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. 825/6prot. Tiranë, më 03.06.2026

REKOMANDIM

Nr. 26, datë 03.06.2026

PËR KONTROLLUESIN SHOQËRIA "CFO PHARMA" 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 "*CFO Pharma*" shpk (në vijim, "*Kontrolluesi*"),

KONSTATOHET SE:

Në zbatim të Urdhrit nr. 62, 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 hetimit administrativ dhe provat e administruara gjatë ushtrimit të hetimit pranë Kontrolluesit, vëren se:

1. Kontrolluesi është subjekt i së drejtës tregtare i organizuar në formën e një shoqërie me përgjegjësi të kufizuar, i regjistruar në Qendrën Kombëtare të Biznesit me NUIS K22305002U me objekt aktiviteti: "*Import-eksport, ruajtje, shpërndarje, shitje me shumicë dhe pakicë e artikujve farmaceutik dhe parafarmaceutik, shtesave ushqimore dhe produkteve bimore, produkteve kozmetike, bimë medicinale etj.,"*

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 grumbullon në arkivin fizik dokumentacionin për personelin aktual dhe të larguar. Nga verifikimi i dosjeve të vendosura në dispozicion, konstatohet se, në dosjet e personelit të larguar ruhen, ndër të tjera, kopje të: "*Letërnjoftimit*"; "*Diplomës"; "Certifikata trajnimi"; "Vërtetim aftësie për punë"*; etj.

   Nga verifikimi i dokumentit "*SOP për Politikën e Mbrojtjes së të Dhënave*" 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 që administron në funksion të veprimtarisë që ushtron.

   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, Kontrolluesi duhet të përcaktojë në mënyrë të qartë dhe të dokumentuar afatet e ruajtjes për çdo kategori të dhënash personale, duke marrë në konsideratë, qëllimin e përpunimit, bazën ligjore përkatëse, detyrimet që rrjedhin nga legjislacioni sektorial, si dhe nevojën për ruajtje për qëllime të mbrojtjes së të drejtave ligjore apo për përmbushjen e detyrimeve kontraktore. Afatet duhet të jenë proporcionale dhe të justifikuara, duke shmangur ruajtjen e të dhënave për një kohë të pacaktuar, 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.

3. Kontrolluesi ka krijuar në platformën "*Instagram*" profil zyrtar, në të cilin pasqyron veprimtari të ndryshme, duke ilustruar nëpërmjet fotografive dhe videove, të dhënat e subjekteve, punonjës, pjesëmarrës, etj.

   Konstatohet se, të dhënat e subjekteve të të dhënave përpunohen/publikohen në rrjetin

social "*Instagram*", në kundërshtim me parimet e mbrojtjes së të dhënave personale dhe kriteret për përpunimin e të dhënave, të parashikuara në nenet 6 dhe 7 të Ligjit, si dhe pa marrë pëlqimin e tyre, sipas parashikimit të nenit 8 të Ligjit.

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.

Bazuar në nenin 8 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 deklarate 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 disponon një akt të brendshëm rregullator "*SOP për Politikën e Mbrojtjes së të Dhënave*". Nga shqyrtimi dhe analizimi i përmbajtjes, rezulton se në të mungojnë parashikime mbi mënyrën e përpunimit të të dhënave personale, si mënyra e mbledhjes, regjistrimit, ruajtjes dhe asgjësimit të tyre, afatet konkrete të ruajtjes së të dhënave personale, etj., 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.

   Zyra e Komisionerit vlerëson se, përshtatja dhe plotësimi i dokumentit "*SOP për Politikën e Mbrojtjes së të Dhënave*", me të gjithë elementët ligjorë të përcaktuar në pikën 1 të nenit 27 të Ligjit, konsiderohet një detyrim shumë i rëndësishëm, në zbatim të nenit 27 dhe 28 të Ligjit, për të mundësuar shmangien e pasojave të rënda që mund të vijnë për subjektet e të dhënave.

   Gjithashtu, në aktin e brendshëm 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. Kontrolluesi ka të instaluar sistemin e video-survejimit (CCTV), përmes së 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 dhe qytetarë, si dhe ambientet e posteve të punës në kundërshtim me pikën 2, të nenit 6 dhe nenin 7 të Ligjit, Udhëzimin nr. 03, datë 30.04.2025, "*Për përpunimin e të dhënave personale nga sistemet e video survejimit*" (në vijim, "*Udhëzimi nr. 3*") dhe Udhëzimin nr. 11.

Nga verifikimet e kryera në sistemin e video-survejimit (CCTV), rezulton 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 Udhëzimin nr. 3, 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. 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 aktet e miratuara nga Komisioneri në lidhje me mbledhjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale, gjatë kryerjes së aktivitetit nga Kontrolluesi.

Sa më sipër, Zyra e Komisionerit vlerëson se, mbikëqyrja e ambienteve të jashtme të Kontrolluesit, nëpërmjet sistemit të video/audio survejimit, si dhe e posteve të punës së punonjësve, është në kundërshtim me parashikimet e neneve 6 dhe 7 të Ligjit.

Nga verifikimi në vend i sistemit të video-survejimit (CCTV), si dhe nga shqyrtimi i dokumentacionit të vënë në dispozicion, konstatohet se Kontrolluesi nuk ka miratuar një rregullore të brendshme për administrimin, aksesin, ruajtjen dhe fshirjen e të dhënave imazh/video të përpunuara përmes këtij sistemi, në kundërshtim me nenin 28 të Ligjit.

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, Zyra e Komisionerit vlerëson se, Kontrolluesi është i detyruar të hartojë rregulla/politika të brendshme specifike për mënyrën e përpunimit të të dhënave personale, nivelet e aksesit, afatet e ruajtjes së të dhënave, etj., nëpërmjet sistemit të video survejimit CCTV, në përputhje me parashikimet e nenit 28 të Ligjit.

6. Kontrolluesi nuk ka marrë masa për përmbushjen e detyrimit për informimin e subjekteve të të dhënave personale nëpërmjet publikimit të rubrikës "*Politikat e Privatësisë*" në faqen zyrtare https://www.cfopharma.com.

   Subjektet e të dhënave personale nuk informohen mbi qëllimin dhe mënyrën e përpunimit të të dhënave personale, personin që do t'i përpunojë të dhënat, të drejtat ligjore që gëzojnë, afatin e mbajtjes së të dhënave dhe masat e sigurisë, 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 i 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 jo ligjore ose të njëanshme të Kontrolluesit gjatë përpunimit të të dhënave personale.

7. 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.

   Referuar nenit 27 të Ligjit, Kontrolluesi ka detyrimin të mbajë dokumentacion, në format të shkruar dhe elektronik, për veprimtaritë e tij përpunuese në mënyrë që të jetë në gjendje të japë të dhëna lidhur me përputhshmërinë me këtë ligj. Referuar nenit 27 pika 4 e Ligjit, çmohet se Kontrolluesi nuk përfshihet në rrethin e subjekteve të përjashtuar nga detyrimet e nenit 27 pika 1 dhe 2 e Ligjit pasi, edhe pse ka më pak se 250 (dyqind e pesëdhjetë) persona të punësuar, gjatë ushtrimit të aktivitetit të tij të biznesit ai bën përpunim të rregullt e të shtrirë në kohë (pra jo rastësor) për kategorinë e të dhënave "*punonjës*", "*klientë*", etj. (*shih pika 4 e nenit 27 të Ligjit*).

   Mungesa e këtij dokumentacioni dhe mosrespektimi 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 të Komisionerit, 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.

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 20.11.2025 "*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*").

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 Udhëzimin 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.

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;

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

- Nuk ka të hartuar planin e politikave të vazhdueshmërisë së biznesit, dokumente këto që do të duhet të përmbanin politikat dhe objektivat që sigurojnë vazhdueshmërinë 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.

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 drejtpërdrejtë 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. 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 garantimi i ndërgjegjësimit dhe përgjegjësisë të çdo nëpunësi që ka akses në të dhëna personale, duke përcaktuar në mënyrë të qartë, kufijtë e përpunimit të lejuar, ndalimin e përdorimit të të dhënave për qëllime personale apo të paautorizuara, detyrimin për ruajtjen e konfidencialitetit edhe pas përfundimit të marrëdhënies së punës. Ky instrument përbën një masë thelbësore organizative në kuadër të parimit të përgjegjshmërisë, duke dokumentuar faktin se, Kontrolluesi ka marrë masa konkrete për të garantuar përpunim të ligjshëm dhe të sigurt të të dhënave personale, sipas parashikimeve të nenit 30 të Ligjit.

10. 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 19.05.2026, të organizuar nga Zyra e Komisionerit, gjatë të cilës ka deklaruar angazhimin për rikuperimin e shkeljeve të konstatuara gjatë hetimit administrativ, si dhe bashkëpunimin me Komisionerin për të siguruar që çdo mangësi të adresohet në përputhje me Ligjin.

Gjithashtu, nga ana e Kontrolluesit, me shkresën nr. 825/5 prot., datë 20.05.2026, është përcjellë dokumentacioni në format CD, në funksion të përmbushjes së detyrimeve të Ligjit dhe masat e marra, i cili përfshin aktet e mëposhtme:

- Rregullore dhe dokumente administrative;
- Dokumentacion lidhur me Sistemin e Menaxhimit të Sigurisë së Informacionit në të cilën përfshihen dokumentet:
- Kodin e sjelljes, i cili parashikon qëllimin, fushën e zbatimit, detyrat dhe përgjegjësitë e punonjësit, dokumente të lidhura të tilla si: politikat SMSI, marrëveshjet e konfidencialitetit, procedurat e brendshme, politikat HSE, etj.;
- Plani i rekuperimit nga fatkeqësitë;
- Kodin e etikës së biznesit, nëpërmjet të cilit parashikohet angazhimi i Kontrolluesit për ushtrimin e përgjegjshëm të veprimtarisë, si dhe masat për mbrojtjen e informacionit;
- Poltikat e sistemit të menaxhimit të sigurisë së informacionit;
- Plan evakuimi në rast emergjence;
- Plan i vazhdimësisë së biznesit;
- Politika e menaxhimit të incidenteve;
- Politikat e rekrutimit;
- Politika e daljes në pension;
- Politika e komunikimit të jashtëm;
- Politika e kontrollit të aksesit;
- Procedura back-up;
- Deklara e pranimit të riskut;
- Raport auditimi i brendshëm për SMSI;
- Raport incidenti;
- Fusha e zbatimit të SMSI-ve;
- Procedura e kërkesave ligjore dhe kontraktuale;
- Politika për përdorimin e internetit, e-mailit dhe kompjuterëve;
- Politikat për pajisjet portative;
- Politikat e tavolinës së pastër;
- Politika për skanimin e cenueshmërive;
- Politika e fjalëkalimeve për llogaritë e përdoruesve;
- Politika e Menaxhimit të Kapaciteteve të Sistemeve IT;
- Politika për menaxhimin e dhunës në vendin e punës;

- Politika e Antivirusit dhe Antispamit;
- Webpage CFO Pharma Privacy Policy;
- 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, 7, 8, 13, 27, 28, 30, 33, 34, 81, 82, 83 dhe 84 të Ligjit, Komisioneri,

REKOMANDON:

1. Kontrolluesi, Shoqëria "*CFO Pharma*" shpk, 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, Shoqëria "*CFO Pharma*" shpk, të ketë në vëmendje përcaktimin e planeve të kamerave përmes sistemit të video-survejimit (CCTV), në përputhje me parashikimet e neneve 6 dhe 7 të Ligjit.

3. Kontrolluesi, Shoqëria "*CFO Pharma*" shpk, të ketë në vëmendje marrjen dhe administrimin e "*Pëlqimit*" të subjekteve të të dhënave në përputhje me parimet dhe kriteret ligjore të sanksionuara në nenet 6, 7 dhe 8 të Ligjit;

4. Kontrolluesi, Shoqëria "*CFO Pharma*" shpk, të ketë në vëmendje përditësimin e rubrikës "*Politikat e Privatësisë*", në faqen zyrtare https://www.cfopharma.com, me qëllim informimin e plotë të subjekteve të të dhënave, sipas parashikimeve të nenit 13 të Ligjit;

5. Kontrolluesi, Shoqëria "*CFO Pharma*" shpk, në zbatim të nenit 27 dhe 28 të Ligjit, të ketë në vëmendje përditësimin e aktit të brendshëm rregullator "*SOP për Politikën e Mbrojtjes së të Dhënave*", 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.;

6. Kontrolluesi, Shoqëria "*CFO Pharma*" shpk, në zbatim të nenit 30 të Ligjit, të ketë në vëmendje hartimin dhe aplikimin e "*Deklaratës së Konfidencialitetit*" për

punëmarrësit, të cilët kanë akses në mbledhjen, përpunimin dhe ruajtjen e të dhënave personale;

7. Kontrolluesi, Shoqëria "*CFO Pharma*" shpk, të marrë masa lidhur me trajnimin e punonjësve që kanë akses dhe përpunojnë të dhëna personale, sipas parashikimeve të neneve 33 dhe 34 të Ligjit;

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

   (i) vazhdimisht, detyrimet e përcaktuara në pikat 1,2, 3, 4, 5 dhe 6 më sipër;
   (ii) brenda 45 (dyzet e pesë) ditëve, detyrimet e përcaktuara në pikën 7 më sipër.

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

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

10. 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 03.06.2026.

KOMISIONERI

Besnik Dervishi