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.697/6 prot. Tiranë më 08.11.2022

REKOMANDIM

Nr. 34, datë 08.11.2022

PËR KONTROLLUESIN *"AUTORITETI I MBIKËQYRJES FINANCIARE"*

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*"), si dhe provave të administruara në ngarkim të kontrolluesit *"Autoriteti i Mbikëqyrjes Financiare"* (në vijim, *"Kontrolluesi"* dhe/ose *"AMF"*),

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 55, datë 01.04.2022 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim, *"Komisioneri"*), u krye hetimi administrativ pranë Kontrolluesit, me objekt:

- *Verifikimi i procesit të përpunimit të të dhënave personale në kuadër të aksesit që ka Kontrolluesi në të gjitha databazat shtetërore veçanërisht në regjistrin e gjendjes civile dhe zbatimi i detyrimeve ligjore në fushën e mbrojtjes së të dhënave personale.*
- *Verifikimi i zbatimit të Rekomandimit nr. 03, datë 07.02.2019 të Komisionerit.*

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 institucion publik i pavarur, përgjegjës për rregullimin dhe mbikëqyrjen e sistemit financiar jo bankar dhe operatorëve që ushtrojnë aktivitetin e tyre në këtë sektor. Fusha kryesore e veprimtarisë së Autoritetit është rregullimi dhe mbikëqyrja e tregut të sigurimeve dhe operatorëve të tij, e tregut të titujve dhe

operatorëve të tij, e tregut të pensioneve private vullnetare dhe operatorëve të tij, si dhe veprimtari të tjera financiare jo bankare.

Kontrolluesi, në zbatim të ligjit nr. 9572, datë 03.07.2006 *"Për Autoritetin e Mbikëqyrjes Financiare"*, mbledh dhe përpunon kategoritë e të dhënave personale, ndër të tjera: *"emër", "mbiemër", "datëlindje", "situata ekonomike e financiare", "numri i sigurimit shoqëror", "jeta profesionale", "adresa", "të dhënat e identifikimit", "formimi-diplomat-medaljet", "gjendja penale", "shëndeti",* etj., për kategoritë e subjekteve *"punonjës", "persona që kërkojnë të pajisen me licence", "agjentë", "brokera", "aktuarë", "vlerësues dëmesh", "anëtar për mbikëqyrjen", "aksionarë", "vizitorë të faqes së internetit www.amf.gov.al", "qytetarë",* etj.

2. Kontrolluesi administron regjistra elektronike për përpunimin e të dhëna personale nëpërmjet Qendrës së Informacionit të Sigurimeve të Detyrueshme, konkretisht:

    - Regjistri Elektronik Online i Shitjeve;
    - Regjistri Elektronik i Dëmeve.

    Regjistri Elektronik Online i Shitjeve (në vijim, *"REOSH"*) mbledh/përmban të dhënat që raportohen nga personat e licensuar/autorizuar për shitje (shoqëritë e sigurimit, agjentë/shoqëritë e agjentëve) të çdo polica sigurimi në kohë reale. Për identifikimin dhe raportimin e shitjeve të policave të sigurimit të detyrueshëm, emetohet një numër unik i rastësishëm në kohë reale, për të identifikuar çdo policë sigurimi që kërkohet të shitet online nga shoqëritë e sigurimit të jo-jetës.

    REOSH përfaqëson një platformë raportimi dhe identifikimi të shitjeve të policave të sigurimit të detyrueshëm motorik, në formën e përgjegjësisë ndaj palëve të treta (TPL e Brendshme), kartonit jeshil, polica kufitare (mjetet motorrike të huaja), sigurimi i përgjegjësisë së pasagjerëve dhe sigurimi i minatorëve. REOSH mundëson raportim të shitjeve të sigurimeve të detyrueshme, mbikëqyrje të tregut si dhe mbrojtje për konsumatorin. Të gjitha policat e shitura nga shoqëritë e sigurimit identifikohen në kohe reale përmes një numri unik raportimi dhe të dhënat e polica-ve të identifikuara përmes këtij numri, vendosen në regjistër.

    Sistemi i REOSH është i ngritur mbi:
    - Sistemin e Operimit Windows Server 2003 32-bit/Windows Server 2008;
    - Databaza: Oracle 32-bit; WebServer: Oracle SOA (8 instanca);
    - Proxy (CentOS) për load balance;
    - Serverat fizik ndodhen në ambientin e AMF.

    Palët e interesuara mund të verifikojnë policat e sigurimit aktiv online në faqen, https://amf.gov.al/mtpl.asp, duke plotësuar dy nga tre kushtet e detyrueshme të cilat janë:
    - Targa e Mjetit;
    - Numri Serial i policës së sigurimit;

- Numri i Shasisë.

REOSH, sipas nenit 34, të ligjit nr. 32/2021 *"Për Sigurimin e Detyrueshëm në Sektorin e Transportit"* (në vijim, *"Ligji 32/2021"*), ndërvepron me anë të platformës qeveritare të ndërveprimit Government Gateway (GG), nga ku merren të dhënat dytësore me institucionet e mëposhtme:

1) Drejtoria e Përgjithshme e Gjendjes Civile - Regjistri Kombëtar i Gjendjes Civile;
2) Drejtoria e Përgjithshme e Shërbimeve të Transportit Rrugor - Regjistri Kombëtar i Mjeteve;
3) Qendra Kombëtare e Biznesit - Regjistri Tregtar - Regjistri Kombëtar i Licencave.

Sistemi REOSH ndërvepron gjithashtu me sistemet elektronike të kompanive të sigurimit që janë: Edusoft, Sigal dhe sistemin Vigsoris. Nëpërmjet këtyre sistemeve të integruara nëpërmjet webservice me bazën e të dhënave REOSH, agjentët e kompanive të sigurimeve popullojnë me të dhëna këtë regjistër.

Gjithashtu, në zbatim të Ligjit nr. 32/2021, ligjit nr. 8378, datë 22.07.1998 *"Kodi Rrugor i Republikës së Shqipërisë"* i ndryshuar, dhe ligjit nr. 108/2014 *"Për Policinë e Shtetit"*, me qëllim bashkëpunimin dhe bashkërendimin e veprimtarisë, shkëmbimin e informacionit dhe kontrollin, AMF, me anë të platformës qeveritare të ndërveprimit (GG), i ofron mundësinë Drejtorisë së Policisë së Shtetit të verifikojë të dhënat e policës së sigurimit, një kërkesë – një përgjigje, të rregulluar sipas Marrëveshjes së Bashkëpunimit përkatëse.

Në Regjistrin Elektronik të Dëmeve (në vijim, *"RED"*), raportohen të dhënat për dëmet e ndodhura nga Shoqëritë e Sigurimit dhe Byroja Shqiptare e Sigurimit.

RED është i ngritur mbi:

- Sistemin e Operimit Windows Server 2008 64-bit. Ubuntu/Linux, për certifikatën e sigurisë;
- Databaza: Oracle 32-bit; WebServer: Tomcat;
- Serverët fizik ndodhen në ambientin e AMF.

Për raportimin elektronik të të dhënave, të dëmeve të sigurimeve të detyrueshme motorike, të verifikimit të historikut të dëmeve të mjetit dhe statusin e dosjes së dëmit, palët e interesuara, ndër të tjera, mund të marrin informacion online në faqen zyrtare https://amf.gov.al/vmws.asp, vetëm nëse plotësohen parametrat e mëposhtëm:

- Numrin e Shasisë - Verifikon Historikun e Dëmeve të Mjetit;
- Kodi i dëmit - Verifikon Statusin e Dosjes së Dëmit.

RED, ndërvepron nëpërmjet webservice-ve me tre sisteme të kompanive të sigurimit që janë: Edusoft, Sigal dhe sistemi Vigsoris. RED ndërvepron gjithashtu edhe me sistemin REOSH, për të verifikuar të dhënat mbi automjetet dhe përdoruesin (për

marrjen e të dhënave të policës së sigurimit për palët e përfshira në aksident). Gjithashtu, Kontrolluesi ka krijuar mundësinë që shoqëritë e sigurimit të aksesojnë regjistrin RED edhe nëpërmjet llogarive/account specifike, në rastet kur rrjeti ka probleme gjatë ndërveprimit të sistemeve respektive nëpërmjet webservice-ve. Përdorues i veçantë është krijuar në këtë sistem edhe për Byronë Shqiptare të Sigurimeve, për qëllim të raportimit të dëmeve të ndodhura.

REOSH ka një ndërfaqe grafike monitorimi të kufizuar në administrimin e të dhënave apo përdorueseve/roleve, etj., duke rritur riskun gjatë përdorimit të tij. Ndërfaqja ndihmon në analizimin e proceseve të punës të sistemit, dhe verifikimin e funksionaliteteve të këtij sistemi. Politikat mbi gjurmët (log-et) në sistemin elektronik dhe infrastrukturën TIK mbështetëse të regjistrave, nuk zbatohen sipas një procedure të rregulluar, me risk në qasje të paautorizuar në të dhënat, kërcënim të sigurisë në fushën e teknologjisë së informacionit dhe mungesë transparence për verifikim. Si rrjedhojë, specialistët IT kanë akses jo të plotë, për të bërë kërkime në mënyrë të shpejtë si: tentativat e dështuara për log-in, numrin e *"login"* nga një PC, etj. REOSH mundëson raportimin e shitjeve të polica-ve sipas skemës Agjent-Ndërmjetës-AMF. Kjo skemë veprimi lejon një sistem tjetër të ndërmjetëm për komunikimin e informacionit, si rrjedhojë sigurimi dhe integriteti i informacionit është me risk të shtuar.

Kontrolluesi ka krijuar infrastrukturë me kapacitete teknike jo të plota për të ruajtur log-et e sistemeve elektronike me qëllim të gjurmueshmërisë së veprimeve të personave që kanë akses si dhe funksioneve të tjera të sistemit, për një afat kohor të përshtatshëm.

Zyra e Komisionerit vlerëson se, ekzistenca e një ndërfaqe monitorimi, ndihmon në analizimin e proceseve të punës të sistemit si dhe në verifikimin e funksionaliteteve të sistemit. Gjithashtu, zbatimi i politikave dhe procedurave të rregulluara minimizon risqet në qasje të paautorizuar në të dhënat, kërcënim të sigurisë në fushën e teknologjisë së informacionit dhe mungesë transparence për verifikim. Krijimi i kapaciteteve të plota për ruajtjen e logeve të sistemeve elektronike, ndihmon çdo kontrollues të gjurmojë veprime të përdoruesve si dhe funksionalitet e sistemit.

Konstatohet se shërbimin e mirëmbajtjes dhe të sigurisë së sistemeve, Kontrolluesi e kryen nëpërmjet punonjësve të drejtorisë TIK.

Kontrolluesi, edhe pse ka të miratuar me Vendim nr. 192 të Bordit, datë 14.10.2019, *"Politika të brendshme të sigurisë së informacionit në AMF",* konstatohet se, Kontrolluesi nuk disponon një plan vazhdimësie të mirë përcaktuar për BCP (Business Continuity Plan) dhe plan rikuperimi DRP (Disaster Recovery Plan) për garantimin e vazhdimësisë së ofrimit të shërbimit.

Gjithashtu, konstatohet se masat e ndërmarra në drejtim të proceseve të Backup-it janë të pamjaftueshme dhe nuk japin siguri në mbështetjen e BCP (Business

Continuity Planning) dhe DRP (Disaster Recovery Plan), në kundërshtim me aktet ligjore apo nënligjorë në fuqi. U konstatua se procedurat e *"backup"* për sistemet elektronike si dhe administrimi i këtyre sistemeve, nuk kryhet në përputhje me VKM nr. 945, datë 02.11.2012, Për Miratimin e Rregullores *"Administrimi i Sistemit të Bazave të të Dhënave Shtetërore" (*në vijim, "*VKM nr. 945*"*),* dhe VKM nr. 710, datë 21.08.2013 *"Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit" (*në vijim *"VKM nr. 710"),* të cilat kanë për qëllim përcaktimin e procedurave standarde të politikave të administrimit dhe funksionimit të sistemeve. Nuk u gjetën procedura të testimit të backup. Kopjet (backup) e të dhënave nuk testohen rregullisht për t'u siguruar që mund të përdoren në raste të nevojshme. Procedurat e rikrijimit (restore) të të dhënave nuk testohen për t'u siguruar që ato janë të efektshme dhe që ato mund të ekzekutohen brenda kohës së lejuar.

Sa i përket pamjaftueshmërisë së masave të ndërmarra në drejtim të proceseve të Backup-it, të cilat japin pasiguri në mbështetjen e BCP (Business Continuity Planning) dhe DRP (Disaster Recovery Plan), Zyra e Komisionerit vlerëson se, këto masa duhet të zbatohen në përputhje me VKM nr. 945, VKM nr. 710, etj., të cilat kanë për qëllim përcaktimin e procedurave standarde të politikave të administrimit dhe funksionimit të sistemeve.

Konstatohet se Backup-et e të dhënave të sistemeve elektronike apo edhe faqes web, kryhen nga vetë stafi i AMF. Gjithashtu, rezulton se nuk ka përgjegjësi individuale për mbarëvajtjen e proceseve të punës si: administrim i të dhënave të dy sistemeve, administrim i faqes web, kontroll të loge-ve të sistemeve, etj.

Sa më sipër, Zyra e Komisionerit vlerëson se, kjo situatë përbën një risk të shtuar 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. Administrimi i këtyre atributeve pa autorizim, nuk jep siguri për kryerjen e detyrave konform dispozitave ligjore si dhe praktikave më të mira.

Kontrolluesi nuk ka mirë përcaktuar personat përgjegjës për të siguruar vazhdimësinë e ofrimit të shërbimit, si dhe nuk janë identifikuar dhe ndarë sipas rëndësisë të dhënat kritike, sistemet, operacionet dhe burimet. Konstatohet që punonjësit kryejnë veprime teknike manuale të pa dokumentuara dhe të paautorizuara në drejtim të ruajtjes së të dhënave në raport më këtë politikë.

Referuar ligjit nr. 10 325, datë 23.09.2010 *"Për bazat e të dhënave shtetërore"* (në vijim, *"ligji 10 325/2010")* dhe VKM nr. 945, AMF ka nisur procesin e regjistrimit të bazës së të dhënave për regjistrin Elektronik online të Shitjeve REOSH (ose siç njihet ndryshe *"Regjistri Elektronik Online i Sigurimit të detyrueshëm Motorik"* me nr. identifikues *"PJP-01-0054")* si bazë të dhënash shtetërore në Autoritetin Rregullator Kombëtar (ARK), por rezulton se ky proces nuk ka përfunduar. Ndërsa

për Regjistrin e sistemit Elektronik të Dëmeve rezulton se nuk është regjistruar si bazë të dhënash shtetërore në ARK.

Zyra e Komisionerit vlerëson se regjistrimi i bazës së të dhënave, është i nevojshëm për standardizimin dhe sigurimin e saj në rast të ndërveprimit të saj nëpërmjet Government Getaway, në kuptim të ligjit nr. 10 325/2010.

AMF nuk ka një strategji të plotë për Teknologjinë e Informacionit dhe Komunikimit (TIK), ku të evidentohen nevojat aktuale dhe të merren në konsideratë ato për vijimësinë e punës së institucionit. Konkretisht, mbi nevojat e kapaciteteve TIK për ofrimin e shërbimeve, duke marrë në konsideratë infrastrukturën TIK aktuale, investimet në infrastrukturë TIK, modelin e ofrimit të shërbimit, burimet e ndryshme, stafin e nevojshëm, si dhe paraqitjen e strategjisë që integron këto elementë në një qasje të përbashkët, me qëllim mirëfunksionimin e veprimtarisë së institucionit në ofrimin e shërbimeve.

Zyra e Komisionerit vlerëson se AMF duhet ti kushtojë një rëndësi të veçantë planifikimit strategjik të teknologjisë së informacionit, duke pasur në konsideratë rëndësinë e të dhënave që institucioni posedon dhe përpunon.

Kontrolluesi nuk disponon Marrëveshje në Nivel Shërbimi (MNSH/SLA) për këto sisteme dhe infrastrukturën mbështetëse të tyre, në kundërshtim me pikën 2, të VKM nr. 710, i ndryshuar, ku citohet: *"Çdo institucion, i cili ka ose do të zhvillojë një sistem në fushën e teknologjisë së informacionit, që ofron shërbime për qytetarët, për biznesin dhe për ndërveprim e shkëmbim informacioni për administratën publike nëpërmjet sistemeve elektronike, duhet të parashikojë dhe të hartojë marrëveshje kontraktuale mbi nivelin e shërbimit (Service Level Agreement - SLA)".* Aktualisht, mirëmbajtja e sistemeve dhe infrastrukturës mbështetëse TIK, kryhet nga vetë personeli në raste kur ndodhin probleme të ndryshme.

Zyra e Komisionerit vlerëson se, mungesa e marrëveshjeve kontraktuale mbi nivelin e shërbimit (Service Level Agreement - SLA), në lidhje me sistemet elektronike nëpërmjet të cilave, ndër të tjera, mbledh, ruan, arkivon, ofron shërbime për qytetarët, biznesin dhe të ngjashme, ekspozon Kontrolluesin në risk të mundshëm sa i përket integritetit dhe disponueshmërisë së sistemeve dhe vetë të dhënave të përpunuara në to.

Kontrolluesi, edhe pse ka hartuar rregulla mbi menaxhimin e incidenteve dhe problemeve, rezulton se ato nuk dokumentohen sipas një plani masash për trajtimin e problemeve dhe incidenteve. Kontrolluesi nuk disponon raporte të administrimit të incidenteve dhe problemeve, me qëllim gjetjen e zgjidhjeve për ti trajtuar ato dhe për të parandaluar ndodhjen e incidenteve në të ardhmen, në mënyrë që shërbimet elektronike të institucionit të mos kompromentohen.

Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI) dhe AMF, kanë lidhur Marrëveshjen e nivelit të shërbimit SLA (me nr. 1139 prot., datë 26.03.2018), për ofrimin e mirëmbajtjes dhe hostimit të infrastrukturës TIK që disponon AMF. Këto shërbime konsistojnë në mirëmbajtjen dhe hostimin e DRP për sistemet, mail server, etj. Megjithëse është lidhur një Marrëveshje midis tyre, konstatohet se zbatueshmëria e saj nuk dokumentohet nëpërmjet raporteve periodike dhe të vazhdueshme, gjë që përbën risk për mbarëvajtjen, monitorimin dhe dokumentimin e shërbimeve TIK në AMF.

Sa i përket gjithë konstatimeve të reflektuara në përmbajtje të kësaj pike, Zyra e Komisionerit vlerëson se, Kontrolluesi nuk ka marrë masa tekniko-organizative të përshtatshme për krijimin e kushteve të nevojshme për të garantuar mbrojtjen e të dhënave personale të qytetarëve, në përputhje me parashikimet e neneve 27 dhe 28 të Ligjit si dhe dispozitave të akteve nënligjore të Komisionerit.

Kontrolluesi ka të parashikuar në pikën 5, të nenit 31, të ligjit 32/2021, periudhën kohore të të dhënave që përpunon, konkretisht: *"... Periudha kohore që duhet të ruhen të dhënat e përmendura në këtë nen është minimalisht 7 (shtatë) vjet nga data e përfundimit të çregjistrimit të mjetit motorik ose pas përfundimit të vlefshmërisë së policës të sigurimit..."* por, rezulton se të gjitha të dhënat e mbledhura nga Kontrolluesi, përpunohen/ruhen që nga koha e krijimit të *çdo praktike dëmi* të hapur, pa përcaktuar një afat maksimal të ruajtjes së tyre dhe pa marrë masa për shkatërrimin e tyre, në funksion të detyrimeve që rrjedhin nga dispozitat e Ligjit.

Zyra e Komisionerit vlerëson se, mbrojtja e të dhënave personale duhet të bazohet, ndër të tjera, në mbajtjen 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, në përputhje me parimin e mbrojtjes së të dhënave personale parashikuar në germën *"d"* , të pikës 1, të nenit 5 të Ligjit.

3. Kontrolluesi ofron mundësinë e aksesit/ndërveprimit të të dhënave në regjistrat elektronik REOSH dhe RED, sipas formave të mëposhtme:

   a. Aksesi në sistemin REOSH nëpërmjet webservice-ve për Policinë e Shtetit, referuar:
      i. Marrëveshjes së bashkëpunimit dhe shkëmbimit të informacionit për sigurimin e detyrueshëm në sektorin e transportit midis AMF-së, Ministrisë së Brendshme dhe Ministrisë së Punëve Publike dhe Transportit (Ministria e Infrastrukturës dhe Energjisë) datë 31.03.2011;
      ii. Urdhër i përbashkët *"Për zbatimin e marrëveshjes së bashkëpunimit dhe shkëmbimit të informacionit midis AMF dhe DPPSH-së"* me nr. 1575 prot., datë 19.09.2011.

b. Akses në sistemin REOSH nëpërmjet webservice-ve për sistemet e shoqërive të sigurimeve: Sigal, Sigma, Insig, Atlantik, Intersig, Eurosig, Albsig, Ansig dhe Sivig.

c. Akses të drejtpërdrejtë në sistemin REOSH kanë:
   i. punonjësit administrativ të AMF;
   ii. llogari/përdorues për agjentet e shoqërive të sigurimeve.

d. Akses të drejtpërdrejtë në sistemin RED kanë:
   i. punonjësit administrativ të AMF;
   ii. një përdorues/user për Byronë Shqiptare e Sigurimit; si dhe,
   iii. llogari/përdorues të drejtpërdrejtë për këto shoqëri të sigurimeve.

e. Aksen për ofrimin e shërbimeve të verifikimit të policës së sigurimit motorik, vërtetimit të historikut të mjetit dhe vërtetimit të historikut të dëmit nëpërmjet platformës *"e-Albania"*.

AMF, nëpërmjet ndërveprimit me platformën *"e-Albania"*, ofron shërbime online në lidhje me:

a. Verifikimin e policës M-TPL për mjetet motorike me të dhënat e marra nga Regjistri Elektronik Online i Shitjeve;
b. Historikun e polica-ve M-TPL të mjeteve motorike me të dhënat e marra nga Regjistri Elektronik Online i Shitjeve;
c. Historikun e dëmeve të mjeteve motorike me të dhënat e marra nga Regjistri Elektronik i Dëmeve;
d. Njoftimin e qytetarëve për përfundimin e policës së sigurimit MTPL në seksionin *"Mesazhet e mia"* në portalin *"e-Albania"*.

Referuar pikës 2, të nenit 34, të ligjit nr. 32/2021 *"...Qendra e Informacionit ndërvepron me anë të platformës qeveritare të ndërveprimit (GG), nga ku do merren të dhënat dytësore me institucionet..."*, AMF legjitimohet të ndërveprojë me GG, vetëm për të marrë të dhëna dytësore në kuptim të ligjit nr. 10 325/2010.

Ndërsa, sa i përket ndërveprimit në portalin *"e-Albania"*, me qëllim ekspozimin e të dhënave parësore të sistemeve REOSH dhe RED në këtë portal, rezulton që Kontrolluesi nuk e ka të parashikuar në një dispozitë ligjore konkrete, këtë lloj ndërveprimi.

Zyra e Komisionerit vlerëson se, ekspozimi i të dhënave parësore të sistemeve REOSH dhe RED në portalin *"e-Albania"*, pa pasur një dispozitë ligjore konkrete për legjitimimin e këtij ndërveprimi, është në kundërshtim me kriteret ligjore të përpunimit, të parashikuara në nenin 6 të Ligjit.

4. Nga verifikimi i kryer në regjistrin elektronik të subjekteve kontrolluese, 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 3, të formularit të njoftimit *"kategoritë e subjekteve të të dhënave personale që përpunohen";*
   ii. Deklarimin në rubrikën 4, të formularit të njoftimit *"kategoritë e të dhënave personale që përpunohen"*;
   iii. Deklarimin në rubrikën 6, të formularit të njoftimit "*qëllimi i përpunimit"*;
   iv. Deklarimin në rubrikën 7, të formularit të njoftimit "*marrësit e të dhënave personale"*;

   Zyra e Komisionerit vlerëson, se konstatimet e mësipërme janë në kundërshtim me parashikimet e neneve 21 dhe 22 të Ligjit.

   Zyra e Komisionerit vlerëson se përmbushja e detyrimit për ndryshimin e gjendjes së "*Njoftimit*" për përpunimin e të dhënave për të cilat Kontrolluesi është përgjegjës, sipas parashikimeve të nenit 21 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.

5. Kontrolluesi disponon rregullore *"Për mbrojtjen e të dhënave personale",* por konstatohet se ajo nuk parashikon proceset, procedurat, masat teknike dhe organizative, etj., sipas parashikimeve të nenit 27 të Ligjit, me qëllim garantimin e përpunimit të ligjshëm dhe sigurisë së të dhënave, në përputhje me proceset përpunuese.

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

   Gjithashtu, 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. Rezulton mosplotësim i detyrimeve në lidhje me ngritjen, administrimin dhe mirëmbajtjen e Sistemit të Menaxhimit së Sigurisë së Informacionit (SMSI) për sa i takon mbrojtjes së të dhënave personale, të parashikuar në Udhëzimin 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 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. Zyra e Komisionerit vlerëson se trajnimet duhet të kryhen me qëllim ndërgjegjësimin e operatorëve të cilët për shkak të proceseve të punës, janë të ngarkuar për përpunimin e të dhënave personale.

Zyra e Komisionerit vlerëson se, për shkak të cilësisë si subjekt i madh përpunues, 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 ngrihet sipas standardit ndërkombëtar 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, "*Udhëzimi nr. 48*"), si dhe duhet të jetë një sistem i certifikueshëm, për qëllime përputhshmërie me standardin e sipërpërmendur, vetëm nga organizma të akreditуar dhe autorizuar sipas parashikimeve të Udhëzimit nr. 48 të Komisionerit.

6. Lidhur me pikën e dytë të objektit të hetimit administrativ: *"Verifikimi i zbatimit të Rekomandimit nr. 03, datë 07.02.2019 të Komisionerit",* rezulton se Kontrolluesi ka marrë masa për përmbushjen e Rekomandimeve dhe me shkresën nr. 339/1 prot., datë 07.02.2019, ka informuar e Zyrën e 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 me rrugë postare nëpërmjet shkresës nr. 697/3 prot., datë 12.09.2022.

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 paraqitën në seancë dëgjimore parashtrimet me shkrim, në lidhje me konstatimet e procesverbalit të hetimit administrativ, nëpërmjet të cilave argumentohet si vijon:

1. Në lidhje me konstatimin sa i përket mos parashikimit të një afati konkret për ruajtjen e të dhënave personale, në sistemin elektronik Regjistri Elektronik i Dëmeve (RED), AMF pretendon se:

   Qendra e informacionit në AMF është krijuar me Ligjin nr. 10 076, datë 12.2.2009 *"Për sigurimin e detyrueshëm në sektorin e transportit"* (sot në fuqi Ligji nr. 32/2021 *"Për sigurimin e detyrueshëm në sektorin e transportit"*). Sipas bazës ligjore në fuqi,

Regjistri Elektronik i Dëmeve mbledh dhe ruan nga shoqëritë e sigurimeve të dhëna për dëmet për të gjitha llojet e sigurimit të detyrueshëm, të përditësuara. Qendra e informacionit furnizohet me të dhëna nga shoqëritë e Sigurimit. Referuar nenit 32 të Ligjit *"Për sigurimin e detyrueshëm në sektorin e transportit"*, Qendra e Informacionit duhet t'ua mundësojë dhënien dhe përdorimin e të dhënave të grumbulluara sipas këtij ligji, të gjitha palëve të dëmtuara dhe pjesëmarrësve në një aksident rrugor për një periudhë 7-vjeçare pas aksidentit.

Sa më sipër, Zyra e Komisionerit vlerëson se, sikurse citohet nga AMF, neni 32, i ligjit 32/2021 parashikon se, *"Qendra e Informacionit duhet t'ua mundësojë dhënien dhe përdorimin e të dhënave, të grumbulluara sipas këtij ligji, të gjitha palëve të dëmtuara dhe pjesëmarrësve në një aksident rrugor për një periudhë 7-vjeçare pas aksidentit..."*. Pra, kjo dispozitë përcakton afatin maksimal që AMF ka detyrimin ligjor për vendosjen në dispozicion të palëve të dëmtuara dhe pjesëmarrësve në një aksident rrugor, të dhëna që lidhen me rastin dhe jo kohën e ruajtjes së të dhënave nga vet Kontrolluesi, në kuptim të germës *"d"*, të pikës 1 të nenit 5 të ligjit.

2. Sa i përket konstatimit në lidhje me *"... shërbimin e mirëmbajtjes dhe të sigurisë së sistemeve, i cili kryhet nga punonjësit e drejtorisë TIK"*, Kontrolluesi bën me dije se, duke u nisur nga situatat e fundit, të ndodhura në vend, Drejtoria e TI është në proces të hartimit të kërkesave teknike për procedurën e mirëmbatjes së sistemeve, saktësisht REOSH dhe RED.

3. Sa i përket konstatimit në lidhje me: *"...pamjaftueshmërinë e masave të ndërmarra në lidhje me proceset e backup, të cilat nuk japin siguri në mbështetjen e BCP (Business Continuity Planning) dhe DRP (Disaster Recovery Plan), në kundërshtim me aktet ligjore apo nënligjore në fuqi"*, Kontrolluesi argumenton se, *"Procedura e Back up në Autoritet kryhet nëpërmjet Veam Software, e cila jep njoftime në rastet kur back up nuk kryhet në mënyrë të rregullt. Në raste të tilla, stafi i Drejtorisë së IT ndërhyn manualisht rifillimin e procesit të Back up-it me qëllim kryerjen e suksesshme të tij. Kontrolli i back up dhe verifikimi i tyre është detyrë funksionale e stafit të Drejtorisë së IT. Ky proces pune është një detyrë e përcaktuar në afate kohore (tasks) ditore, javore dhe mujore. Gjithashtu, në raste të evidentimit të ndonjë problematike, kryhet Raportimi me email tek eprorët."*

Sa më sipër, Zyra e Komisionerit vlerëson se pretendimet e Kontrolluesit nuk qëndrojnë pasi dokumentimi i masave përkatëse teknike dhe administrative, sa i përket konstatimeve të mësipërme, duhet të ishte kryer/demonstruar/dokumentuar nga nëpunësit e caktuar të AMF, gjatë procesit të hetimit administrativ.

4. Në lidhje me konstatimin se *"..nuk ka një akt të brendshëm, për caktimin e personave/strukturës përgjegjës për mbarëvajtjen e proceseve të punëve ..."*, Kontrolluesi argumenton se, *"Me qëllim mbarëvajtjen e proceseve të punës në Autoritet, detyrat funksionale të stafit të drejtorisë së IT janë të përcaktuara në*

rregulloren e brendshme të Autoritetit. Çdo detyrë analitike e punonjësve të Drejtorisë së IT është e përcaktuar në rregulloren e përshkrimit të detyrave të miratuara nga Bordi AMF-së".

Sa më sipër, Zyra e Komisionerit vlerëson se pretendimet e Kontrolluesit nuk qëndrojnë pasi caktimi i personave përgjegjës lidhet ngushtë me funksionimin e infrastrukturës dhe sistemeve respektive, si dhe në përmbushje të detyrimeve të VKM nr. 710, etj.

5. Në lidhje me konstatimin se *"...Kontrolluesi nuk disponon një plan vazhdimësie të mirë përcaktuar për BCP (Business Continuity Plan) dhe plan rikuperimi DRP (Disaster Recovery Plan) për garantimin e vazhdimësisë se ofrimit të shërbimit..."*, Kontrolluesi argumenton se, *"Bordi i Autoritetit ka miratuar në datë 16.12.2020 vendimin e Bordit nr. 186 "Mbi planin e vazhdueshmërisë së Aktivitetit të AMF". Aktualisht ekspertët e projektit të BB po punojnë për të përditësuar DRP për garantimin e vazhdimësisë së ofrimit të shërbimit nga IT. Nga ana juaj nuk na u kërkua ky material, do prezantohet."*

   Sa më sipër, Zyra e Komisionerit vlerëson se pretendimet e mësipërme nuk qëndrojnë, pasi gjatë hetimit administrativ është kërkuar që nga ana e përfaqësuesve të Kontrolluesit të vlerësohet çdo dokument plotësues, në funksion të objektit të hetimit.

6. Në lidhje me konstatimin se, *".. AMF ka nisur procesin e regjistrimit të Bazës së të dhënave për regjistrin Elektronik online të Shitjeve REOSH, me nr. identifikues "PJP-01-0054", si bazë të dhënash shtetërore në ARK, por rezulton se ky proces nuk ka përfunduar. Ndërsa për regjistrin e sistemit elektronik, të Dëmeve rezulton se nuk është regjistruar si bazë të dhënash shtetërore në ARK"*, Kontrolluesi argumenton se, *"Sipas shkresës nr. 1273 Prot., datë 29.06.2021, Autoriteti i Mbikëqyrjes Financiare ka nisur regjistrimin e Bazës së të dhënave për REOSH dhe ngelemi në pritje të një njoftimi nga Autoriteti përgjegjës për vijimin e procedurës. Sapo të kemi një njoftim, do të vijojmë procesin edhe për Regjistrin Elektronik të Dëmeve".*

   Zyra e Komisionerit vlerëson se regjistrimi i bazës së të dhënave, është i nevojshëm për standardizimin dhe sigurimin e saj në rast të ndërveprimit nëpërmjet Government Getaway, në kuptim të ligjit nr. 10325/2010.

7. Në lidhje me konstatimin se, *"AMF nuk ka një strategji të plotë për Teknologjinë e Informacionit dhe Komunikimit (TIK), ku të evidentohen nevojat aktuale dhe të merren në konsideratë ato për vijimësinë e punës së institucionit..."*, Kontrolluesi argumenton se, *"Aktualisht AMF ka planin e strategjisë 2018-2022 ku përfshihet dhe pjesa teknologjike e publikuar ne faqen zyrtare te AMF. Autoriteti deri më tani nuk e ka vlerësuar të nevojshme hartimin e një strategjie të veçantë sipas departamenteve/drejtorive".*

Sa më sipër, Zyra e Komisionerit vlerëson se pasja e një strategjie të plotë për Teknologjinë e Informacionit dhe Komunikimit (TIK), adreson qartë objektivat në fushën e Teknologjisë së Informacionit, duke marrë në konsideratë faktorë të ndryshëm si kohën, burimet e nevojshme, etj. Gjithashtu, zhvillimi i teknologjisë së Informacionit në mungesë të një Strategjie mund të sjellë pasqyrimin jo të qartë të objektivave të institucionit lidhur me infrastrukturën TI dhe burimet e nevojshme për ngritjen, zhvillimin dhe mirëmbajtjen e saj.

8. Në lidhje me konstatimin se, *"... edhe pse ka hartuar rregulla mbi menaxhimin e incidenteve dhe problemeve, rezulton se ato nuk dokumentohen sipas një plani masash për trajtimin e problemeve dhe incidenteve...",* Kontrolluesi argumenton se, *"Drejtoria TIK ka miratuar regjistrin e incidenteve i cili regjistron çdo ngjarje të raportuar nga stafi AMF-së, me qëllim parandalimin e rasteve që mund të shkaktojnë probleme".*

   Sa më sipër, Zyra e Komisionerit vlerëson se, pretendimet e mësipërme nuk qëndrojnë, pasi gjatë hetimit administrativ u është kërkuar përfaqësuesve të AMF dokumentimi i regjistrave të incidenteve dhe problemeve të ndryshme të infrastrukturës TIK dhe sistemeve elektronike, por një gjë e tillë nuk është mundësuar.

9. Në lidhje me konstatimin se, *"AKSHI dhe AMF, kanë lidhur marrëveshjen e nivelit të shërbimit SLA, për ofrimin e mirëmbajtjes dhe hostimit të infrastrukturës TIK që disponon AMF*. Këto shërbime konsistojnë në mirëmbajtjen dhe hostimin e DRP për sistemet, mail server, etj.) *Megjithëse është e lidhur një marrëveshje midis tyre, konstatohet se zbatueshmëria e saj nuk dokumentohet nëpërmjet raporteve periodike dhe të vazhdueshme, gjë që përbën risk për mbarëvajtjen, monitorimin dhe dokumentimin e shërbimeve TIK në AMF.",* Kontrolluesi pretendon se: *"Marrëveshja e Nivelit të Shërbimit (SLA) ndërmjet dy institucioneve, synon ofrimin e shërbimeve me qëllim rritjen e efektivitetit, kohëzgjatjes, kufizimin e risqeve teknike, pra në ruajtjen e integritetit, konfidencialitetit dhe vazhdueshmërisë së punës objekt i kësaj marrëveshje. Për shkak të natyrës teknike që ka kjo marrëveshje, stafi i Autoritetit është në komunikim të vazhdueshëm nëpërmjet postës elektronike/telefonit me stafin e AKSHI-t për sa kërkohet në marrëveshje, më qëllim kontrollet periodike."*

   Sa më sipër, Zyra e Komisionerit vlerëson se, Kontrolluesi është i detyruar të dokumentojë masat tekniko-organizative të përshtatura dhe të zbatuara për garantimin e mbrojtjes së të dhënave personale, në përputhje me ligjin dhe rregullore të tjera. Në këtë kuadër, është tepër i rëndësishëm dokumentimi i proceseve të punës, dhe për më tepër, gjatë ofrimit të mirëmbajtjes dhe hostimit të infrastrukturës TIK që Kontrolluesi disponon.

10. Në lidhje me konstatimin se, *"Kontrolluesi nuk ka marrë masa tekniko-organizative të përshtatshme, për krijimin e kushteve të nevojshme për të garantuar mbrojtjen e të dhënave personale të qytetareve, në përputhje me parashikimet e neneve 27 dhe 28 të*

Ligjit si dhe dispozitave të akteve nënligjore të Komisionerit.", Kontrolluesi pretendon se:

a. Autoriteti është i pavarur në ushtrimin e kompetencave të përcaktuara në këtë ligj ose në legjislacionin në fuqi dhe nuk lejohet ndërhyrja në veprimtarinë e tij, e cila mund të cenoje pavarësinë e Autoritetit. Autoriteti për përmbushjen e funksioneve rregullatorë dhe mbikëqyrëse, si dhe për organizimin dhe funksionimin e Autoritetit për veprimtarinë që ushtron, në përputhje me Ligjin nr. 9572, datë 3.7.2006 "*Për Autoritetin e Mbikëqyrjes Financiare*", i ndryshuar, raporton në Kuvend.
b. Një nga funksionet e Autoritetit është ai rregullues, që do të thotë që në zbatim të ligjit funksional të cituar më sipër, janë miratuar ligje që rregullojnë fushat e veprimtarisë së tij, rregullore, udhëzime etj.
c. Në lidhje me sigurinë e të dhënave, ligji nr. 9572, date 3.7.2006 "*Për Autoritetin e Mbikëqyrjes Financiare*", i ndryshuar, i ka dhëne kompetencë Bordit të miratojë politikat dhe rregulloret për sigurinë e këtyre të dhënave.
d. Fillimisht me miratimin e ligjit nr. 32/2021 "*Për sigurimin e detyrueshëm në sektorin e transportit*", pati tjetër qasje me sigurinë e të dhënave nisur nga miratimi i funksionimit të Qendrës së Informacionit dhe parashikimi i zbatimit të legjislacionit në fuqi për mbrojtjen e të dhënave personale.

   Ashtu siç ua kemi venë në dispozicion AMF ka të miratuar edhe rregullore të tjera në funksion të mbrojtjes së të dhënave personale. Burimet Teknologjisë së Informacionit (TI) të Autoritetit të Mbikëqyrjes Financiare si pajisjet kompjuterike (desktop, Laptop, Servera fizik dhe virtual, printera, switch), rrjeti i networkut, email, si dhe të dhënat dhe burimet digjitale përcaktohen në bazën ligjore në fuqi dhe në rregulloret dhe udhëzimet e miratuara nga Bordi i AMF-së të cilat janë të detyrueshme për t'u zbatuar nga punonjësit të cilët kanë akses në to. Disa nga aktet të cilat ua kemi vënë në dispozicion në funksion të mbrojtjes se të dhënave personale të miratuara nga AMF:

   - ✓ *Rregullore për organizimin, funksionimin dhe përshkrimin e detyrave miratuar me vendimin e bordit nr. 109, date 29.07.2020, Ndryshuar me Vendimin e Bordit nr. 104, datë 28.04.2022;*
   - ✓ *Rregullore "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale" Miratuar me vendim bordi Nr. 93 datë 25.09.2013;*
   - ✓ *"Udhëzim mbi parimet dhe rregullat e përgjithshme të sigurisë së informacionit" miratuar me Vendim Bordi nr.20 datë 06.02.2018;*
   - ✓ *Politikat dhe Procedurat për Sigurinë e TI (TI-POL-001), miratuar me vendim bordi Nr. 192, datë 14.10.2019;*
   - ✓ *Rregullore e brendshme "Rregullorja e përdorimit të resurseve të teknologjisë së informacionit nga stafi për Autoritetin e Mbikëqyrjes Financiare";*
   - ✓ *Rregullore për konfidencialitetin në Autoritetin e Mbikëqyrjes Financiare, miratuar me vendim bordi nr.114, datë 11.09.2008, i ndryshuar;*

- ✓ *Rregullore "Për Regjistrin Elektronik Online të Shitjeve" Miratuar me vendim bordi Nr. 159, datë 29.09.2021, i ndryshuar;*
- ✓ *Rregullore "Për Regjistrin Elektronik të Demeve të Sigurimeve të Detyrueshme Motorike" - Miratuar me vendim bordi Nr. 249, datë 24.12.2019;*
- ✓ *Rregullore "Për regjistrin elektronik të demeve të byrosë shqiptare të sigurimit" - Miratuar me vendim bordi Nr. 105, datë 30.06.2021.*

Sa më sipër, lidhur me këtë argument të dhënë nga Kontrolluesi, Zyra e Komisionerit vlerëson se, konstatimi mbi mungesën e marrjes së masave teknike dhe organizative vlen për të gjitha konstatimet e pikës 2 dhe nuk është një konstatim i shkëputur më vete. Ndërkohë, sa i takon argumenteve të dhëna nga Kontrolluesi se është Autoritet i pavarur në ushtrimin e kompetencave të përcaktuara në këtë ligj ose në legjislacionin në fuqi, dhe nuk lejohet ndërhyrja në veprimtarinë e tij, e cila mund të cenojë pavarësinë e Autoritetit, Zyra e Komisionerit vlerëson se edhe ky pretendim nuk e përligj mosmarrjen e masave të përshtatshme teknike dhe organizative nga ana e Kontrolluesit. Përcaktimet e legjislacionit për mbrojtjen e të dhënave personale janë të detyrueshme për tu zbatuar, ndër të tjera, nga çdo kontrollues i vendosur në Republikën e Shqipërisë, përfshirë edhe AMF.

11. Në lidhje me konstatimin se, *"...Qendra e Informacionit ndërvepron me anë të platformës qeveritare të ndërveprimit (GG), nga ku do merren të dhënat dytësore me institucionet...", AMF legjitimohet të ndërveprojë me GG, vetëm për të marrë të dhëna dytësore në kuptim të ligjit nr. 10 325/2010, Ndërsa, sa i përket ndërveprimit në portalin "e-Albania", ... në kundërshtim me kriteret ligjore të përpunimit, të parashikuara në nenin 6 të Ligjit,* Kontrolluesi argumenton se "*..do bëhet ndryshim në marrëveshjen me AKSHIN për të parashikuar këtë ekspozim të të dhënave."*

Sa më sipër, Zyra e Komisionerit vlerëson se, ndërveprimi i sistemeve me qëllim shkëmbimin e të dhënave, legjitimohet vetëm nëse përmbushet një prej kritereve të përpunimit të parashikuar në nenin 6 të Ligjit.

12. Në lidhje me konstatimin se, *"Nga verifikimi i kryer në regjistrin elektronik të subjekteve kontrolluese, 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...",* Kontrolluesi argumenton se:

Autoriteti i Mbikëqyrjes Financiare ka zbatuar rekomandimet nr. 03, datë 07.02.2019 dërguar me shkresën m. 116/4, datë 07.02.2019 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, ku me shkresën nr. 339/1 prot, datë 07.02.2019 ka informuar Komisionerin mbi masat e marra nga AMF, për zbatimin e tyre. Në lidhje me rekomandimet janë marrë masat që në faqen zyrtare të AMF-së, të jetë e pasqyruar në fund të saj, rubrika "Politikat e Privatësisë". Gjithashtu për çdo rast ku përdoruesi vendos të dhënat për të kërkuar informacion,

është shtuar opsioni i pranimit të detyruar të Politikave të Privatësisë sa më poshtë: "Verifikoni statusin e dosjes së Dëmit" sipas linkut https://amf.gov.al/vdws.asp "Verifikoni policen tuaj" sipas linkut https://amf.gov.al/mtpl.asp, "Depozito ankesën online" sipas linkut https://crm.amf.gov.al/complaint "Verifikoni historikun e dëmeve të mjetit" sipas linkut, https://amf.gov.al/vmws.asp.

Gjithashtu, janë marrë masa nga Autoriteti për vendosjen e tabelave informuese mbi prezencën e sistemit të video survejimit sipas standardit të parashikuar në Udhëzimin nr. 3/2010, të Komisionerit, "Për përpunimin e të dhënave personale me sistemin e video survejimit në ndërtesa dhe mjedise të tjera".

Sa më sipër, Zyra e Komisionerit vlerëson se, përmbushja e detyrimit për përditësimin e gjendjes së njoftimit të përpunimit të të dhënave, të njoftuar më parë, sipas parashikimeve të nenit 21 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.

Në lidhje me konstatimin se, Kontrolluesi disponon rregullore "*Për mbrojtjen e të dhënave personale*", por konstatohet se ajo nuk parashikon proceset, procedurat, masat teknike dhe organizative, etj., sipas parashikimeve të nenit 27 të Ligjit, Kontrolluesi argumenton se: *Autoriteti i Mbikëqyrjes Financiare ka miratuar në zbatim të ligjit nr.9887, datë 10.3.2008 "Për mbrojtjen e të dhënave personale", si dhe në bazë të udhëzimeve nga ana e Komisionerit për mbrojtjen e të dhënave personale rregulloren "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale" - Miratuar me vendim bordi nr. 93, datë 25.09.2013. Bazuar në nenin 2 të kësaj rregullore përcaktohet shprehimisht se ky akt bazohet dhe është në zbatim të ligjit nr. 9887, datë 10.3.2008. Ju konstatoni se ajo nuk parashikon proceset procedurale, masat teknike etj., sipas parashikimeve të nenit 27 të Ligjit. Nisur nga parimi i hierarkisë legjislative rregullorja hartohet me qëllim parashikimin e procedurave me të detajuara të cilat nuk mund të parashikohen në ligj. Dhe po sipas këtij parimi në rast se rregullorja nuk parashikon një procedure atëherë vijohet me zbatimin drejtpërdrejtë të dispozitës të parashikuar në ligj. Kjo do të thotë që Autoriteti në çdo rast është subjekt i zbatimit të dispozitave ligjore të cilat parashikojnë proceset procedurat, masat teknike për ruajtjen dhe sigurinë e të dhënave personale për aq kohë sa është në fuqi ligji nr. 9887, datë 10.3.2008. Për më tepër përveç rregullores "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale", Autoriteti ka të miratuara dhe akte të tjera nënligjore të tilla si "Udhëzimi mbi parimet dhe rregullat e përgjithshme të sigurisë së informacionit", miratuar me Vendim Bordi nr. 20, datë 06.02.2018; Politikat dhe Procedurat për Sigurinë e TI (TJ-POL-001), miratuar me vendim bordi Nr. 192, datë 14.10.2019; Rregullore e brendshme "Rregul1orja e përdorimit të resurseve të teknologjisë së informacionit nga stafi për Autoritetin e Mbikëqyrjes Financiare"; rregullore "Për Regjistrin Elektronik Online të Shitjeve" - Miratuar me vendim bordi nr. 159, datë 29.09.2021, e ndryshuar; Rregullore "Për Regjistrin Elektronik të Dëmeve të*

Sigurimeve të Detyrueshme Motorike" - Miratuar me vendim bordi nr. 249, datë 24.12.2019; Rregullore "Për regjistrin elektronik të dëmeve të Byrosë Shqiptare të Sigurimit" - Miratuar me vendim bordi nr. 105, datë 30.06.2021, etj., të cituara edhe më sipër të cilat kanë të përcaktuara në mënyre të detajuar proceset, procedurat, masat teknike dhe organizative për ruajtjen e të dhënave personale. Sa me sipër për nga ana rregullative e kuadrit ligjor, Autoriteti i ka marrë të gjitha masat për rregullimin procedurave të përpunimit dhe ruajtjes së sigurisë së të dhënave."

Sa më sipër, 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 subjektesh), 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.

Hartimi i një rregulloreje standarde për mbrojtjen e të dhënave personale, në të cilën mungojnë rregullat e qarta për garantimin e mbrojtjes, përpunimin, ruajtjen dhe sigurinë e të dhënave personale, e lidhur specifikisht me veprimtarinë dhe proceset përpunuese që kryen Kontrolluesi, nuk përmbush kërkesat e nenit 27 të Ligjit si dhe Vendimi nr. 6, datë 05.08.2013 i Komisionerit "*Për përcaktimin e rregullave të hollësishme për sigurimin e të dhënave personale*" (në vijim, "*Vendimi nr. 6*").

13. Në lidhje me konstatimin se, *"Kontrolluesi nuk ka ndërmarrë masa konkrete në kuadër të trajnimit të punonjëseve që kanë akses dhe përpunojnë të dhëna personale lidhur me legjislacionin në fuqi për mbrojtjen e të dhënave personale..."*, Kontrolluesi argumenton se:

Stafi i AMF dhe personat që kanë akses në asetet e informacionit të Autoritetit janë të detyruar të zbatojnë të gjithë kuadrin ligjor të parashikuar për funksionimin e AMF. Veçanërisht për pjesën e sigurisë së të dhënave Bordi i Autoritetit ka miratuar me Vendimin nr. 20, datë 06.02.2018 "Udhëzimin mbi Parimet dhe Rregullat e përgjithshme të Sigurisë së Informacionit, ku janë parashikuar parimet dhe rregullat e përgjithshme të sigurisë së informacionit në AMF. Ky udhëzim zbatohet për çdo pjesëtar të personelit, i cili akseson informacionin në pronësi ose të administruar nga AMF. Referuar pikës 4.4 të këtij udhëzimi: "Personat që kanë akses në asetet e informacionit të Autoritetit janë të detyruar të jenë të vetëdijshëm për rregullat dhe standardet e sigurisë në Autoritetit. I gjithë personeli duhet të marrë trajnimin e nevojshëm për rregullat dhe për procedurat organizative dhe të sigurisë. Ky trajnim kryhet sa më shpejtë që të jetë e mundur pas fillimit të punës së punonjësve të rinj."

Objektivat e edukimit ne lidhje me sigurinë janë:

- Krijimi i kulturës së sigurisë në të gjithë Autoritetin;
- Edukimi i personelit mbi pasojat e veprimeve të tyre mbi sigurinë e informacionit;

- Udhëzimi i personelit për rregullat dhe procedurat e sigurisë sipas pozicioneve përkatëse;
- Përcaktimi i përgjegjësive që mban çdo person mbi sigurinë dhe detyra e secilit për të raportuar çdo shkelje të rregullave të sigurisë.

Gjithashtu, i gjithë personeli duhet të trajnohet për përdorimin korrekt të sistemeve kompjuterike dhe të aseteve të informacionit. Kjo bëhet para se t'u jepet e drejta të aksesojnë sistemet. Drejtoria e TI përgjigjet për zhvillimin dhe për shpërndarjen e materialeve të trajnimit. Të gjithë specialistet e teknologjisë së informacionit duhet të marrin rregullisht trajnime përmirësuese ne fushat e tyre të specializimit. Kjo duhet të përfshije veçanërisht personelin e sigurisë, administratorët e bazave të të dhënave, administratorët e sistemeve operative dhe sistemeve te sigurisë (p.sh. Firewall, IDS, IPS, Network Management, Content Filtering, Application Security, etj.) I gjithë personeli i teknologjisë së informacionit duhet të ndjekë seminare periodike në fushat e interesit të përgjithshëm, veçanërisht në ato që lidhen me sigurinë.

Sa i përket këtij argumenti, Zyra e Komisionerit vlerëson se pretendimet e Kontrolluesit nuk qëndrojnë për arsye se, 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. Zyra e Komisionerit vlerëson se trajnimet duhet të kryhen me qëllim ndërgjegjësimin e operatorëve të cilët për shkak të proceseve të punës, janë të ngarkuar për përpunimin 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.

PËR KËTO ARSYE:

Në zbatim të neneve 5, 6, 21, 22, 27, 28, 29, 30, 31 (pika 1, germa "a/1"), si dhe 32 të Ligjit,

REKOMANDOJ:

1. Kontrolluesi të ketë në vëmendje të vazhdueshme përpunimin e të dhënave personale në përputhje me dispozitat e parashikuara në Kreun II të Ligjit.

2. Kontrolluesi, në zbatim të nenit 21 të Ligjit, të *"Njoftojë"* Zyrën e Komisionerit, për ndryshimin e gjendjes së njoftimit të përpunimit të të dhënave personale për të cilat është përgjegjës;

3. Kontrolluesi, në zbatim të neneve 27 dhe 28 të Ligjit, të marrë masa për hartimin e dokumentacionit të proceseve të punës, gjatë ushtrimit të aktivitetit;

4. Kontrolluesi, në zbatim të nenit 27 të Ligjit, të ketë në vëmendje përditësimin e rregullores "*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, etj., në funksion të aktivitetit të tij, për çdo proces përpunimi;

5. Kontrolluesi, me qëllim garantimin e sigurisë së të dhënave personale duhet të zbatojë detyrimet e përcaktuara në të Udhëzimit nr. 47, lidhur me krijimin, mirëmbajtjen dhe administrimin e Sistemit të Menaxhimit të Sigurisë së Informacionit (SMSI) për mbrojtjen e të dhënave personale;

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

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

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

7. Kontrolluesi të njoftojë Komisionerin për masat e marra;

8. Në rast mos përmbushje të detyrimeve të parashikuara në këtë akt, Komisionerit 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 08.11.2022.

KOMISIONERI

Besnik Dervishi