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. 824/6 prot. Tiranë, më 17.06.2026

REKOMANDIM

Nr. 31, datë 17.06.2026

PËR KONTROLLUESIN SHOQËRIA "ORANGE FARMACI" 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 "*Orange Farmaci*" shpk (në vijim, "*Kontrolluesi*"),

KONSTATOHET SE:

Në zbatim të Urdhrit nr. 61, datë 19.3.2026 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim, "*Komisioneri*"), u krijua grupi i punës, i cili kreu hetimin administrativ pranë Kontrolluesit, me objekt:

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

Komisioneri, pasi shqyrtoi relacionin e hetimit administrativ, 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. Si i tillë ai është i regjistruar në Qendrën Kombëtare të Biznesit me NUIS L82322031K me objekt aktiviteti: "*Import, eksport, tregti me shumicë dhe pakicë i produkteve farmaceutike, barnave për përdorim human dhe veterinar, kozmetike, bimë medicinale, shtesave ushqimore dhe dietike. Ngritje dhe menaxhim i farmacive dhe klinikave private në fushën e mjekësisë etj.*".

Kontrolluesi mbledh dhe përpunon të dhëna personale për kategorinë e të dhënave "*punonjës*", "*pacientë*", "*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, nëpërmjet dosjeve fizike dhe për klientët në mënyrë elektronike nëpërmjet sistemit të regjistrimit të klientit. 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.

   Konstatohet 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, 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 lidhur me kategoritë e të dhënave të grumbulluara, në funksion të ushtrimit të veprimtarisë së tij, Kontrolluesi duhet të parashikojë mbajtjen e të dhënave personale të grumbulluara në atë formë, që lejon identifikimin për një kohë të caktuar, por jo më tepër se sa është e nevojshme për të përmbushur qëllimin për të cilin të dhënat janë grumbulluar. 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, 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.

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*", 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 nuk ka hartuar dhe publikuar "*Politikat e Privatësisë*" në faqen zyrtare të internetit https://orangefarmaci.al/. Subjektet e të dhënave nuk informohen mbi qëllimin dhe mënyrën e përpunimit të të dhënave personale, personin që do t'i përpunojë të dhënat, të dhënat e kontaktit të përfaqësuesit të Kontrolluesit, si dhe 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.

4. Nga verifikimi në vend, rezulton se, Kontrolluesi e ka të organizuar rrjetin e brendshëm të intranetit dhe atë të njësive të shërbimit (si farmacitë) me pajisje kompjuterike, të cilat nuk janë të qendërzuara 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 kërkesat e nenit 27 dhe 28 të Ligjit për garantimin e konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave personale përmes masave të përshtatshme teknike.

Zyra e Komisionerit vlerëson se, në referim të kërkesave të përcaktuara në nenin 28 të Ligjit, Kontrolluesi duhet të zbatojnë masat e duhura teknike dhe organizative për të siguruar një nivel të përshtatshëm ndaj rrezikut. Në vlerësimin e nivelit të përshtatshëm të sigurisë duhet të merren parasysh veçanërisht rreziqet që shkaktohen nga përpunimi, specifikisht, nga shkatërrimi aksidental ose i paligjshëm, humbja, ndryshimi, përhapja e paautorizuar ose aksesi në të dhënat personale të transmetuara, të ruajtura ose të përpunuara në çfarëdolloj mënyre.

Gjithashtu, 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.

5. Konstatohet se, Kontrolluesi nuk disponon një akt/rregullore "*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 dhe sensitive, konfidencialitetin, afatet e mbajtjes së të dhënave, 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 që kryen, sipas parashikimeve të nenit 27 dhe 28 të Ligjit.

   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*", 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 një akti të brendshëm/rregullore 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.

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, 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 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 Udhëzimin nr. 08 dhe nr. 09.

   Në rastin konkret, Zyra e Komisionerit ka vlerësuar 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 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;
   - 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 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 të sigurisë, 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.

8. Në vijim të hetimit, rezultoi se Kontrolluesi nuk aplikon për punëmarrësit, të cilët kanë akses në informacionin e mbajtur nga ana e tij "*Deklaratën e Konfidencialitetit*", në përmbushje të detyrimit ligjor që buron nga neni 30 i Ligjit, si dhe Vendimi nr. 6 i Komisionerit.

   Zyra e Komisionerit vlerëson se, qëllimi i nënshkrimit të "*Deklaratës së Konfidencialitetit*" është që të gjithë punonjësit, të cilët kanë akses për arsye profesionale në procese përpunuese dhe në të dhënat personale, të kuptojnë qartë dhe drejtë, detyrimet dhe përgjegjësitë që ata kanë mbi përpunimin e të dhënave personale dhe ruajtjen e konfidencialitetit.

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, 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. 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.

Bazuar në pikën 2 të nenit 34 të Ligjit, i cili përcakton se nëpunësi caktohet në bazë të aftësive profesionale të certifikuara, Kontrolluesi ka detyrimin që të sigurojë trajnimin e nëpunësit të caktuar nga ana e tij në përputhje me pikën 6 të nenit 34 të Ligjit.

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 18.05.2026, 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. Nga ana e Kontrolluesit, është përcjellë dokumentacioni mbështetës/teknik i Sistemit të Menaxhimit të Sigurisë së Informacionit, lidhur me masat e marra, i cili përfshin aktet e mëposhtme:

- Planin e Evakuimit në Rast Emergjence (EEP), Planin e Vazhdimësisë së Biznesit (BCP), Kodi i Etikës së Biznesit (C-03), Kodin e Sjelljes (C-01);
- Politika e Sistemit të Menaxhimit të Sigurisë së Informacionit (SMSI/ISMS), Politika e Sigurisë së Informacionit (PO-02), Politika e Rekrutimit (PO-03);

- Politika e Komunikimit të Jashtëm (PO-05), Politika e Kontrollit të Aksesit (PO-06), Politika e Menaxhimit të të Incidenteve të Sigurisë së Informacionit (PO-07);
- Politika për përdorimin e internetit, e-mailit dhe kompjuterëve, Politika për Pajisjet Portative, Politika e Skanimin e Cenueshmërive, Politika e Cilësisë, Politika e fjalëkalimeve për llogaritë e përdoruesve dhe shërbimeve, Politika e Menaxhimit të kapaciteteve të sistemeve IT, Politika e Antivirusit dhe Antispamit;
- Politika e Menaxhimit të Trajnimeve dhe Eventeve; Procedura e dokumentacionit të SMSI-së; Procedura e Rekrutimit; Procedura e menaxhimit të riskut;
- Procedura e të drejtave të aksesit të përdoruesve; procedura e menaxhimit të incidenteve të sigurisë së informacionit; Procedura e aksesit në dhomat teknike; Rolet dhe përgjegjësitë në SMSI; Procedura për implementimin e projekteve; Procedura për rishikimin nga menaxhmenti; Procedura për menaxhimin e çelësave të enkriptimit; Procedura për mospërputhjet, veprimet korrigjuese dhe parandaluese;
- Procedura e kërkesave ligjore dhe kontraktuale, Procedura e përgjigjes dhe raportimit të incidenteve të sigurisë së sistemeve të informacionit;
- Procedura e Backup-it dhe restore-it, Raport Auditimi i Brendshëm i SMSI-së, Raport incidenti;
- Marrëveshje konfidenciaiteti, Skema e klasifikimit dhe etiketimit të informacionit;
- Etj.

Gjithashtu, gjatë seancës dëgjimore, përfaqësuesi i Kontrolluesit ka parashtruar verbalisht pretendime lidhur me gjetjet e Procesverbalit të hetimit administrativ, dhe konkretisht:

- Lidhur me pikën 2 të Procesverbalit të hetimit administrativ, Kontrolluesi parashtron se ka qenë bashkëpunues dhe ka vendosur në dispozicion të gjithë dokumentacionin e kërkuar nga grupi i hetimit administrativ. Sa i përket dokumentimit për asgjësimin e të dhënave personale për punonjësit e larguar, Kontrolluesi pretendon se të dhënat personale janë fshirë nga kompjuteri dhe është hequr dosja përkatëse. Për më tepër, ndërmarrja është shumë e re, pasi është bashkim i shumë farmacive dhe mund të rezultojë që të mos ketë punonjës të larguar vitet e fundit.

  Zyra e Komisionerit vlerëson se ky pretendim nuk qëndron. *Së pari*, Kontrolluesi ka qenë bashkëpunues me grupin e hetimit dhe autoritetin mbikëqyrës gjatë gjithë procedurës së hetimit administrativ, pasi siç rezulton edhe nga Procesverbali i hetimit, mungesa e bashkëpunimit nuk është evidentuar si shkelje nga ana e grupit të kontrollit. *Së dyti*, Lidhur me pretendimin e Kontrolluesit se të dhënat e punonjësve të larguar janë asgjësuar, Zyra e Komisionerit vlerëson se pretendimi dhe deklarimi i kontrolluesit nuk përbën në vetvete provë të mjaftueshme për përmbushjen e këtij detyrimi. Kontrolluesi duhet të disponojë dokumentacion mbështetës që demonstron/vërteton pretendimet e tij, si për shembull procesverbal, evidenca, regjistra ose dokumente të tjera që përcaktojnë kohën, mënyrën, personat

përgjegjës, etj., në mënyrë që të garantohet verifikueshmëria e procesit. Sa i përket pretendimit se Kontrolluesi është një shoqëri/ndërmarrje e re, Zyra e Komisionerit vlerëson se ky pretendim nuk qëndron. Dokumentimi i të gjitha proceseve përpunuese , nuk lidhet me kohën e krijimit të shoqërisë/afatin e ushtrimit të veprimtarisë.

Detyrimet që burojnë nga legjislacioni për mbrojtjen e të dhënave personale duhet të zbatohen që në momentin e fillimit të përpunimit të të dhënave personale, pavarësisht kohës së krijimit ose nivelit të zhvillimit të aktivitetit. Edhe në rastet kur Kontrolluesi pretendon se për shkak të kohës së shkurtër të ushtrimit të aktivitetit, nuk ka kryer ende procese asgjësimi, ai duhet të disponojë procedura dhe mekanizma dokumentimi që mundësojnë evidentimin dhe provueshmërinë e këtyre proceseve sapo ato të realizohen.

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, 30, 33, 34, 81- 84 të Ligjit, Komisioneri,

REKOMANDON:

1. Kontrolluesi, Shoqëria "*Orange Farmaci*" shpk, të marrë masa për 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, Shoqëria "*Orange Farmaci*" shpk, të marrë masa për hartimin dhe publikimin e rubrikës "*Politikat e Privatësisë*", në faqen zyrtare www.orangefarmaci.al, me qëllim informimin e plotë të subjekteve të të dhënave, sipas parashikimeve të nenit 13 të Ligjit;

3. Kontrolluesi, Shoqëria "*Orange Farmaci*" shpk, në zbatim të nenit 27 dhe 28 të Ligjit, të marrë masa për hartimin e rregullores "*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*", duke parashikuar në të, masa konkrete teknike dhe organizative për mbrojtjen e të dhënave personale, mënyrat e përpunimit të të dhënave, të drejtat e subjekteve të të dhënave, garantimin e konfidencialitetit etj., në funksion të aktivitetit të tij, për çdo proces përpunimi;

4. Kontrolluesi, Shoqëria "*Orange Farmaci*" shpk, në zbatim të nenit 30 të Ligjit, të marrë masa për aplikimin e "*Deklaratës së Konfidencialitetit*", si dhe të reflektojë në mënyrë të qartë detyrimet dhe përgjegjësitë me punëmarrësit të cilët kanë akses në mbledhjen, përpunimin dhe ruajtjen e të dhënave personale;

5. Kontrolluesi, Shoqëria "*Orange Farmaci*" shpk, të marrë masa për 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) brenda 15 (pesëmbëdhjetë) ditëve, detyrimet e përcaktuara në pikat 1 dhe 2 më sipër;
   (ii) brenda 30 (tridhjetë) ditëve, detyrimet e përcaktuara në pikat 3, 4 dhe 5 më sipër;

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

7. Kontrolluesi, Shoqëria "*Orange Farmaci*" shpk, 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 17.06.2026.

KOMISIONERI

Besnik Dervishi