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.594/5 prot. Tiranë më 01.6.2023

VENDIM

Nr. 23, datë 01.6.2023

PËR KONTROLLUESIN "POSTA SHQIPTARE SH.A SI DHE STRUKTURA NË VARËSI TË SAJ (ZYRA POSTARE TIRANA 5, ZYRA POSTARE TIRANA 2, ZYRA POSTARE TIRANA 8)"

Në mbështetje të neneve 29, 30, 31 dhe 32 të ligjit nr. 9887, datë 10.03.2008 *"Për mbrojtjen e të dhënave personale*" i ndryshuar (në vijim, *"Ligji"*), neneve 77-112 të ligjit nr. 44/2015 *"Kodi i Procedurave Administrative të Republikës së Shqipërisë"* (në vijim, *"Kodi i Procedurave Administrative"*), procesverbalit të hetimit administrativ dhe provave të administruara në ngarkim të Kontrolluesit *"Posta Shqiptare SH.A si dhe struktura në varësi të saj (Zyra Postare Tirana 5, Zyra Postare Tirana 2, Zyra Postare Tirana 8)"*.

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 45, datë 15.03.2023 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim, *"Komisioneri"*), u krye hetim administrativ pranë Kontrolluesit *"Posta Shqiptare SH.A si dhe struktura në varësi të saj (Zyra Postare Tirana 5, Zyra Postare Tirana 2, Zyra Postare Tirana 8)"* (në vijim, *"Kontrolluesi"*) me objekt:

- *Zbatimi i ligjit nr. 9887, datë 10.03.2008 "Për mbrojtjen e të dhënave personale", i ndryshuar dhe akteve të miratuara nga Komisioneri në lidhje me mbledhjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale, gjatë kryerjes së aktivitetit nga Kontrolluesi "Posta Shqiptare SH.A si dhe struktura në varësi të saj (Zyra Postare Tirana 2, Zyra Postare Tirana 5, Zyra Postare Tirana 8)".*

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

Komisioneri, pasi shqyrtoi relacionin e hetimit administrativ, procesverbalin e konstatimit dhe provat e administruara gjatë ushtrimit të hetimit pranë Kontrolluesit, vëren se:

1. Posta Shqiptare SH.A, ushtron veprimtarinë në tregun e shërbimeve postare, bazuar në Ligjin nr. 46/2015 "*Për Shërbimet Postare në Republikën e Shqipërisë*"; Ligjin nr. 9901, datë 14.04.2008 "*Për Tregtarët dhe Shoqëritë Tregtare*", i ndryshuar; Ligjin nr. 9918, datë 19.05.2008 "*Për Komunikimet Elektronike në Republikën e Shqipërisë*", i ndryshuar, si dhe aktet e tjera normative të dala në zbatim të tyre. Kontrolluesi, gjatë ushtrimit të aktivitetit në funksion të përmbushjes së qëllimit si ofrues i shërbimeve postare kryen dhe ofron shërbime financiare dhe bankare.

   Kontrolluesi, operon nëpërmjet filialeve rajonale dhe zyrave postare në të gjithë territorin e Republikës së Shqipërisë. Kontrolluesi, ka një shtrirje të gjerë përgjatë gjithë territorit të Republikës, mbi 2400 punonjës dhe rreth 533 zyra postare.

   Kontrolluesi, përpunon të dhëna personale për subjektet e të dhënave personale "*klientë*", "*punonjës*", "*vizitorë*", "*ish-punëmarrës*", "*kandidatë për punë*", etj. Përpunimi i të dhënave kryhet në mënyrë manuale dhe elektronike.

2. Konstatohet se, të dhënat e *"ish-punëmarrësve"* dhe *"kandidatë për punë"*, ruhen në arkivën fizike dhe elektronike të Kontrolluesit. Përmbajtja e dosjeve personale të ish-punëmarrësve konsiston në dokumente origjinale, të noterizuara dhe/ose të fotokopjuara të tilla si "*jetëshkrim, kopje të kartës së identitetit, vërtetim i gjendjes gjyqësore, etj*.". Gjithashtu, të dhënat e kandidatëve për punë si "*emër, mbiemër, nr.tel, adresa, arsimimi, etj*.", ruhen në arkivat elektronike. Këto të dhëna, ruhen nga Kontrolluesi pa përcaktuar një afat konkret të ruajtjes së tyre, në kundërshtim me germën "*d*", të pikës 1, të nenit 5 të Ligjit dhe Udhëzimin nr. 42 , datë 22 .07.2014 për "*Përpunimin e të dhënave personale të kandidatëve për punë*".

   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, në përputhje me parashikimin e germës *"d",* të pikës 1, të nenit 5 të Ligjit.

   Kontrolluesi ka detyrimin të përpunojë të dhënat personale, për aq kohë sa ekziston qëllimi për të cilin ato janë mbledhur. Në momentin e përfundimit të qëllimit të përpunimit, duhet të realizojë shkatërrimin e këtyre të dhënave, pasi përpunimi i mëtejshëm i tyre konsiderohet i paligjshëm.

3. Veprimtaria e Kontrolluesit realizohet, ndër të tjera, nëpërmjet sistemeve elektronike si, Eterna Postare, Eterna Financiare (me modulet: financë kontabilitet, burime

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

njerëzore, magazinë), Eposta-Versioni mobile II, Sistemit Core Eterna, IPS-International Postal System, CDS-Custom Declaration System, Sistemi i monitorimit të rrjetit PRTG.

Qendra e të dhënave të Kontrolluesit është infrastruktura kompjuterike ku bëhet përpunimi dhe ruajtja e të gjithë informacionit, mbi të gjithë shërbimet e ofruara nga zyrat postare, degët dhe filialet e shoqërisë. Mbi këtë infrastrukturë është ngritur sistemi qendror i shoqërisë, për ofrimin e shërbimeve të informatizuara postare dhe financiare, nëpërmjet të cilit ofrohet një numër shumë i madh ndërfaqesh që mundësojnë lidhjen e sistemit qendror të shoqërisë, me infrastruktura dhe palë të treta.

Sistemet kryesore që Posta Shqiptare realizon veprimtarinë e saj janë, sistemi elektronik Eterna Posta dhe Eterna Financiare.

Sa i përket sistemit Eterna Posta, Posta Shqiptare përcakton qëllimet dhe mënyrën e përpunimit të të dhënave personale dhe si i tillë referuar pikës 5, të nenit 3 të Ligjit, gëzon cilësinë e Kontrolluesit. Sa i përket sistemit Eterna Financiare, Posta Shqiptare përpunon të dhëna personale në emër të palëve të treta, me qëllim ofrimin e shërbimeve financiare për ta.

Sistemet Eterna Posta dhe Eterna Financiare hostohen në makina virtuale në server-a fizik, me komponentë mbështetës TIK. Përdoruesit administrativ të sistemeve, operatorë/punonjës dhe klientët, kanë mundësi që ti aksesojnë online. Site "*Primar*" dhe site "*DRC*", janë të ngritura si makina virtuale, të mbështetura sipas metodave "*VMware vSphere*". Komponentët e infrastrukturës së rrjetit përfshijnë: Firewall, Hardware Load Balancer, Switches, Storage Backup, etj.

Sistemet Eterna financiare dhe Eterna Posta ngrihen mbi:

a. Sisteme Operimi Windows Server 2012/64;
b. Database: SQL Server;
c. Application server;
d. Database Server;
e. Datawarehouse Server;
f. Makina për virtualizim;
g. vCenter;
h. NAS (Network Attached Storage);
i. SAN (Storage Area Network);
j. vSphere.

Eterna Posta përbëhet nga modulet: Pranimi i objekteve, Konfigurim dhe përshtatja, Dorëzimi, Gjurmimi, Përpunim dhe shpërndarje, Thasët, Transporti, Dogana, Sorter, IPS-International, E-Postieri, E-Posta.

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

Sistemi Eterna Posta, me qëllim shkëmbimin e të dhënave, ndërvepron me sistemin ndërkombëtar të postave IPS (Internacional Postal System), në të cilën shkëmbehen të dhëna të klientëve dërgues dhe marrës (Emër, Mbiemër, adresa, numri i celularit, etj.). Në çdo rast, janë klientët të cilët paraqiten në sportelin e zyrave postare dhe japin informacion dhe të dhënat në lidhje me shërbimin postar që kërkojnë.

Eterna Financiare përbëhet nga modulet: Shërbime Financiare në Sportel, Utilitete, Ndihma ekonomike, Shërbime Bankare, Kopshte/Çerdhe, Transferta Parash, Taksa dhe Tatime, Pagesa të përgjithshme, Eterna Gateway, Core Banking, Administrim i klientëve, Llogaritë e Klientëve, Transaksione të Përgjithshme, Burime Njerëzore, Asete, Financë dhe Kontabilitet, Ndërveprime dixhitale me palët e treta, Raporte të integruara, etj.

Sistemi Eterna Financiare, ndërvepron me sistemin Eterna Posta, si dhe me sisteme të palëve të treta, të tilla si, institucione shtetërorë (OSHE, Policia, etj.), institucionet financiare jo bankare (NOA, Iutecredit, etj.).

Konstatohet se, Kontrolluesi disponon gjithashtu aplikacionin "*e-Posta*", i cili operon online për klientët, me qëllim marrjen e shërbimeve nga sistemi Eterna Posta dhe Eterna Financa. Çdo përdorues që regjistrohet nëpërmjet këtij aplikacioni, plotëson të dhënat si, "*emri, mbiemri, adresa e email-it dhe numri i telefonit*". Adresa e email-it shërben në mënyrë që të merret kodi i aktivizimit. Aplikacioni e-Posta, është një platformë digjitale e cila mundëson që nëpërmjet kompjuterit, smartphone-it ose tablet-it të kryhen veprimet e mëposhtme:

- Shkarkimi në mobile i aplikacionit e-Posta dhe regjistrimi fillestar i përdoruesit;
- Kryerjen e veprimeve financiare;
- Aprovim i llogarisë së klientit pranë sporteleve të Postës Shqiptare;
- Ngarkim i gjendjes së llogarisë së klientit e-Wallet (Llogaria e-Wallet është një portofol elektronik i Postës Shqiptare që mund të përdoret nga klientët e saj për të bërë pagesa të utiliteteve të ndryshme, me komision 0) pranë sporteleve të postës shqiptare;
- Lidhja me profilin e klientit të kontratave dhe shërbimeve të klientit (kontratë e energjisë elektrike, kontratë e ujësjellësit, pagesa gjobash, pagesa të detyrimeve doganore, si dhe shërbime të tjera që do të mundësohen nëpërmjet kësaj platforme);
- Kontrolli në kohë reale dhe në mënyrë të sigurt të të gjithë veprimeve financiare dhe Postare;
- Kontrollin e transfertave të parave në rolin e marrësit ose të dërguesit;
- Aksesim i sistemit e-Posta nga web, mobile;
- Kontroll për pakot postare dhe regjistrim i tyre për verifikim të mëtejshëm;
- Opsion për të gjetur zyrën postare më të afërt nisur nga lokacioni i klientit.

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

Nga verifikimi on-site i sistemeve *"Eterna Posta dhe Eterna Financiare"* dhe aplikacionit "*e-Posta*" si dhe nga shqyrtimi i procedurave rregulluese që disponon Kontrolluesi, rezulton se:

- Nuk ka praktika të dokumentuara për menaxhimin e riskut, teknikat e menaxhimit dhe të performancës të përcaktuara sipas procedurës të parashikuar në aktin me nr. 2144/2 prot, datë 09.08.20219 "*Metodologjia e vlerësimit të riskut*";
- Nuk ka formalizuar një procedurë zyrtare të raportimit dhe menaxhimit ndaj incidenteve të teknologjisë së informacionit;
- Nuk ka të hartuar planin e politikave të vazhdueshmërisë së biznesit, dokumente këto që do të duhet të përmbanin politikat dhe objektivat e miratuara që sigurojnë vazhdueshmërinë e punës së sistemeve;
- Nuk ka një rregullore apo procedurë të miratuar për personat e autorizuar që mund të hyjnë në dhomën e server-ave;
- Nuk ka kryer auditime në lidhje me riskun dhe kontrolli e sigurisë së aplikacionit e-Posta, në të dy versionet e ofruara, Android dhe IOS;
- Nuk ka marrë masa për të kryer një vlerësim të ndikimit të operacioneve të përpunimit në të dhënat personale.

Kontrolluesi disponon disa politika/procedura si: Standardi i Menaxhimit të Problemeve dhe Incidenteve, Rregullore për lidhjen në distancë, megjithatë konstatohet se këto dokumente nuk janë të miratuara nga asnjë prej organeve drejtuese të Kontrolluesit.

Zyra e Komisionerit vlerëson se, Kontrolluesi duhet të kryejë auditime të vazhdueshme mbi hedhjen e të dhënave dhe funksionimin e sistemeve respektive, kjo me qëllim për të parandaluar çdo cedim të mundshëm të funksionimit të sistemit. Analizimi periodik i veprimeve/gjurmëve të përdoruesve apo të funksionimit të sistemit nëpërmjet log-eve/events, minimizon rrezikun si dhe rrit sigurinë mbi verifikimin, apo lokalizimin e problemit.

Krijimi i procedurave të backup dhe vazhdimësisë së punës për Sistemet e Informacionit si dhe zbatimi i tyre, duhet të adresohet nga strukturat përgjegjëse me qëllim garantimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të shërbimit.

Ofrimi i aksesit online të sistemeve elektronike për përdoruesit nëpërmjet aplikacionit e-Posta, kërkon marrjen e masave teknike të shtuara, të tilla si, auditime dhe vlerësime teknike të sigurisë së aplikacionit e-Posta.

Sa më sipër, Zyra e Komisionerit vlerëson se, kjo situatë përbën një risk të shtuar për sa i përket sigurisë së të dhënave, pasi në rast të një dëmtimi, humbjeje apo kompromentimi të këtyre të dhënave, nuk mund të identifikohet gjurmimi dhe përgjegjësia.

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

Përveç sistemeve elektronike që disponon Kontrolluesi, punonjësit aksesojnë sisteme elektronike të tjera që kryejnë veprime dhe raporte mbi shitjet e kryera, konkretisht: Portali i pagesave të pensioneve; e-Albania; Moneygram; Digitalb; etj. Konstatohet se, Kontrolluesi për shërbimet që kryhen nëpërmjet portalit e-Albania, regjistron subjektet e të dhënave "*klientë*", manualisht në sistemin Eterna Finaciare, po ashtu dhe fatura printohet nga sistemi me kushtin nëse regjistrimi është kryer njëherë në këtë sistem.

Kontrolluesi nëpërmjet zyrave postare, mundëson gjithashtu edhe ofrimin e shërbimeve qeveritare për qytetarët nëpërmjet portalit e-Albania. Për të kryer një shërbim, punonjësi duhet të logohet në portalin e-Albania, dhe mund të gjenerojë nga portali dokumentin e kërkuar, nga subjektet e të dhënave, qytetar apo përfaqësues të biznesit, të cilët janë paraqitur me një dokument identifikimi, si dhe duhet të japin pëlqimin përmes një formulari *"Autorizim për gjenerimin e dokumenteve nga portali e-Albania"*. Niveli i aksesimit të portalit e-Albania nga Kontrolluesi është në nivele supervisori, përdoruesi dhe administratori, sipas funksionit administrativ të punonjësit. Punonjësit që kryejnë këtë shërbim janë të pajisur me llogari (user) respektive në portalin e-Albania. Punonjësit që kanë akses në këto sisteme elektronike rezultojnë se nuk janë të trajnuar mbi këto sisteme, si dhe nuk janë të informuar se nëpërmjet shërbimeve e-Albania kryhet përpunim i të dhënave personale të qytetarëve, të cilat mbrohen me Ligj.

Zyra e Komisionerit vlerëson se, për shkak të natyrës së veprimtarisë së Kontrolluesit, punonjësit duhet të kryejnë trajnime në lidhje me sistemet e brendshme apo dhe sistemet e jashtme sipas proceseve të punës, me qëllim ndërgjegjësimin e punonjësve të cilët për shkak të punës përpunojnë të dhëna personale.

Për sa më sipër konstatohet se, Kontrolluesi nuk ka parashikuar rregulla të qarta dhe të hollësishme për sigurimin e të dhënave personale të cilat përpunon, në kundërshtim me parashikimet e 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*").

Grupi i hetimit konstaton se, në Sistemet Eterna Posta dhe Eterna Financiare, ruhen të dhënat e subjekteve të të dhënave "*klientë*" që nga koha e krijimit dhe ngarkimit të tyre në bazat e të dhënave, nëpërmjet moduleve respektive, në kundërshtim me parimin e mbrojtjes së të dhënave personale, të parashikuar në germën "*d*", të pikës 1, të nenit 5 të Ligjit.

Gjithashtu, konstatohet se në sistemin Eterna Financiare ngarkohen manualisht në formatin "*Excel*", të dhënat për subjektet e të dhënave "*Përfitues së ndihmës ekonomike*" dhe "*Përfitues të skemës së aftësive të kufizuara*". Këto të dhëna dërgohen nga njësitë bashkiake në formatin elektronik dhe manual, në filialet rajonale të Postës Shqiptare, dhe punonjësit e këtyre filialeve kryejnë dhe ngarkimin e tyre në sistem.

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

Konstatohet se, për këto subjekte, të dhënat e tyre ruhen pa afat në databazë. Gjithashtu, konstatohet se këto të dhëna të dërguara në rrjet, nëpërmjet komunikimeve elektronike, të tilla si posta elektronike, përbëjnë risk për sigurinë e të dhënave, në kundërshtim me parashikimet e nenit 27 të Ligjit.

Grupi i hetimit ka shtrirë hetimin edhe në Zyrën Postare Tirana 2, Zyrën Postare 5, dhe Zyrën Postare 8, të cilat janë në varësi të Filialit Tiranë, dhe veprojnë sipas udhëzimeve të këtij filiali, si dhe të Postës Shqiptare. Nga verifikimi në vend rezultoi se, në Zyrën Postare 2, në regjistrat fizik të historikut të shërbimeve postare, ruhen pa afat të dhënat e klientëve si "*emër, mbiemër, NID, firma*", në kundërshtim me germën "*d*", të pikës 1, të nenit 5 të Ligjit.

Zyra e Komisionerit vlerëson se, Kontrolluesi duhet të bëjë një vlerësim rast pas rasti, për të gjitha proceset e përpunimit të të dhënave në mbështetje të ligjeve apo akteve nënligjore që rregullojnë fushën e veprimtarisë dhe mbas analizimit të secilit proces përpunimi, duhet të marrë masa për përcaktimin dhe rregullimin e afateve kohore për ruajtjen e të dhënave për secilën kategori të dhënash, në sistemet elektronike dhe në arkivën fizike. Koha e ruajtjes së të dhënave duhet të përcaktohet nga Kontrolluesi, në përputhje me parashikimet ligjore specifike dhe qëllimin e përpunimit.

Gjithashtu, Zyra e Komisionerit vlerëson 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 27 të Ligjit, si dhe Udhëzimit nr. 47, datë 14.09.2018 të Komisionerit *"Për përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga subjektet përpunuese të mëdha"*, (në vijim*, "Udhëzimi nr.47"*).

4. Kontrolluesi ka të instaluar një sistem video-survejimi, CCTV *(HikCentral Professional)* me anë të së cilit mbikëqyr korridoret, ambientet e brendshme, si dhe Zyrat Rajonale të Filialeve. Nga verifikimi në sistemin e video-survejimit (CCTV), konstatohet se të dhënat imazhe-video ruhen për një periudhë mbi 60 ditë, në kundërshtim me germën "*d*", të pikës 1, të nenit 5 të Ligjit, si dhe me Udhëzimin nr. 3, datë 05.03.2010 të Komisionerit "*Mbi përpunimin e të dhënave personale me sistemin e video survejimit në ndërtesa dhe mjedise të tjera*", i ndryshuar (në vijim, "*Udhëzimi nr. 3*").

   Zyra e Komisionerit vlerëson se, Kontrolluesi ka detyrim të përpunojë të dhënat personale të subjekteve të të dhënave nëpërmjet sistemit CCTV për aq kohë sa ekziston qëllimi për të cilin janë grumbulluar dhe përpunuar. Në momentin që qëllimi ka përfunduar duhet të realizojë shkatërrimin e të dhënave imazheve/video, në të

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

kundërt përpunimi i mëtejshëm i të dhënave konsiderohet i paligjshëm, në përputhje me Udhëzimin nr. 3 të Komisionerit dhe me germën "*d*", të pikës 1, të nenit 5 të Ligjit.

5. Posta Shqiptare nëpërmjet formularit *"Deklaratë burimi i pasurisë"*, përpunon të dhëna personale për subjektet e të dhënave, për efekt të vërtetësisë së plotësimit të formularit të veprimeve cash. Konstatohet se, Kontrolluesi në këtë formular që aplikon "*Deklaratë burimi i pasurisë*" nuk ka të parashikuar asnjë rubrikë, në mënyrë që të informojë subjektet e të dhënave mbi përpunimin e të dhënave, në kundërshtim me parashikimet e nenit 18 të Ligjit.

   Zyra e Komisionerit vlerëson se, informimi i subjekteve të të dhënave personale është një nga detyrimet bazë të Kontrolluesit pasi u jep mundësinë subjekteve të të dhënave personale të njihen me të drejtat që gëzojnë dhe mundësinë e ushtrimit të tyre në praktikë. Mospërmbushja e këtij detyrimi nga Kontrolluesi mund të sjellë pasoja të rënda sa i përket privatësisë dhe përpunimit të të dhënave personale të subjekteve të të dhënave. Informimi sipas përcaktimeve të nenit 18 të Ligjit, duhet të aplikohet për çdo proces përpunimi të të dhënave personale të subjekteve të të dhënave, që kryen Kontrolluesi.

6. Kontrolluesi ka marrëdhënie kontraktuale me palët e treta, për marrjen e shërbimeve gjatë ushtrimit të veprimtarisë së tij, konkretisht:

   Kontrolluesi ka lidhur më datë 18.07.2019, me subjektin "Helius System shpk" kontratë *"Mirëmbajtja e Moduleve të Eternës (Financa-kontabilitet, Burimet njerëzore, Magazina, Help Desk)" për 4 vite.*
   Kontrolluesi ka lidhur kontratë me subjektin "Helius System shpk" me objekt *"Mirëmbajtja e Sistemit Eterna për tre vite"*.

   Gjithashtu, në cilësinë e ofruesit të shërbimeve, për palët e treta konstatohet se ka lidhur marrëveshje, kontrata, të tilla si:

   Akt-marrëveshje, datë 26.11.2015, midis "*IuteCredit Albania*" dhe Posta Shqiptare me objekt *"Posta i ofron "Iutecredit Albania" shërbimin e pagesës së mikrokredive dhe arkëtimin e kësteve të kredisë të klientëve të saj, si dhe transferimin e fondeve të arkëtuara për llogari të "Iutecredit Albania"*.

   Kontratë, datë 28.06.2017, midis Iutecredit Albania dhe Posta Shqiptare me objekt "*Qëllimi i kontratës është zgjerimi i marrëdhënieve ndërmjet dy palëve ku nëpërmjet të cilit bihet dakord që Posta Shqiptare do të ofrojë në çdo pikë të vetën, ku plotësohen kushtet për realizimin e objektit të kësaj marrëveshje...*"

   Si dhe kontrata të tjera si:
   - Kontratë shërbimi, datë 13.01.2020, midis "Furnizuesi i Shërbimit Universal Sh.A" dhe Posta Shqiptare;

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

- Marrëveshje për shërbimet financiare, datë 13.02.2020, midis Autoritetit Kombëtar të Ushqimit (AKU) dhe Postës Shqiptare;
- Marrëveshje bashkëpunimi, datë 19.12.2022, midis Bashkisë Kamëz dhe Posta Shqiptare;
- Akt-Marrëveshje, datë 28.02.2006, midis Korporatës Elektroenergjitike Shqiptare dhe Postës Shqiptare;
- Marrëveshje për shërbimet publike elektronike në portalin unik qeveritar e-Albania, datë 25.01.2019, midis Agjencisë Kombëtare të Shoqërisë së Informacionit dhe Postës Shqiptare;
- Kontrolluesi disponon modelin *"tip"* kontratë shërbimi midis punonjësve të postës dhe Klientëve të e-Posta. Gjithashtu, Kontrolluesi disponon modelin "*tip*" kontratë për shërbim të parasë elektronike për biznesin.

Nga shqyrtimi i përmbajtjes së marrëveshjeve/kontratave të cituara më sipër rezulton se, nuk janë reflektuar detyrimet sipas parashikimeve të nenit 20 të Ligjit dhe Udhëzimit nr. 19, datë 03.08.2012 të Komisionerit *"Mbi rregullimin e marrëdhënieve mes kontrolluesit dhe përpunuesit në rastet e delegimit të përpunimit të të dhënave dhe përdorimin e një kontrate tip në rastet e këtij delegimi" i ndryshuar (në vijim*, "Udhëzimi nr. 19").

Zyra e Komisionerit vlerëson se, të gjitha detyrimet e sanksionuara në nenin 20 të Ligjit dhe Udhëzimit nr. 19 të Komisionerit, duhet të jenë të përfshira në kontratën dhe/ose aneks kontratën e shkruar mes Kontrolluesit dhe Përpunuesit. Çdo kontratë përpunimi (*outsourcing*) që ka për qëllim delegimin e përpunimit të të dhënave personale duhet të përmbaj dispozita që vendosin rregulla për përpunimin e të dhënave personale, sipas legjislacionit në fuqi.

Në rastet e delegimit të përpunimit të të dhënave dhe/ose shërbimit, Kontrolluesi duhet të sigurohet që përpunuesi të garantojë përpunim të ligjshëm dhe të sigurt të të dhënave. Detyrimet e përpunuesit për përpunim të ligjshëm të të dhënave personale, parashikohen në nenin 20 të Ligjit dhe rregullohen me aplikimin e parashikimeve të Udhëzimit nr. 19.

7. Nga verifikimi i kryer në Regjistrin Elektronik të subjekteve kontrolluese dhe në protokollin e Zyrës së Komisionerit rezulton se, Kontrolluesi ka "*Njoftuar*" mbi përpunimin e të dhënave personale për të cilat është përgjegjës. Gjatë hetimit administrativ të ushtruar, është konstatuar se "*Njoftimi*" ka mangësi në deklarim, sa i përket rubrikave të formularit si vijon:

   i. Deklarimin në rubrikën 1.2, të formularit të njoftimit *"personi i kontaktit i ngarkuar nga subjekti";*
   ii. Deklarimin në rubrikën 3, të formularit të njoftimit *"kategoritë e subjekteve të të dhënave personale që përpunohen",* të tilla si *"vizitorë";*

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

iii. Deklarimin në rubrikën 4, të formularit të njoftimit *"kategoritë e të dhënave personale që përpunohen"*, të tilla si *"video"*;
iv. Deklarimin në rubrikën 6, të formularit të njoftimit "*qëllimi i përpunimit"* të tilla si *"ofrimi i shërbimeve për kontrollues privatë"*.

Konstatimet e mësipërme janë në kundërshtim me parashikimet e neneve 21 dhe 22 të Ligjit.

Zyra e Komisionerit vlerëson se, realizimi i detyrimit për ndryshimin e gjendjes së "*Njoftimit*" të përpunimit të të dhënave sipas parashikimeve të nenit 21 dhe 22 të Ligjit është i rëndësishëm, pasi i jep mundësinë subjekteve të të dhënave që të informohen mbi përpunimin që kryen Kontrolluesi dhe realizimin e detyrimeve ligjore. Kjo i jep mundësi reale subjektit të të dhënave për të ushtruar në mënyrë korrekte të drejtat që i jep Ligji.

8. Kontrolluesi ka miratuar Rregulloren "*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*". Megjithatë, konstatohet se Rregullorja nuk parashikon proceset, procedurat, masat teknike dhe organizative specifike mbi mënyrën e përpunimit të të dhënave personale, sigurinë e të dhënave, konfidencialitetin, afatet e mbajtjes së të dhënave, etj., në kundërshtim me parashikimet e nenit 27 të Ligjit.

   Zyra e Komisionerit vlerëson se, hartimi i një Rregullore specifike "*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*", në të cilën të parashikohen rregulla dhe procedura organizative specifike mbi mënyrën e përpunimit të të dhënave personale (*për çdo kategori të dhënash*), sigurinë e të dhënave, konfidencialitetin, afatet e mbajtjes së të dhënave, nivelet e aksesit etj., konsiderohet një detyrim shumë i rëndësishëm në zbatim të nenit 27 të Ligjit, pasi shmang pasojat e rënda që mund të vijnë për subjektet e të dhënave.

9. Kontrolluesi nuk ka ndërmarrë masa konkrete në kuadër të trajnimit të punonjësve që kanë akses dhe përpunojnë të dhëna personale lidhur me legjislacionin në fuqi për mbrojtjen e të dhënave personale. Grupi i kontrollit konstaton mosplotësim të detyrimeve në lidhje me ngritjen, administrimin dhe mirëmbajtjen e sistemit të menaxhimit së sigurisë së informacionit (SMSI) lidhur me mbrojtjen e të dhënave personale, të parashikuara në Udhëzimin nr. 47 të Komisionerit, për shkak të cilësisë si subjekt përpunues i madh, si dhe për shkak të natyrës së veçantë të veprimtarisë që Kontrolluesi ushtron.

   Zyra e Komisionerit vlerëson se Kontrolluesi duhet të marrë masa konkrete në kuadër të trajnimit të punonjësve që kanë akses dhe përpunojnë të dhëna personale, bazuar në legjislacionin në fuqi për mbrojtjen e të dhënave personale. Trajnimet në lidhje me mbrojtjen e të dhënave personale duhet të jenë të vazhdueshme dhe të përshtatura sipas nevojave dhe proceseve të punës të Kontrolluesit. Sipas përcaktimeve të Kreut

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

IV, të Udhëzimit nr. 47, është detyrim i subjektit përpunues të të dhënave personale që ti siguroj trajnim profesional operatorëve të cilët për shkak të proceseve të punës, janë të ngarkuar për përpunimin e të dhënave personale, me qëllim ndërgjegjësimin e tyre për detyrimet e Ligjit.

Zyra e Komisionerit vlerëson se, për shkak të cilësisë si subjekt përpunues i madh, si dhe për shkak të natyrës së veprimtarisë që ushtron, e cila kërkon masa të shtuara teknike dhe organizative për garantimin e sigurisë së të dhënave personale, Kontrolluesi, është i detyruar të krijojë, mirëmbajë dhe administrojë SMSI në përputhje me parashikimet e Udhëzimit nr. 47.

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

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 vënë në dispozicion Kontrolluesit përmes nëpunësit të protokollit të Zyrës së Komisionerit.

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 gjatë seancës dëgjimore nuk paraqiti pretendime me shkrim, megjithatë lidhur me shkeljet e konstatuara nga grupi i kontrollit, ngritën pretendimet si më poshtë:

1. Lidhur me konstatimin se *"...ruhen të dhënat e subjekteve të të dhënave "klientë" që nga koha e krijimit dhe ngarkimit të tyre në bazat e të dhënave nëpërmjet moduleve respektive, në kundërshtim me parimet e mbrojtjes së të dhënave personale...",* Kontrolluesi argumenton se, *"..në rregulloren e AML-së është specifikuar që të dhënat e klientit, hapjen e llogarisë, kryerjen e një shërbimi rastësor, të dhënat mbahen 5 vite dhe maksimumi 40 vite. Megjithatë kjo rregullore nuk është vendosur në dispozicion të grupit të kontrollit.."*

   Lidhur me këtë pretendim të Kontrolluesit, Zyra e Komisionerit vlerëson se nuk qëndron pasi, në kontekstin e plotë të konstatimeve të pikës 3, të procesverbalit të hetimit administrativ, ka rezultuar se, të dhënat që popullojnë të dy sistemet kryesore Eterna Financiare dhe Eterna Postare ruhen në bazën e të dhënave respektive që nga koha e krijimit.

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

Zyra e Komisionerit vlerëson se, të dhënat personale të subjekteve të të dhënave duhet të mbahen në atë formë, që të lejojë identifikimin e subjekteve të të dhënave për një kohë, por jo më tepër sesa është e nevojshme për qëllimin, për të cilin ato janë grumbulluar ose përpunuar më tej.

Gjithashtu, Zyra e Komisionerit vlerëson se, përcaktimi i afateve kohore duhet të jetë i parashikuar konkretisht në akte të brendshme rregullore/politika, etj. Kontrolluesi duhet të identifikoj rast pas rasti kategoritë e të dhënave që përpunon dhe duhet të përcaktojë afatet e ruajtjes së këtyre të dhënave në aktet e veta të brendshme rregullatore, në përputhje me qëllimin e grumbullimit, apo afate të tjera të përcaktuara në një dispozitë ligjore konkrete.

Në përfundim, shkeljet e konstatuara gjatë ushtrimit të hetimit administrativ, në kuptim të germave *"a", "b", "ç", "d"* dhe *"dh"* të pikës 1 të nenit 39 të Ligjit, përbëjnë kundërvajtje administrative dhe sanksionohen me gjobë, si më poshtë:

a) kontrolluesit, që përdorin të dhëna personale në kundërshtim me kreun II "Përpunimi i të dhënave personale", dënohen me 10 000 deri në 500 000 lekë;
b) kontrolluesit, që nuk përmbushin detyrimin për të informuar, të përcaktuar në nenin 18 të këtij ligji, dënohen me 10 000 deri në 300 000 lekë;
ç) kontrolluesit ose përpunuesit, që nuk zbatojnë detyrimet e përcaktuara në nenin 20 të këtij ligji, dënohen me 10 000 deri në 300 000 lekë;
d) kontrolluesit, që nuk përmbushin detyrimin për të njoftuar, sipas përcaktimit në nenin 21 të këtij ligji, dënohen me 10 000 deri në 500 000 lekë;
dh) kontrolluesit ose përpunuesit, që nuk marrin masat e sigurisë së të dhënave dhe nuk zbatojnë detyrimin për ruajtjen e konfidencialitetit, të përcaktuara përkatësisht në nenet 27 dhe 28 të këtij ligji, dënohen me nga 10 000 deri në 150 000 lekë;

Në bazë të pikës 2 të nenit 39 të Ligjit, personat juridikë, për kundërvajtjet e mësipërme administrative, dënohen me dyfishin e gjobës së përcaktuar në pikën 1 të këtij neni.

Për zgjedhjen e masës së gjobës, Zyra e Komisionerit ka parasysh faktin që, shkeljet e konstatuara janë serioze nga ky Kontrollues. Ato lidhen me garantimin e parimeve dhe përpunimin e ligjshëm të të dhënave, me informimin dhe garantimin e të drejtave të subjekteve të të dhënave, si dhe marrjen e masave të përshtatshme tekniko-organizative për sigurinë e të dhënave personale. Gjithashtu, vendimi bazohet edhe në faktin se Kontrolluesi ka qenë edhe më herët subjekt kontrolli nga Zyra e Komisionerit, dhe ende reflekton mungesë angazhimi për të zbatuar detyrimet e legjislacionit për mbrojtjen e të dhënave.

PËR KËTO ARSYE:

Sa më sipër, në zbatim të neneve 5, 6, 18, 20, 21, 22, 27, 29, 30, 39 pika 1, germat *"a", "b", "ç", "d"* dhe *"dh"*, si dhe nenet 40 dhe 41 të Ligjit,

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

V E N D O S A:

1- Dënimin e Kontrolluesit me gjobë në vlerën 300 000 (treqind mijë) lekë, për shkelje të detyrimeve të përcaktuara në Kreun II të Ligjit;

2- Dënimin e Kontrolluesit me gjobë në vlerën 180 000 (njëqind e tetëdhjetë mijë) lekë, për shkelje të detyrimit të përcaktuar në nenin 18 të Ligjit;

3- Dënimin e Kontrolluesit me gjobë në vlerën 180 000 (njëqind e tetëdhjetë mijë) lekë, për shkelje të detyrimit të përcaktuar në nenin 20 të Ligjit;

4- Dënimin e Kontrolluesit me gjobë në vlerën 300 000 (treqind mijë) lekë, për shkelje të detyrimit të përcaktuar në nenet 21dhe 22 të Ligjit;

5- Dënimin e Kontrolluesit me gjobë në vlerën 150 000 (njëqind e pesëdhjetë mijë) lekë, për shkelje të detyrimit të përcaktuar në nenin 27 të Ligjit;

6- Kontrolluesi, të ketë në vëmendje proceset e përpunimit të të dhënave personale, për përcaktimin e afateve kohore për ruajtjen e të dhënave, në përputhje me germën *"d"*, të pikës 1, të nenit 5 të Ligjit;

7- Kontrolluesi, në zbatim të nenit 18 të Ligjit, të marrë masa konkrete, për përmbushjen e detyrimit për informimin e subjekteve të të dhënave personale;

8- Kontrolluesi, në zbatim të neneve 21 dhe 22 të Ligjit, të marrë masa për përditësimin e *"Njoftimit"* në lidhje me ndryshimin e gjendjes së njoftimit të përpunimit të të dhënave personale, të cilat përpunon;

9- Kontrolluesi, në zbatim të nenit 27 të Ligjit, të marrë masa për hartimin e një Rregullore specifike *"Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale"*, duke parashikuar 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;

10- Kontrolluesi, me qëllim garantimin e sigurisë së të dhënave personale, të zbatojë detyrimet e përcaktuara në Udhëzimin nr. 47, lidhur me trajnimin e stafit të tij si dhe sa i përket krijimit, mirëmbajtjes dhe administrimit të Sistemit të Menaxhimit të Sigurisë së Informacionit (SMSI) për mbrojtjen e të dhënave personale;

11- Kontrolluesi, për shkak të natyrës së veçantë të aktivitetit që ushtron, duhet të marrë masat e nevojshme për të vlerësuar mbi certifikimin e Sistemeve të Menaxhimit të

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al

Sigurisë së Informacionit, të të dhënave personale dhe mbrojtjes së tyre, sipas parashikimeve të Udhëzimit nr. 48;

12- Në zbatim të pikës 1 të nenit 32 të Ligjit, të përmbushen detyrimet sipas këtij akti brenda afateve si vijon:

i. vazhdimisht, detyrimet e përcaktuara në pikën 6 më sipër;
ii. brenda 15 (pesëmbëdhjetë) ditëve, detyrimet e përcaktuara në pikat 7 dhe 8 më sipër;
iii. brenda 30 (tridhjetë) ditëve, detyrimin e treguar në pikën 9 më sipër;
iv. brenda 45 (dyzetë e pesë) ditëve, detyrimet e treguara në pikën 10 më sipër;

Afatet e sipërpërmendura fillojnë nga data e marrjes në dijeni të këtij akti;

13- Kontrolluesi të njoftojë Zyrën e Komisionerit për masat e marra;

14- Gjoba arkëtohet nga kundërvajtësi në Buxhetin e Shtetit, jo më vonë se 30 (tridhjetë) ditë nga komunikimi i këtij Vendimi. Me kalimin e këtij afati, ky Vendim kthehet në titull ekzekutiv dhe ekzekutohet në mënyrë të detyrueshme nga Zyra e Përmbarimit;

15- Kundër këtij Vendimi mund të bëhet ankim në Gjykatën Administrative të Shkallës së Parë Tiranë, brenda 30 (tridhjetë) ditëve nga komunikimi i këtij Vendimi.

Ky Vendim u shpall sot më datë 01.6.2023.

KOMISIONERI

Besnik Dervishi

Adresa: Rruga *"Abdi Toptani"*, Nd.5, Tiranë Telefon: +355 42237200 www.idp.al, info@idp.al