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. 570 prot. Tiranë, më 31.01.2025

REKOMANDIM

Nr. 02, datë 31.01.2025

PËR KONTROLLUESIN "BANKA E PARË E INVESTIMEVE ALBANIA SHA"

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 *"Banka e Parë e Investimeve Albania sha"* (në vijim, *"Kontrolluesi"*),

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 189, datë 08.11.2024 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim, *"Komisioneri"*), u krye hetimi administrativ pranë Kontrolluesit, me objekt:

- *Zbatim i ligjit nr. 9887, datë 10.03.2008 "Për mbrojtjen e të dhënave personale", i ndryshuar, me fokus masat tekniko-organizative për përpunimin e tyre, veçanërisht sistemet e menaxhimit të sigurisë së informacionit (SMSI).*

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

1. Kontrolluesi është personi juridik i regjistruar në Regjistrin Tregtar Shqiptar me NIPT K72014801J dhe ushtron veprimtari bankare dhe veprimtari të tjera tregtare të përcaktuara me rregullore nga Banka e Shqipërisë, në Republikën e Shqiperisë, sipas përcaktimeve të ligjit Nr. 9662, datë 18.12.2006 "*Për Bankat në Republikën e Shqipërisë*" dhe të ligjit Nr. 8269, datë 23.12.1997 "*Për Bankën e Shqipërisë*".

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

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

2. Kontrolluesi administron dokumentacionin për punonjësit aktual dhe punonjësit e larguar, në dosje fizike si dhe në mënyrë elektronike.

   Konstatohet 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, në kundërshtim me germën "*d"* të pikës 1, të nenit 5 të Ligjit si dhe me Udhëzimin nr. 11, datë 08.09.2011 të Komisionerit "*Mbi përpunimin e të dhënave të punonjësve në sektorin privat*", i ndryshuar (në vijim, "*Udhëzimi nr. 11*").

   Zyra e Komisionerit vlerëson se, lidhur me të dhënat personale të grumbulluara, Kontrolluesi duhet të parashikojë ruajtjen e të dhënave personale në atë formë, që lejon identifikimin për një kohë të caktuar, por jo më tepër se sa është e nevojshme për të përmbushur qëllimin e grumbullimit. Koha e ruajtjes së të dhënave personale duhet të përcaktohet nga Kontrolluesi, në përputhje me parashikimet ligjore specifike dhe qëllimin e grumbullimit të informacionit.

3. Nga verifikimi i dosjeve të punonjësve aktual dhe të larguar konstatohet se përpunohet dokumentacioni si vijon:
   - Dokument identifikimi;
   - Foto;
   - Libreza e Punës;
   - Vërtetimin mjeko-ligjor;
   - Dëshmi Penaliteti;
   - Diplomë me listën e notave (fotokopje e noterizuar), si dhe certifikata kualifikimesh, trajnimesh, etj.;
   - Adresa e vendbanimit ose Certifikatë Personale;
   - Vërtetim Page (nga punësimi i fundit);
   - Dokumenta që vërtetojnë punët e mëparshme (vërtetime, rekomandime, etj.);
   - Job Announcement;
   - Job Application;
   - Deklaratë për ruajtjen e sekretit professional;
   - Letër dorëheqje/ Shkresë për tërheqje dokumentacioni në rastin e punonjësit të larguar.

   Konstatohet se Kontrolluesi mbledh informacion për kategoritë e subjekteve si "*Bashkëshorti(ja); Atësia; Mëmësia; Fëmijët; Vëllezër dhe/ose Motra*". Gjithashtu, në dosjen e punonjësit administrohet ndër të tjera dokumenti "*Certifikatë lindje*", e cila i përket fëmijës së punonjësit, në kundërshtim këto me parimin e mjaftueshmërisë sipas germës *"c",* të pikës 1, të nenit 5 të Ligjit.

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

Zyra e Komisionerit vlerëson se, kategoritë e të dhënave të mbledhura/ruajtura, duhet të jenë në përputhje me parimin e mjaftueshmërisë së të dhënave, të cilat duhet të lidhen me qëllimin e përpunimit dhe të mos e tejkalojnë këtë qëllim, si dhe mbajtjen në atë formë që të lejojë identifikimin e subjekteve të të dhënave për një kohë, por jo më tepër se sa është e nevojshme për qëllimin për të cilin ato janë grumbulluar ose përpunuar më tej.

4. Veprimtaria e Kontrolluesit për përpunimin e të dhënave personale realizohet, ndër të tjera, nëpërmjet sistemit elektronik Core banking (Datamax).

   Core Banking (përbëhet nga modulet për menaxhimin e llogarive, klientëve, transaksionet, kreditë, hipotekat, depozitave, investimeve, swift, kontrolli financiar, procesorët e kartave, raportimi, etj.) është infrastruktura kompjuterike ku kryhet përpunimi dhe ruajtja e të gjithë informacionit, mbi të gjithë shërbimet e ofruara në degët dhe filialet e shoqërisë. Mbi këtë infrastrukturë është i ngritur sistemi qendror i shoqërisë për ofrimin e shërbimeve të informatizuara financiare, ku nëpërmjet të cilit ofrohet një numër shumë i madh ndërfaqesh që mundësojnë lidhjen e sistemit qendror të shoqërisë me filialet në të gjithë vendin. Përdoruesit e këtij sistemi janë, klientët, arkëtarët, oficerët e kredive dhe administratorët IT. Ky sistem centralizon dhe automatizon funksionet thelbësore bankare, duke bërë që shërbimet të jenë të aksesueshme në degë, ATM, platforma online dhe aplikacione mobile.

   Sistemi Core banking hostohet në makina virtuale dhe server-a fizik, me komponentë të ndryshëm mbështetës të teknologjisë së informacionit. 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 dhe/ose fizike. Komponentët e infrastrukturës së rrjetit përfshijnë: Firewall, Hardware Servera, Switches, Storage Backup, etj.

   Kontrolluesi disponon gjithashtu aplikacionin Fibank Mobile, i cili operon online për klientët, me qëllim marrjen e shërbimeve nga sistemet elektronike. Çdo përdorues që regjistrohet nëpërmjet këtij aplikacioni, plotëson të dhënat si, emri, mbiemri, adresa e email-it, numri i telefonit, etj. Aplikacioni Fibank Mobile, është një platformë digjitale e cila mundëson që nëpërmjet kompjuterit, smartphone-it ose tablet-it të kryhen veprimet e mëposhtme:

   - Regjistrimi i përdoruesit/klientit;
   - Kryerjen e veprimeve financiare dhe informuese;
   - Ngarkim i gjendjes së llogarisë së klientit;
   - Lidhja me profilin e klientit të shërbimeve të klientit;
   - Kontrolli në kohë reale të gjithë veprimeve financiare;
   - Kontrollin e transfertave të parave në rolin e marrësit ose të dërguesit;

   Nga verifikimi on-site i sistemeve elektronike dhe aplikacionit "Fibank Mobile", si dhe nga shqyrtimi i procedurave rregulluese që disponon Kontrolluesi, konstatohet se:

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

- Nuk ka të specifikuar/dokumentuar kohën maksimale në të cilën shërbimet dhe sistemet nuk mund të jenë funksionale.
- Nuk ka kryer auditim në lidhje me riskun dhe kontrolli e sigurisë së aplikacionit Fibank Mobile në të dy versionet e ofruara, Android dhe IOS.
- Grupi i politikave/procedurave që ka vendosur në dispozicion në lidhje me sigurinë e të dhënave personale gjatë përpunimit të të dhënave nëpërmjet sistemeve elektronike rezulton se, janë hartuar gjatë periudhës nëntor 2024 dhe nuk janë të miratuara nga organet drejtuese të Kontrolluesit.
- Nuk ka marrë masa për të kryer një vlerësim të ndikimit të operacioneve të përpunimit në të dhënat personale.

Për sa më sipër, 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*").

Zyra e Komisionerit vlerëson se, krijimi i procedurave dhe politikave të përdorimit të infrastrukturës TIK dhe sistemeve elektronike ku të specifikohet koha maksimale në të cilën shërbimet dhe sistemet janë funksionale dhe të disponueshëm, është një nga masat kryesore që duhet të ndërmarrë Kontrolluesi, në lidhje me sigurinë dhe funksionimin e sistemeve të teknologjisë së informacionit.

Gjithashtu, Kontrolluesi duhet të kryejë auditime të vazhdueshme të sigurisë së informacionit gjatë përpunimit të tyre nëpërmjet sistemeve elektronike apo aplikacioneve. Gjetjet nga auditimet, duhet të adresohen dhe të analizohen në mënyrë periodike me qëllim parandalimin e çdo cedimi të mundshëm të funksionimit të sistemit dhe integritetit të të dhënave që përpunohen nëpërmjet përdorimit të aplikacioneve në të dy versionet e ofruara, Android dhe IOS.

Zyra e Komisionerit vlerëson se, vlerësimi i ndikimit të proceseve të përpunimit i jep mundësi Kontrolluesit që të analizojë rreziqet dhe masat mbrojtëse me qëllim rritjen e sigurisë së të dhënave personale.

Sa më lart, 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 dhe Udhëzimit nr. 47, të Komisionerit.

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

5. Kontrolluesi nëpërmjet aplikacionit Fibank Mobile ofron shërbimin e regjistrimit dhe të marrjes së shërbimeve "e-banking" për qytetarët. Gjatë procesit të regjistrimit të subjekteve të të dhënave Kontrolluesi përpunon të dhënat, emri, mbiemri, emri i babait, ID personale, email, nr. cel, emri i përdoruesit, fjalëkalimi, etj.,

   Konstatohet se, për të dhëna që përpunon nëpërmjet aplikacionit mobile nuk ka të publikuar "*Politikat e Privatësisë*". Subjektet e të dhënave nuk informohen mbi qëllimin dhe mënyrën e përpunimit të të dhënave personale, personin që do t'i përpunojë të dhënat, 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 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, si 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 disponon një sistem të video-survejimit (CCTV) për mbikëqyrjen e ambienteve të jashtme dhe të brendshme. Nga verifikimi i kryer në vend konstatohet se, Kontrolluesi nuk disponon tabelë informimi për mbikëqyrjen e ambienteve me sistemin CCTV, në kundërshtim me parashikimin e nenit 18 të Ligjit dhe 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, informimi i subjekteve të të dhënave personale mbi prezencën e sistemit të video-survejimit (CCTV) është një nga detyrimet bazë të Kontrolluesit, pasi u jep mundësinë subjekteve të të dhënave personale të njihen me të drejtat që gëzojnë dhe mundësinë e ushtrimit të tyre në praktikë.

7. Kontrolluesi ka lidhur disa kontrata shërbimi me palë të treta ndër to dhe me "Datamaks Sha.", me objekt vënien në dispozicion të "Produktit Programor" për mirëmbajtje teknologjike të sistemeve, si dhe me "Albanian Eagle Security Systems shpk" për mirëmbajtjen e sistemeve të sigurisë së bankës (sistemet e alarmit, akses kontrollit, CCTV).

   Konstatohet se, në përmbajtje të kontratës nuk janë reflektuar detyrimet sipas parashikimeve në nenin 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"*).

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

Zyra e Komisionerit vlerëson se, në rastet e delegimit të përpunimit të të dhënave Kontrolluesi duhet të miratoj një kontratë, që palët duhet të përdorin në rast të këtij delegimi, me anë të së cilës të garantojë përcaktimin e rregullave në marrëdhënien e tij me përpunuesin, me qëllim që delegimi i përpunimit të këtyre të dhënave të jetë në përputhje me nenin 20 të Ligjit dhe me Udhëzimin nr. 19 të Komisionerit.

8. Nga verifikimi i kryer në regjistrin elektronik të subjekteve kontrolluese, si dhe në protokollin e Zyrës së Komisionerit, rezulton se Kontrolluesi ka njoftuar mbi përpunimin e të dhënave personale për të cilat është përgjegjës. Nga analizimi i Formularit, është konstatuar se "*Njoftimi*" ka mangësi në deklarim, sa i përket rubrikave të formularit si vijon:

   - Deklarimin në rubrikën 3.1, të formularit të njoftimit *"Kategoritë e subjekteve të të dhënave personale që përpunohen"* të tilla si *"vizitorë, etj.";*
   - Deklarimi në rubrikën 4.1, të formularit të njoftimit *"Kategoritë e të dhënave personale që përpunohen"* të tilla si "*të dhëna të familjarëve, etj*.*";*

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

   Zyra e Komisionerit vlerëson se realizimi i detyrimit për përditësimin e ndryshimit të 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.

9. Kontrolluesi nuk ka hartuar Rregullore "*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 subjekti të dhënash) sigurinë e të dhënave, afatet e mbajtjes së të dhënave, masat teknike dhe organizative etj., në kundërshtim me nenin 27 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, sigurinë e të dhënave, afatet e mbajtjes së të dhënave, etj., konsiderohet një detyrim shumë i rëndësishëm në zbatim të nenit 27 të Ligjit, për të mundësuar shmangien e pasojave të rënda që mund të vijnë për subjektet e të dhënave.

10. Kontrolluesi vendosi në dispozicion një grup politikash lidhur me sigurinë e informacionit, konkretisht:

    1. Minutes of the ALCO Meeting - 15.10.2024 extract file Archiving;
    2. Extract of MM - SC 18.10.2024 File Archive Regulation;
    3. MM - SC 20.05.2024 extract Code of Ethic;

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

4. Extraordinary ALCO Meeting Protocol - Approval of updated procedures;
5. IT Asset Management Policy;
6. IT Configuration Management Policy;
7. Procedura DM Regjistrim Klienti;
8. Risk Management Policy;
9. File Archiving Regulation;
10. Procedure on blocking and sequestration of costumer accounts;
11. Etj.

Rezulton se, këto politika i përkasin periudhës nëntor 2024, pas marrjes dijeni të urdhrit të hetimit administrativ, dhe nuk janë të miratuara nga organet drejtuese të Kontrolluesit. Megjithatë, nga analizimi i tyre konstatohet se mungojnë dhe elementë të tjerë të sigurisë së të dhënave si, "*Analizën e Ndikimit në të Dhënat Personale*", "*Raport vlerësimi mbi sigurinë në sistemin e arkivimit*", "*Hapat që duhet të ndërmerren në rast incidentesh të shkeljes së sigurisë së të dhënave personale*", etj., në kundërshtim me parashikimet e nenit 27 të Ligjit dhe Udhëzimit nr. 47 të Komisionerit.

Kontrolluesi nuk ka kryer trajnime konkrete të punonjësve që kanë akses dhe përpunojnë të dhëna personale lidhur me legjislacionin në fuqi për mbrojtjen e të dhënave personale, sipas parashikimeve të nenit 27 të Ligjit dhe sipas përcaktimeve në Kapitullin IV, të Udhëzimit nr. 47 të Komisionerit.

Gjithashtu, konstatohet mosplotësimi i detyrimeve në lidhje me ngritjen, administrimin dhe mirëmbajtjen e Sistemit të Menaxhimit të Sigurisë së Informacionit (SMSI), lidhur me mbrojtjen e të dhënave personale, sipas parashikimeve të Udhëzimit 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, sipas parashikimeve të Kreut IV të Udhëzimit nr. 47, 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. Ky është një detyrim i vazhdueshëm i Kontrolluesit që personeli i subjektit përpunues të të dhënave personale të trajnohet rregullisht për mbrojtjen e të dhënave personale.

Gjithashtu, 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,

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

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 dërguar Kontrolluesit me rrugë postare nëpërmjet shkresës nr. 2373/2 prot., datë 24.12.2024.

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.

Përfaqësuesit e Kontrolluesit, janë paraqitur në seancën dëgjimore datë 15.01.2025, dhe kanë parashtruar pretendimet me shkrim si dhe dokumentacion plotësues (CD) mbi konstatimet e procesverbalit të hetimit administrativ, duke bashkëlidhur dokumentacion si:

- Vlerësimi i Sigurisë së Informacionit 23.10.2024
- Evidence External Web Application Penetration Testing Report 08.04.2024
- Evidence External Penetration Test Report 25.03.2021
- SWIFT Audit report 2024
- SWIFT Audit Report 2023
- Extraordinary ALCO Meeting Protocol - Approval of Operational Procedures
- AKSK Audit RAPORT 2023
- AKSK Audit RAPORT 2024
- Digital Banking AGREEMENT Company final;
- Digital Banking AGREEMENT Individuals final;
- Imazhi për qaje ne llogari nga ana e klientit;
- Evidencat lidhur me tabelat informuese për CCTV.

- Lidhur me pikën 2 të konstatimeve Kontrolluesi pretendon se *"...afati i ruajtjes së dokumentacionit në dosjen e punonjësit zbatohet në respektim të afatit 6 muaj sipas Kodit të Punës, si rrjedhojë e çdo pretendimi të mundshëm që mund të ketë punëmarrësi nga punëdhënësi".*

  Zyra e Komisionerit vlerëson se, lidhur me të dhënat personale të grumbulluara, Kontrolluesi duhet të parashikojë ruajtjen e të dhënave personale në atë formë, që lejon identifikimin për një kohë të caktuar, por jo më tepër se sa është e nevojshme për të përmbushur qëllimin e grumbullimit. Koha e ruajtjes së të dhënave personale duhet të përcaktohet nga Kontrolluesi, në përputhje me parashikimet ligjore specifike dhe qëllimin e grumbullimit të informacionit.

- Lidhur me pikën 3 të konstatimeve Kontrolluesi pretendon se *"...në lidhje me informacionin e mbledhur për familjarët e punonjësve, Kontrolluesi shprehet se ndihmon në vlerësimin e rreziqeve të mundshme të brendshme, siç janë lidhjet me individë që mund të jenë të përfshirë në aktivitete të paligjshme ose që mund të jenë të lidhur me aktivitete që bien ndesh me interesat e Bankës. Gjithashtu, bën me dije se në dosjen e punonjësit*

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

administrohet ndër të tjera dokumenti "Certifikatë lindje", e cila i përket fëmijës së punonjësit për verifikimin e moshës për përfitimin e bonuseve dhe dhuratave për fëmijët deri në 12 vjeç".

Zyra e Komisionerit vlerëson se, kategoritë e të dhënave të mbledhura/ruajtura, duhet të jenë në përputhje me parimin e mjaftueshmërisë së të dhënave, të cilat duhet të lidhen me qëllimin e përpunimit dhe të mos e tejkalojnë këtë qëllim, si dhe mbajtjen në atë formë që të lejojë identifikimin e subjekteve të të dhënave për një kohë, por jo më tepër se sa është e nevojshme për qëllimin për të cilin ato janë grumbulluar ose përpunuar më tej.

- Lidhur me pikën 5 të konstatimeve Kontrolluesi shprehet se *"...sa i takon aplikacionit Fibank Mobile, regjistrimi i klientit nuk kryhet online, por është vetëm hapi i parë i regjistrimit që kryhet online me qëllim gjenerimin e username dhe password por pa mundësuar akses në aplikacionin Fibank Mobile. Këto të dhëna konsistojnë në të dhëna si emër, mbiemër, atësi, Id, etj., të cilat nuk përpunohen nga banka pasi konsiderohen nga burime të pakonfirmuara deri në hapin e dytë, prandaj nuk është i nevojshëm publikimi i Politikave të Privatësisë*".

  Zyra e Komisionerit vlerëson se, për sa kohë që subjekti i të dhënave plotëson online rubrika të tipit "*contact-form*" me të dhënat e tij personale edhe pse për të aksesuar aplikacionin si hap i dytë duhet të paraqitet pranë bankës, informimi është i rëndësishëm si një nga detyrimet bazë të Kontrolluesit, pasi u jep mundësinë subjekteve të të dhënave personale të njihen me të drejtat që gëzojnë, si 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.

- Lidhur me pikën 10 të konstatimeve Kontrolluesi shprehet se *"...banka kryen trajnime për çdo punonjës të ri nga Departamenti i Sigurisë së Informacionit dhe Departamenti i Përputhshmërisë, materiale të cilat lidhen me informacionin që përpunohet dhe detyrimet që lindin nga ligji për mbrojtjen e të dhënave personale. Gjithashtu, dokumentet e vendosura në dispozicion "It security file Komisioneri" janë derivat i politikave të miratuara në maj 2024 konkretisht IT Asset Management Policy, It Configuration Menagement Policy, Risk Menagement Policy*".

  Lidhur me këtë pretendim, Zyra e Komisionerit vlerëson se Kontrolluesi nuk ka vendosur në dispozicion evidenca/procesverbale ku të vërtetohen se janë kryer trajnime të punonjësve. 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.

  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.

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

PËR KËTO ARSYE:

Në zbatim të neneve 5, 18, 20, 21, 22, 27, 29, 30, 31 (pika 1, germa "a/1"), si dhe 32 të Ligjit,

REKOMANDOJ:

1. Kontrolluesi, të marrë masa për përcaktimin e afateve kohore për ruajtjen e të dhënave personale, në përputhje me germën "*d*", të pikës 1, të nenit 5 të Ligjit;

2. Kontrolluesi, në zbatim të nenit 5 të Ligjit, të marrë masa që mbledhja e të dhënave personale nga ana e tij, të kryhet në mënyre të ligjshme, informacioni të grumbullohet vetëm për qëllime specifike, të përcaktuara qartë, e legjitime dhe përpunimi i të dhënave të kryhet në përputhje me këto qëllime, duke ju përmbajtur gjithashtu parimit të mjaftueshmërisë së të dhënave, të cilat duhet të lidhen me qëllimin e përpunimit dhe të mos e tejkalojnë ketë qëllim;

3. Kontrolluesi, të marrë masa për zbatimin e detyrimeve, në lidhje me informimin e plotë të subjekteve të të dhënave, sipas parashikimeve të nenit 18 të Ligjit;

4. Kontrolluesi, të marrë masa për të rishikuar kontratën me përpunuesin duke specifikuar detyrimet midis palëve, sipas dispozitave të parashikuara në nenin 20 të Ligjit dhe Udhëzimin nr. 19;

5. Kontrolluesi, në zbatim të nenit 27 të Ligjit, të hartojë Rregullore *"Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale"*, duke parashikuar 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, etj.;

6. Kontrolluesi, me qëllim garantimin e sigurisë së të dhënave personale duhet të zbatojë detyrimet e përcaktuara në Udhëzimin nr. 47, lidhur me trajnimin e punonjësve që kanë akses dhe përpunojnë të dhëna personale si dhe krijimin, mirëmbajtjen dhe administrimin e Sistemit të Menaxhimit të Sigurisë së Informacionit (SMSI) për mbrojtjen e të dhënave personale;

7. Kontrolluesi, për shkak të natyrës së veçantë të aktivitetit që ushtron, duhet të marrë masat e nevojshme për të vlerësuar mbi certifikimin e sistemeve të menaxhimit të sigurisë së informacionit, të të dhënave personale dhe mbrojtjes së tyre, sipas parashikimeve të Udhëzimit nr. 48;

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

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

(i) brenda 15 (pesëmbëdhjetë) ditëve, detyrimet e treguara në pikat 1, 2 dhe 3 më sipër;
(ii) brenda 30 (tridhjetë) ditëve, detyrimet e treguara në pikat 4 dhe 5 më sipër;
(iii) brenda 45 (dyzetë e pesë) ditëve, detyrimet e përcaktuara në pikën 6 më sipër.

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

9. Kontrolluesi të njoftojë Zyrën e Komisionerit për masat e marra;

10. Në rast mos përmbushje të detyrimeve të parashikuara në këtë akt, Komisioneri vepron sipas pikës 2 të nenit 30 dhe nenit 39 të ligjit, të cilët parashikojnë se në rast shkeljesh serioze, të përsëritura ose të qëllimshme të Ligjit nga një kontrollues ose përpunues, veçanërisht në rastet e përsëritura të moszbatimit të rekomandimeve të tij, Komisioneri vendos sanksione administrative për kundërvajtjet administrative përkatëse dhe e denoncon publikisht ose e raporton çështjen në Kuvend dhe në Këshillin e Ministrave.

Ky Rekomandim u shpall sot më 31.01.2025.

KOMISIONERI

Besnik Dervishi

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