Survejimit (CCTV)*", e vendosur në dispozicion nga Kontrolluesi, në nenin 8, seksioni 8.2, shkronja "c", parashikohet se: "*Të dhënat e mbajtura me anë të sistemit të video-survejimit do të ruhen për një periudhë deri në dy muaj dhe pas kalimit të kësaj periudhe të dhënat do të fshihen*", konstatohet se të dhënat imazhe/video ruhen përtej afatit ligjor, në kundërshtim me parimin e ruajtjes në kohë, sipas pikës 5 të nenit 6 të Ligjit dhe nenit 3, pika 2, shkronja "b", e Udhëzimit nr. 03 të Komisionerit.

   Zyra e Komisionerit vlerëson se një nga mjetet e rëndësishme të përpunimit të të dhënave personale është edhe sistemi i video-survejimit (CCTV). Për këtë arsye, Zyra e Komisionerit ka hartuar një akt nënligjor të posaçëm (Udhëzimi nr. 03, i cituar më sipër) për rregullimin e kësaj veprimtarie përpunuese. Të dhënat e ruajtura në këto sisteme, si "imazhe" e "video", janë të dhëna personale dhe përpunimi i tyre duhet të jetë në përputhje me parashikimet e Ligjit, si dhe aktit nënligjor të miratuar nga Komisioneri në lidhje me mbledhjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale, gjatë kryerjes së aktivitetit nga Kontrolluesi.

   Gjithashtu, vlerësohet se periudha e mbajtjes së të dhënave nuk duhet të kalojë kufirin maksimal të afatit të lejuar, për përmbushjen e qëllimit të video-survejimit. Të dhënat e mbajtura me anë të sistemit të video-survejimit duhet të ruhen për një periudhë jo më të gjatë se 30 ditë (neni 3, pika 2/b e Udhëzimit nr. 03 të Komisionerit) dhe në momentin që qëllimi për të cilin janë mbledhur të dhënat është realizuar dhe ka përfunduar, duhet të vijohet me shkatërrimin e të dhënave imazhe/video, në të kundërt përpunimi i mëtejshëm i të dhënave konsiderohet i paligjshëm, sipas parashikimeve të pikës 5 të nenit 6 të Ligjit dhe Udhëzimit nr. 03 të Komisionerit.

4. Kontrolluesi ka të publikuar në faqen zyrtare https://deltapharma-adria.com/ rubrikën "Politikat e Privatësisë", të cilat janë modele standarde (*template*) të politikave të privatësisë. Konstatohet se Kontrolluesi nuk informon në gjuhën shqipe 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, të drejtën për akses, të

drejtën për fshirje dhe/ose korrigjim të të dhënave, të dhënat e kontaktit të nëpunësit për mbrojtjen e të dhënave 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 rubrikës "Politikat e 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 joligjore ose të njëanshme të Kontrolluesit gjatë përpunimit të të dhënave personale.

5. Rezulton se Kontrolluesi nuk disponon rregullore "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale", ku të parashikohen rregulla specifike mbi kategoritë e të dhënave personale, mënyrën e përpunimit të të dhënave, sigurinë e të dhënave personale dhe sensitive, konfidencialitetin, afatet e mbajtjes së të dhënave, të drejtat e subjekteve, të dhënat e kontaktit të nëpunësit për mbrojtjen e të dhënave personale etj., sipas parashikimeve të neneve 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 neneve 27 dhe 28 të Ligjit, si dhe Vendimit nr. 6, demonstron 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 nenet 27 dhe 28 të Ligjit. Në të duhet të përcaktohen në mënyrë të detajuar rregullat dhe procedurat 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.

6. 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 të Komisionerit.

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 20.12.2025, të Komisionerit "Për kriteret e përgjithshme për certifikimin dhe për dhënien e vulave dhe të shenjave të mbrojtjes së të dhënave personale" (në vijim "Udhëzimi nr. 09").

Kuadri ligjor evropian mbi mbrojtjen e të dhënave personale, të cilin Ligji transpozon dhe praktika më e mirë evropiane, e konsideron certifikimin si një mekanizëm përputhshmërie me Ligjin[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 këtë kuadër, në zbatim të nenit 37 të Ligjit, i cili parashikon dhe rregullon mekanizmin e certifikimit, Komisioneri ka miratuar Udhëzimin nr. 08, datë 20.11.2025 "Për kriteret shtesë për akreditimin e organizmave certifikues" (në vijim "Udhëzimi nr. 08") dhe Udhëzimin nr. 09.

Udhëzimi nr. 09 referon në Sistemet e Menaxhimit të të Dhënave Personale (*Privacy Information Management System "PIMS"*) dhe Komisioneri inkurajon kontrolluesit, të cilët për shkak të natyrës së veprimtarisë së tyre e kanë të nevojshëm ngritjen e një sistemi të tillë me qëllim standardizimin dhe rregullimin e veprimtarisë përpunuese dhe garantimin e sigurisë së përpunimit të të dhënave personale, të zbatojnë Udhëzimet nr. 08 dhe nr. 09.

Në rastin konkret, Zyra e Komisionerit vlerëson se, për shkak të natyrës së veprimtarisë që ushtron, e cila kërkon masa të shtuara teknike dhe organizative për garantimin e sigurisë së të dhënave personale, Kontrolluesi duhet të krijojë, 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.

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

[1] *Pika 3 e nenit 22, pika 3 e nenit 23 dhe pika 3 e nenit 28.*

- 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 përkatëse 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 moshartimin 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 mospërcaktimi 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 të sigurisë së të dhënave 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.

8. 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, si dhe publikimi i vazhdueshëm i imazheve dhe videove në rrjetet sociale, që përfshijnë punonjës, klientë dhe persona të tretë, 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.

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 18.05.2026, të organizuar nga Zyra e Komisionerit, gjatë së cilës ka deklaruar angazhimin për rikuperimin e shkeljeve të konstatuara gjatë hetimit administrativ, si dhe bashkëpunimin me Komisionerin për të siguruar që çdo mangësi të adresohet në përputhje me Ligjin.

Gjithashtu, nga ana e Kontrolluesit, me shkresën nr. 138 prot., datë 15.05.2026, protokolluar me tonën me nr. 822/5 prot., datë 15.05.2026, Kontrolluesi ka paraqitur pretendimet ndaj procesverbalit të hetimit administrativ, si vijon:

- Lidhur me pikën 2 të procesverbalit, Kontrolluesi pretendon se: *"Shoqëria ka hartuar dhe ka në fuqi Rregulloren dhe dokumentet e evidentuara në pikat 1-4, ku janë parashikuar masat e marra në zbatim të ligjit nr. 124/2024 "Për mbrojtjen e të dhënave personale", për shkatërrimin e dokumentacionit dhe informacionit personal, në përfundim të afatit ligjor për përpunimin e tyre".*

  Zyra e Komisionerit vlerëson se ky pretendim nuk qëndron. 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.

  Gjithashtu, 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 informacion lidhur me përputhshmërinë me këtë Ligj. Në këtë kuadër, mosdisponimi dhe mosdokumentimi i procedurave të brendshme rregullatore për asgjësimin e të dhënave personale të subjekteve të të dhënave, për të cilat ka përfunduar qëllimi i përpunimit të tyre, sipas kërkesave të nenit 27 të Ligjit, si dhe Vendimit nr. 6, demonstron 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.

- Lidhur me pikën 3 të procesverbalit, Kontrolluesi pretendon se: *"Në përputhje me ligjin nr. 124/2024 "Për mbrojtjen e të dhënave personale", si dhe aktet nënligjore në zbatim të tij, në veçanti Udhëzimin 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 dhe Vendimin "Për përcaktimin e rregullave të hollësishme për sigurimin e të dhënave personale",*

shoqëria ka hartuar dhe ka në fuqi kontratën e shërbimit për përpunimin e të dhënave personale nëpërmjet sistemit CCTV".

Zyra e Komisionerit vlerëson se pretendimi i Kontrolluesit se shërbimi i video-survejimit (CCTV) është deleguar tek një palë e tretë nëpërmjet një kontrate shërbimi, nuk qëndron si shkak për përjashtimin nga përgjegjësitë e parashikuara në Ligj. Delegimi i një procesi përpunues nuk sjell transferimin e përgjegjësisë ligjore të Kontrolluesit sa i takon respektimit të detyrimeve që burojnë nga legjislacioni për mbrojtjen e të dhënave personale.

Në rastin konkret, subjekti mbetet kontrollues i të dhënave personale, pasi është ai që përcakton qëllimet dhe mjetet kryesore të përpunimit të të dhënave nëpërmjet sistemit CCTV. Për rrjedhojë, Kontrolluesi mban përgjegjësinë për të garantuar që sistemi të funksionojë në përputhje me kërkesat e ligjit, përfshirë respektimin e parimit të përpunimit në përputhje me qëllimin, parimit të minimizimit të të dhënave, si dhe parimit të kufizimit të ruajtjes në kohë, sipas parashikimeve të pikave 2, 3 dhe 5 të nenit 6 të Ligjit.

Fakti që administrimi teknik i sistemit kryhet nga një palë e tretë nuk e përjashton Kontrolluesin nga detyrimi për të siguruar që kamerat të jenë të pozicionuara në mënyrë të ligjshme dhe proporcionale me qëllimin e mbikëqyrjes, si dhe që afatet e ruajtjes së pamjeve të jenë në përputhje me kufijtë e përcaktuar nga legjislacioni dhe aktet nënligjore përkatëse.

Për më tepër, neni 26 i Ligjit parashikon se Kontrolluesi duhet të zgjedhë përpunues që ofrojnë garanci të mjaftueshme për zbatimin e masave teknike dhe organizative të përshtatshme dhe të ushtrojë mbikëqyrje efektive mbi veprimtarinë e tyre. Si rrjedhojë, çdo mospërputhje lidhur me orientimin e kamerave apo periudhën e ruajtjes së pamjeve video mbetet në sferën e përgjegjësisë së Kontrolluesit dhe nuk mund të justifikohet vetëm me ekzistencën e një kontrate shërbimi me një palë të tretë.

Në përmbledhje të sa më sipër, delegimi i shërbimit për përpunimin e të dhënave personale nëpërmjet sistemit CCTV përbën vetëm një mënyrë organizimi të veprimtarisë së Kontrolluesit dhe nuk përbën shkak ligjor për shmangien apo transferimin e detyrimeve dhe përgjegjësive të parashikuara në Ligj.

- Lidhur me konstatimin në pikën 4 të procesverbalit, Kontrolluesi pretendon se: *"Shoqëria, për shkak të aktivitetit të shitjeve jashtë vendit, ka ngritur dhe mban faqen web, vetëm në gjuhë të huaj, për prezantimin e aktivitetit për qëllime publiciteti dhe lidhjesh me shoqëri të huaja. Kjo faqe është e orientuar për marrëdhënie kompani me kompani (B2B) dhe jo kompani me privat/klient individ fundor (B2C), në këto kushte kjo faqe nuk është në gjuhën shqipe. Në kushtet e një marrëdhënieje biznes me biznes, ku të dhënat personale nuk përpunohen apo kërkohen për qëllim të aksesit në faqen web, shoqëria nuk i ka vendosur këto detyrime në gjuhën shqipe".*

Zyra e Komisionerit vlerëson se ky pretendim nuk qëndron. 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 dhe jo në gjuhën shqipe kufizon informacionin e nevojshëm të subjekteve mbi qëllimin dhe mënyrën e përpunimit të të dhënave personale.

Në analizë të funksionimit të faqeve të internetit, konstatohet se, edhe në rastet kur ato deklarohen si platforma B2B, ato përbëjnë një mjet komunikimi publik dhe potencialisht të aksesueshëm nga çdo subjekt i të dhënave, përfshirë persona fizikë. Për më tepër, funksionimi i zakonshëm i faqeve web, përfshirë përdorimin e *cookies*, *log*-eve të serverit, adresave IP dhe elementeve të tjera teknike, sjell në mënyrë të pashmangshme përpunim të të dhënave personale, pavarësisht qëllimit fillestar të deklaruar nga Kontrolluesi.

Në këtë kuadër, Zyra e Komisionerit vlerëson se faqja zyrtare e internetit përbën një pikë të parë dhe të drejtpërdrejtë kontakti ndërmjet Kontrolluesit dhe subjekteve të të dhënave, ndaj Kontrolluesi ka detyrimin të sigurojë transparencë të plotë dhe të aksesueshme mbi përpunimin e të dhënave personale, në përputhje me nenin 13 të Ligjit nr. 124/2024.

Publikimi i rubrikës "Politikat e Privatësisë" të qartë, të plotë dhe lehtësisht të aksesueshme është një detyrim thelbësor ligjor, i cili nuk kushtëzohet nga natyra B2B apo B2C e marrëdhënies, por nga vetë fakti i përpunimit të mundshëm apo potencial i të dhënave personale.

Gjithashtu, Zyra e Komisionerit vlerëson se ofrimi i këtij informacioni vetëm në gjuhë të huaj nuk garanton transparencë efektive për subjektet e të dhënave në territorin e Republikës së Shqipërisë. Në zbatim të parimit të transparencës dhe të drejtës për informim, informacioni mbi përpunimin e të dhënave personale duhet të jetë i qartë, i kuptueshëm dhe i aksesueshëm për subjektet e të dhënave, çka nënkupton domosdoshmërinë e publikimit edhe në gjuhën shqipe.

Mungesa e një politike privatësie në gjuhën shqipe dhe publikimi i saj në mënyrë të paplotë apo jo të aksesueshme cenon drejtpërdrejt të drejtën e informimit të subjekteve të të dhënave dhe bie ndesh me kërkesat e nenit 13 të Ligjit.

Njëkohësisht, informimi i plotë dhe transparent shërben si parakusht për ushtrimin efektiv të të drejtave të subjekteve të të dhënave, si dhe shërben si mekanizëm parandalues ndaj përpunimeve të paligjshme apo joproporcionale nga ana e Kontrolluesit.

- Lidhur me konstatimin në pikën 8 të procesverbalit, Kontrolluesi pretendon se: *"Lidhur me këtë çështje, konfirmojmë se shoqëria jonë përdor sisteme të certifikuara dhe zyrtare. Asnjë nga pajisjet nuk ka ndonjë program/aplikacion apo sistem që nuk është zyrtar, i përditësuar dhe i protokolluar. Arkitektura e infrastrukturës TIK është projektuar sipas parimit të mbrojtjes në thellësi (Layered Defense), me segmentim të*

rrjetit, firewall segmentation dhe monitorim të vazhdueshëm të trafikut. Lidhjet nga jashtë realizohen vetëm përmes VPN me autentifikim të shumëfishtë. Shoqëria përdor një sistem antivirus, anti phishing, kundër ndërhyrjeve të palejuara. Përdoren VLAN-et për izolimin e rrjetit të brendshëm dhe zona DMZ për serverat web që komunikojnë me jashtë. Lidhur me sigurinë e të dhënave, shoqëria përdor SSL/TLS për të dhënat në transit dhe mbrojtja e të dhënave në Data Center me akses të kufizuar. Përditësimet kryhen në mënyrë të rregullt pas skanimeve për dobësi në sistemet IT. Për identifikimin dhe menaxhimin e vulnerabiliteteve kryhen skanime periodike të vulnerabiliteteve dhe aplikohen masa korrigjuese për të adresuar çdo dobësi të identifikuar...".

Zyra e Komisionerit vlerëson se ky pretendim nuk qëndron. Në analizë të dokumentacionit dhe provave të paraqitura, edhe pse Kontrolluesi disponon disa politika/procedura (të cilat nuk plotësojnë elemente formale për t'u administruar), ekzistenca e masave teknike, pavarësisht nivelit të tyre të avancimit, nuk përbën në vetvete provë të përputhshmërisë me legjislacionin në fuqi, në mungesë të një qasjeje të strukturuar dhe të dokumentuar të bazuar në menaxhimin e riskut.

Në këtë kuadër, mungesa e një procesi formal për identifikimin, analizimin dhe vlerësimin e rreziqeve ndaj të dhënave personale, si dhe mungesa e një metodologjie të dokumentuar për trajtimin e këtyre rreziqeve, cenon drejtpërdrejt parimin e llogaridhënies, të parashikuar në nenin 6, si dhe detyrimet për marrjen e masave të përshtatshme teknike dhe organizative, sipas nenit 28 të këtij Ligji.

Për më tepër, konstatohet mungesa e auditimeve të brendshme periodike dhe e mekanizmave të monitorimit të vazhdueshëm të efektivitetit të masave të sigurisë, çka nënkupton se Kontrolluesi nuk është në gjendje të verifikojë në mënyrë të vazhdueshme nëse këto masa janë të mjaftueshme dhe funksionale në praktikë.

Në të njëjtën kohë, mungesa e planeve të formalizuara të vazhdueshmërisë së biznesit (BCP) dhe të rikuperimit nga katastrofat (DRP), si dhe mospërcaktimi i parametrave kritikë të rikuperimit, si RTO dhe RPO, tregojnë një nivel të pamjaftueshëm të organizimit për garantimin e disponueshmërisë, integritetit dhe reziliencës së sistemeve që përpunojnë të dhëna personale.

Këto mangësi krijojnë një rrezik të lartë që, në rast incidentesh të sigurisë apo ndërprerjesh të shërbimit, të dhënat personale të humbasin, të komprometohen ose të mos rikuperohen në kohë të pranueshme, duke cenuar të drejtat dhe liritë e subjekteve të të dhënave.

Gjithashtu, konstatohet mungesa e procedurave të standardizuara për administrimin dhe ruajtjen e *log*-eve, si dhe mungesa e evidencave mbi monitorimin dhe analizimin e tyre. Kjo situatë cenon gjurmueshmërinë e veprimeve mbi të dhënat personale dhe kufizon aftësinë për të identifikuar dhe hetuar incidente të mundshme sigurie. Njëkohësisht, evidentohet se proceset e *backup*-it nuk janë të mbështetura nga procedura të dokumentuara dhe nuk shoqërohen me testime periodike të rikthimit të

të dhënave (*restore testing*), duke krijuar pasiguri mbi efektivitetin real të këtyre masave në rast nevoje.

Sa më sipër, Zyra e Komisionerit vlerëson se masat e ndërmarra nga Kontrolluesi rezultojnë të fragmentuara dhe të padokumentuara në mënyrë të mjaftueshme, duke mos përmbushur kërkesat e nenit 28 të Ligjit dhe të Vendimit nr. 6 të Komisionerit.

Në përfundim, Zyra e Komisionerit vlerëson bashkëpunimin e Kontrolluesit me grupin e kontrollit gjatë ushtrimit të hetimit administrativ, si dhe angazhimin e tij për të rikuperuar shkeljet e konstatuara. Plotësimi i këtyre detyrimeve nga ana e Kontrolluesit është mjaft i rëndësishëm, pasi garanton përpunimin e ligjshëm, sigurinë e të dhënave personale dhe shmang mundësinë e përhapjes së tyre në mënyrë të paligjshme.

PËR KËTO ARSYE:

Në zbatim të neneve 6, 7, 13, 27, 28, 33, 81-84 të Ligjit, Komisioneri,

REKOMANDON:

1. Kontrolluesi, shoqëria "DELTA PHARMA-AL" sh.p.k., të marrë masa për caktimin e afateve kohore për ruajtjen e të dhënave, për të gjitha proceset e përpunimit, në përputhje me pikën 5 të nenit 6 të Ligjit. Në momentin e përfundimit të qëllimit të përpunimit, Kontrolluesi duhet të realizojë shkatërrimin e këtyre të dhënave, pasi përpunimi i mëtejshëm i tyre konsiderohet i paligjshëm; si dhe 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;

2. Kontrolluesi, shoqëria "DELTA PHARMA-AL" sh.p.k., të marrë masa për përcaktimin e planeve të kamerave përmes sistemit të video-survejimit (CCTV), si dhe përcaktimin e afateve kohore për ruajtjen e të dhënave, për të gjitha proceset e përpunimit, në përputhje me pikën 5 të nenit 6 të Ligjit. Në momentin e përfundimit të qëllimit të përpunimit, Kontrolluesi duhet të realizojë shkatërrimin e këtyre të dhënave, pasi përpunimi i mëtejshëm i tyre konsiderohet i paligjshëm;

3. Kontrolluesi, shoqëria "DELTA PHARMA-AL" sh.p.k., të ketë në vëmendje përditësimin e rubrikës "Politikat e Privatësisë", në faqen zyrtare të internetit https://deltapharma-adria.com/, me qëllim informimin e plotë të subjekteve të të dhënave, sipas parashikimeve të nenit 13 të Ligjit;

4. Kontrolluesi, shoqëria "DELTA PHARMA-AL" sh.p.k., në zbatim të neneve 27 dhe 28 të Ligjit, të marrë masa për dokumentimin e proceseve përpunuese, si dhe masa konkrete teknike dhe organizative për mbrojtjen e të dhënave personale, në funksion të aktivitetit të tij, për çdo proces përpunimi;

5. Kontrolluesi, shoqëria “DELTA PHARMA-AL” sh.p.k., në zbatim të neneve 27 dhe 28 të Ligjit, të marrë masa për hartimin 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, të dhënat e kontaktit të nëpunësit për mbrojtjen e të dhënave etj.;

6. Kontrolluesi, shoqëria “DELTA PHARMA-AL” sh.p.k., të marrë masa për caktimin e nëpunësit për mbrojtjen e të dhënave personale, sipas parashikimit të nenit 33 të Ligjit, si dhe të njoftojë Komisionerin për caktimin e tij sipas parashikimit të nenit 34 të Ligjit;

7. Në zbatim të nenit 84 të Ligjit, të përmbushen detyrimet sipas këtij akti, brenda afateve, si vijon:

   i) vazhdimisht, detyrimin e përcaktuar në pikën 3 më sipër;
   ii) brenda 15 (pesëmbëdhjetë) ditëve, detyrimet e përcaktuara në pikat 1 dhe 2 më sipër;
   iii) brenda 30 (tridhjetë) ditëve, detyrimet e përcaktuara në pikat 5 dhe 6 më sipër;
   iv) 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.

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

9. Komisioneri, bazuar në shkronjën “a” të pikës 2 të nenit 83 të Ligjit, paralajmëron kontrolluesit ose përpunuesit se veprimet e përpunimit mund të rezultojnë në mosplotësim të dispozitave ligjore dhe u jep atyre rekomandime lidhur me përputhshmërinë me Ligjin. Në rast të moszbatimit të tyre, Komisioneri vepron sipas neneve 92, 93 dhe 94 të Ligjit, për vendosjen e sanksioneve administrative në përputhje me nenet përkatëse, si dhe në përputhje me legjislacionin në fuqi për kundërvajtjet administrative, në mënyrë të tillë që këto masa të jenë efektive, proporcionale dhe me karakter parandalues.

Ky Rekomandim u shpall sot, më 05.08.2026.

KOMISIONERI

Besnik Dervishi