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 PERGJITHSHME PËR MBROJTJEN E TË DHËNAVE PERSONALE
DREJTORIA E HETIMIT SEKTORIAL DHE SIGURISË SË TË DHËNAVE

Nr.366/1 prot. Tiranë më 15.02.2023

VENDIM

Nr. 03, datë 15.02.2023

PËR KONTROLLUESIN "*INSIG" SHA*

Në mbështetje të neneve 29, 30 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 *"Insig" SHA* (në vijim, *"Kontrolluesi"*),

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 196, datë 10.11.2022, të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim, "*Komisioneri*"), u krye hetimi administrativ pranë Kontrolluesit, me objekt:

- *Zbatimi 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) dhe verifikim rekomandimi.*

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

1. Kontrolluesi ushtron veprimtarinë në tregun e sigurimeve, bazuar në Ligjin nr. 32/2021, datë 16.03.2021 "*Për sigurimin e detyrueshëm në sektorin e transportit*", Ligjin nr. 52, datë 22.05.2014 "*Për veprimtarinë e sigurimit dhe të risigurimit*", Ligji nr. 9901, datë 14.4.2008 "*Për Tregtarët dhe Shoqëritë Tregtare*", i ndryshuar, si dhe akteve të tjera normative të dala në zbatim të tyre, nga Autoriteti i Mbikëqyrjes Financiare (AMF). Kontrolluesi, gjatë ushtrimit të aktivitetit në funksion të

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

përmbushjes së qëllimit si një shoqëri sigurimi, ofron për shitje produkte për sigurimin e detyrueshëm (*Policë për sigurimin e detyrueshëm të mbajtësve të mjeteve motorike për përgjegjësi ndaj palëve të treta (TPL), certifikatë ndërkombëtare e sigurimit motorik (karton jeshil) dhe policë kufitare*), si dhe të gjitha llojet e sigurimit vullnetar (*sigurim shëndeti, prone, përgjegjësish, garanci, etj.*).

Kontrolluesi operon nëpërmjet agjenteve/degëve në të gjithë territorin e Republikës së Shqipërisë.

Kontrolluesi përpunon të dhëna personale për subjektet e të dhënave si *"klientë*", "*individë*", "*përfitues apo shkaktarë të dëmeve të përfshirë në një aksident automobilistik*", "*punonjës*", "*aksionerë*", "*vizitorë*", etj. Përpunimi i të dhënave kryhet në mënyrë manuale dhe elektronike.

2. Kontrolluesi përpunon të dhëna personale dhe sensitive, nëpërmjet krijimit të dosjeve fizike, për subjektet e të dhënave personale individë/klientë, në rastet e çeljes së praktikave të dëmshpërblimit shëndetësor, material dhe praktikave të tjera ligjore. Të dhënat sensitive që mblidhen, lidhen me shëndetin e klientit (*vendime paaftësie, diagnoza sëmundjesh, ekzaminime të ndryshme mjekësore, etj.*).

   Përpunimi i të dhënave personale nga Kontrolluesi bëhet në rrugë manuale, nëpërmjet krijimit të dosjeve fizike të trajtimit të dëmeve shëndetësore dhe materiale, si dhe në rrugë elektronike nëpërmjet krijimit të regjistrave elektronikë me bazë të dhënash për mënyrën e trajtimit të dosjeve të shëndetit dhe dosjeve materiale.

   Të dhënat e *"ish-punëmarrësve", "kandidatë për punë"* si dhe *"klientë të praktikave të dëmshpërblimit shëndetësor"* ruhen pa afat në arkivin fizik dhe elektronik të Kontrolluesit, në kundërshtim me parimin e mbrojtjes së të dhënave personale, të parashikuar në germën "*d*", të pikës 1, të nenit 5 të Ligjit, si dhe Udhëzimin nr. 11 datë 08.09.2011 *"Për përpunimin e të dhënave të punonjësve në sektorin privat",* i ndryshuar (në vijim, *"Udhëzimi nr. 11"*).

   Zyra e Komisionerit vlerëson se, lidhur me kategoritë e të dhënave të grumbulluara në funksion të ushtrimit të veprimtarisë së tij, Kontrolluesi duhet të parashikojë mbajtjen 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.

   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.

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

3. Kontrolluesi ka të instaluar një sistem video-survejimi (CCTV) për mbikëqyrjen e ambienteve të brendshme (korridoreve) dhe ambienteve të jashtme, për qëllim të sigurisë së aseteve. Në ambientet e brendshme të shoqërisë, oborrit etj., janë vendosur tabela informuese mbi prezencën e sistemit të video-survejimit (CCTV), por tabela nuk përmban elementët informues sipas parashikimeve të Udhëzimit 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"*).

   Kontrolluesi, në dokumentin tip për *"Kërkesë për dëmshpërblim"* si dhe në dokumentin *"Pyetësor"*, 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. Mos përmbushja e këtij detyrimi nga ana e Kontrolluesit mund të sjellë pasoja të rënda sa i përket privatësisë dhe përpunimit të të dhënave personale të subjekteve të të dhënave.

4. Veprimtaria e Kontrolluesit realizohet, ndër të tjera, nëpërmjet sistemit elektronik "*E-insure*", i përbërë nga pesë module si : *"Moduli i shitjeve të policave", "Moduli i magazinës", Moduli i financës", "Moduli i dëmeve"* dhe *"Moduli i burimeve njerëzore"*.

   Kontrolluesi ushtron veprimtarinë në të gjithë territorin e Republikës së Shqipërisë. Departamenti i shitjeve është ai që ofron për shitje produktet e Kontrolluesit, të tilla si: policat e detyrueshme dhe vullnetare për klientët. Nëpërmjet departamentit të shitjeve dhe dëmeve, Kontrolluesi menaxhon mbledhjen, përpunimin e të dhënave personale të klientëve në sistem elektronik dhe në rrugë manuale nëpërmjet krijimit të dosjeve për policat vullnetare.

   Kontrolluesi ofron, shitjen e policave të detyrueshme të tilla si: *Policë për sigurimin e detyrueshëm të mbajtësve të mjeteve motorike për përgjegjësi ndaj palëve të treta (TPL); Certifikatë ndërkombëtarë e sigurimit motorik (karton jeshil); Policë kufitare, në të gjitha kontratat vullnetare; Sigurim shëndeti, prone, sigurim kasko, sigurim oferte, sigurim nga zjarri etj., si dhe gjatë krijimit të praktikave për trajtimin e dëmeve shëndetësore dhe materiale në momentin e ndodhjes së "rastit të sigurimit".*

   Konstatohet se, Policat e sigurimit përmbajnë të dhënat personale që lidhen me: "*emrin, mbiemrin e përdoruesit/ve, gjinia, datëlindja, adresa, telefoni, të dhëna për mjetin, etj*.".

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

Sistemi elektronik *"E-insure*" hostohet në makina virtuale në server-a fizik, me infrastruktura mbështetëse TIK. Përdoruesit e sistemit (*operatorë ose/dhe punonjës, apo agjentë*) kanë mundësi që ta aksesojnë online nëpërmjet domain-it *"shitje.insig.com.al",* vetëm me "*password*" dhe *"username".* Site primar dhe site "*test*" i sistemit elektronik janë të ngritura si makina virtuale, të mbështetura sipas metodave të Microsoft për "*Virtualizim*" dhe "*Failover"*. Komponentët e infrastrukturës së rrjetit përfshijnë: *Firewall, Hardware Load Balancer, Switches, etj*.

Sistemi i "*E-insure*" është i ngritur mbi:

a. Sistemin e Operimit Windows Server 2012 /Windows Server 2016;
b. Databaza: SQL Server;
c. Microsoft për Virtualizim dhe *Failover*.

Konstatohet se, pajisjet e infrastrukturës hardware dhe software në të cilën ngrihet sistemi elektronik *"E-insure",* janë pjesë përbërëse e të njëjtës infrastrukturë TIK me palë të tjera, pjesë e të njëjtit grupit financiar Eurosig-Insig-UBA.

Menaxhimi i përdoruesve të sistemit kryhet nga përdoruesit me rol *"Administrator"*, si dhe nga ofruesi i shërbimit të mirëmbajtjes së sistemit në rastet kur kërkohet nga Kontrolluesi. Gjatë krijimit të një përdoruesi të ri, përcaktohet edhe roli i tij. Roli i secilit përdorues në sistem lidhet me një profil të caktuar (*menu, nyje dhe funksionalitete*). Kur një përdorues i caktohet një rol, automatikisht i jepen të drejta mbi profilin e këtij roli. Konstatohet se rolet janë, *"Administrator", "Agjent", "Anulon", "Auditi", "Burimet njerëzore", "Dëmet", "Financa", "Financa shef", "IT departament", "Konfirmim", "Magazina", "Ndryshon policën", "Përgjegjës i degës", "Raportimi", "Raportimi Jete", "Raportimi jo jetë".*

Ky sistem ndërvepron online nëpërmjet webservice me regjistrat e Autoritetit të Mbikëqyrjes Financiare (AMF), si Regjistri Elektronik Online i Shitjeve (*REOSH*) dhe Regjistri Elektronik i Dëmeve (*RED*).

Nga verifikimi rezulton se, sistemi *"E-insure"* ka disa dhënës informacioni me të cilët popullon bazën e të dhënave. Konkretisht, dhënësit e informacionit për sistemin elektronik *"E-insure"* janë: të dhënat e marra nga institucione të tjera, si Qendra Kombëtare e Biznesit (QKB), Drejtoria e Përgjithshme e Shërbimeve të Transportit Rrugor (DPSHTRR), Drejtoria e Përgjithshme e Gjendjes Civile (DPGJC) nëpërmjet komunikimit të webservice të sistemit "*E-insure*" me sistemin "*REOSH*" të AMF-së, si dhe nëpunës apo agjentët e shitjeve të policave.

Agjenti në momentin e shitjes të një prej produkteve/policave të detyrueshme, plotëson elektronikisht të dhënat personale të klientit në rubrikat e domosdoshme të formateve *"tip"*, etj. Shitja e policave të detyrueshme bëhet nga agjentët të cilët e regjistrojnë dhe në mënyrë elektronike në sistemin *"E-insure"*. Ky sistem raporton

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

shitjen e policave në sistemin elektronik REOSH të Autoritetit të Mbikëqyrjes Financiare.

Nga verifikimi on-site i sistemit *"E-insure"* si dhe nga shqyrtimi i procedurave rregulluese që disponon Kontrolluesi, rezulton se:

- Nuk ka plane të dokumentuara për menaxhimin e riskut, teknikat e menaxhimit dhe të performancës;
- 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 që sigurojnë vazhdueshmërinë e punës së sistemeve;
- Nuk ka të specifikuar/dokumentuar kohën maksimale në të cilën shërbimet dhe sistemet nuk mund të jenë funksionale. Nuk janë planifikuar masa që në rast dështimi të një/disa pajisjeve të mos ndikohet në funksionimin e sistemeve dhe shërbimeve të ofruara;
- Konstatohet se në ambientin *"test"* të sistemit *"E-insure",* punohet me të dhëna reale;
- Nuk ka kryer auditime të brendshme me qëllim garantimin e mirëfunksionimit të këtyre teknikave për menaxhimin e riskut (ose në mungesë të teknikave, identifikim të riskut).

Kontrolluesi me vendimin nr. 8, datë 22.12.2022, ka miratuar rregulloren për *"Për teknologjinë e informacionit në shoqërinë INSIG SH.A"*. Referuar pikës 2, të nenit 6, të kësaj rregullore, konstatohet se duhet të mbikëqyret regjistri i veprimeve (*Activity logs*), në rastet e ndonjë aktiviteti të dyshimtë gjatë përdorimit të sistemeve dhe pajisjeve TIK. Megjithatë konstatohet se, politikat mbi gjurmët (*log-et*) të sistemin *"E-insure"* dhe infrastrukturës mbështetëse TIK, 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.

Gjithashtu, konstatohet se masat e ndërmarra në drejtim të *backup*-it janë të pamjaftueshme dhe nuk japin siguri në mbështetjen e planit të vazhdueshmërisë së biznesit (BCP) dhe planit të rimëkëmbjes nga katastrofa (DRP), në kundërshtim kjo me masat e sigurisë së informacionit. Nuk u gjetën procedura të testimit të *backup*-it. Kopjet (*backup*) e të dhënave nuk testohen rregullisht për t'u siguruar që mund të përdoren në raste të nevojshme. Nuk u gjetën procedurat e rikrijimit (*restore*) të backup-it të të dhënave, me qëllim testimin e tyre për t'u siguruar që ato janë të efektshme dhe që mund të ekzekutohen brenda kohës së lejuar. Këto procedura duhet të testohen rregullisht, sistematikisht dhe vazhdimisht.

Nga kontrolli i përdoruesve të sistemit dhe përgjegjësive që ata kanë në sistemin *"E-insure"*, janë konstatuar disa problematika me ndikim/impakt në sigurinë e të dhënave, si vijon:

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

- Në sistem rezultojnë si përdorues mbi 860 *user*-a, ndër to dhe *user*-at që janë përdorur për testimet e implementimit të sistemit, apo përdorues të krijuar me të dhëna jo të plota. Referuar organizimit dhe funksionimit, rezulton se duhet të jenë më pak se 860 usera/përdorues të sistemit *"E-insure"* për kryerjen e detyrave funksionale;
- Në sistemin 9, *"E-insure"*, nuk janë sistemuar përdoruesit.

Zyra e Komisionerit vlerëson se, Kontrolluesi duhet të kryejë auditime të vazhdueshme mbi hedhjen e të dhënave dhe logim-et në sistem. 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, minimizon rrezikun që ngjarje të tilla të verifikohen dhe të lokalizojnë problemin.

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

Menaxhimi i përdoruesve të sistemit *"E-insure"* nga ana e administratorëve, duhet të jetë koherent me çdo ndryshim të funksionalitetit të punës apo në rastet e largimit nga pozicionet e punës, pasi veprimet e këtyre përdoruesve nuk mund të identifikohen dhe përbëjnë risk.

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.

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"*).

5. Kontrolluesi i ka rregulluar marrëdhëniet për ofrimin e shërbimit për veprimtarinë e sigurimit dhe risigurimit me agjentët nëpërmjet një kontratë *"tip"*.

Nga shqyrtimi i kontratës me palën e tretë, rezulton se në përmbajtje të saj 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*

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

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*). Gjithashtu, nga provat e administruara dhe konstatimet në vend rezulton se, mirëmbajtja e sistemit *"E-insure"* kryhet nga kompania Edusoft. Nga shqyrtimi i dokumentacionit të venë në dispozicion, rezulton së Kontrolluesi nuk është palë në këtë kontratë.

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 te përpunuesit të jetë në përputhje me legjislacionin 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, në përputhje me nenin 20 të Ligjit dhe me parashikimet e Udhëzimit nr. 19.

6. 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 megjithatë është konstatuar se "*Njoftimi*" ka mangësi në deklarim sa i përket rubrikave të formularit si vijon:

   - Deklarimin në rubrikën 1.1, të formularit të njoftimit *"Të dhënat e subjektit kontrollues";*
   - Deklarimin në rubrikën 1.2, të formularit të njoftimit *"Personi i kontaktit ngarkuar nga subjekti";*
   - Deklarimin në rubrikën 2.1, të formularit të njoftimit "*Fusha e veprimtarisë*";

   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.

7. Kontrolluesi me Vendimin e Këshillit Mbikëqyrës nr. 14, datë 24.03.2015, ka miratuar Rregulloren "*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*".

   Konstatohet se Rregullorja nuk parashikon proceset, procedurat, masat teknike dhe organizative ku të parashikohen rregulla dhe procedura organizative specifike mbi

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

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, dhe Vendimin 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*").

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.

8. 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 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, 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 akredituar 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.

   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.

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

Përfaqësuesi i Kontrolluesit u paraqit në seancën dëgjimore, ku parashtroi se qëndrimin mbi konstatimet e Grupit të hetimit do ti paraqesë me shkrim.

Me shkresën nr. 1928/4 prot., datë 19.12.2022, Kontrolluesi parashtroi argumentet si më poshtë:

Lidhur me pikën 2, të procesverbalit Kontrolluesi pretendon se *"Sa i përket të dhënave të ish-punonjësve, ato ruhen për arsye të ligjit nr.7703, datë 11.5.1993 "Për Sigurimet shoqërore në Republikën e Shqipërisë", për arsye se referuar këtij ligji, punëmarrës dhe ish-punëmarrës të shoqërisë kërkojnë herë pas here vërtetime lidhur me vitet e punësimit pranë shoqërisë INSIG sh.a". Lidhur me mbajtjen e të dhënave të klientëve të praktikave të dëmshpërblimit shëndetësor, bëjmë me dije se, në asnjë rast nuk është e përcaktuar apo e ditur se nga momenti i regjistrimit të kërkesës për dëmshpërblim, kur do të jetë afati përfundimtar i punës me një praktikë dëmi, pasi në disa raste shoqëria është përballur me çështje gjyqësore që i përkasin praktikave të dëmit tepër të hershme. Në çdo rast të dhënat e administruara nga INSIG sh.a kanë miratimin e plotë të personit disponues të tyre dhe se përgjithësisht grumbullohen me kërkesë të tyre në zbatim të ligjeve të sipërcituara".*

Zyra e Komisionerit vlerëson se, Kontrolluesi ka detyrim të përpunojë të dhënat personale për aq kohë sa ekziston qëllimi për të cilin janë grumbulluar dhe përpunuar (neni 5/1/d) dhe në momentin që qëllimi ka përfunduar të realizojë shkatërrimin e tyre, në të kundërt përpunimi i mëtejshëm i të dhënave konsiderohet i paligjshëm. Koha e ruajtjes së të dhënave personale duhet të përcaktohet nga Kontrolluesi, në përputhje me parashikimet ligjore specifike dhe qëllimin e përpunimit.

Lidhur me pretendimet e parashtruara nga Kontrolluesi se, në asnjë rast nuk mund të dihet se cili do të jetë afati përfundimtar i punës me një praktikë dëmi, Zyra e Komisionerit vlerëson se, vetë Kontrolluesi rast pas rasti duhet të bëjë një vlerësim, për të gjitha proceset e përpunimit 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 të grumbulluar.

- Lidhur me pikën 4, të procesverbalit Kontrolluesi shprehet se "*860 është numri i përdorueseve të krijuar dhe aktualisht janë vetëm 240 përdorues me status aktiv. Pjesa tjetër e përdorueseve, pra rreth 620 të tillë janë me status pasiv, pra me asnjë mundësi qasje në këtë sistem, të cilëve u ka ndryshuar statusi nga aktiv në pasiv në momentin që zgjidhin kontratën e punës. Të gjithë përdoruesit e këtij sistemi elektronik, pavarësisht statusit të tyre, konsiderohen si plotësisht të sistemuar dhe me privilegje të mirë përcaktuara në funksion të detyrave që ata kryejnë në këtë sistem.*

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

Gjithashtu, referuar konstatimit për politikat mbi gjurmët (log-et) theksojmë se në mbështetje të kësaj aplikohen këto masa dhe mekanizma sigurie: Mekanizëm sigurie i aplikuar në nivel aplikacioni; Mekanizëm sigurie i aplikuar në nivel database; Mekanizëm sigurie i aplikuar në nivel network; Mekanizëm sigurie i aplikuar në nivel sistemi software-ik. Në momentin e një aplikimi/tentative për login në këtë sistem, vihen në funksionim mekanizmat e autentifikimit të kësaj kërkese për akses.

E gjithë pjesa e infrastrukturës TIK është ideuar dhe realizuar për të mundësuar planin e vazhdueshmërisë së biznesit e mbështetur kjo në ngritjen e mekanizmit të failover-it, duke dublikuar pajisjet me potencial për dështim të mundshëm. Procesi i backup-it realizohet në periudha të përcaktuara më parë sipas një grafiku dhe po sipas këtij plani bëhet restore në ambientin test të sistemit elektronik me qëllim për të parë efiçencën e një procesi të tillë. Kjo është edhe arsyeja pse sistemi elektronik "test" është i njëjtë me atë live në të dhëna. Për sa i përket planit të rimëkëmbjes nga katastrofa (DRP), kontrolluesi është në proces të ngritjes dhe implementimit të këtij plani për të qenë funksional në fillim të vitit që vjen.

Referuar kontratës së lidhur me kompaninë Edusoft e cila realizon outsourcing për sistemin E-Insure, Insig sh.a është në proces rishikimi dhe përditësimi të një versioni të ri për këtë qëllim".

Zyra e Komisionerit vlerëson se, krijimi i procedurave dhe politikave të përdorimit të infrastrukturës TIK dhe sistemeve elektronike nga Kontrolluesi si dhe zbatimit praktik të tyre, është një ndër masat kryesore që duhet të marrë Kontrolluesi, në lidhje me sigurinë dhe funksionimin e sistemeve të teknologjisë së informacionit.

Struktura përgjegjëse e Kontrolluesit duhet të kryejë auditime të vazhdueshme mbi hedhjen e të dhënave dhe *log*-eve në sistem, etj. Analizimi periodik i veprimeve/gjurmëve të përdoruesve apo të funksionimit të sistemit nëpërmjet log-eve, minimizon riskun dhe lokalizon problemin me qëllim për të parandaluar çdo cedim të mundshëm të funksionimit të sistemit.

Krijimi, monitorimi dhe zbatimi i procedurave të *backup*-it dhe vazhdimësisë së punës për Sistemet e Informacionit në sistemin *E-Insure*, duhet të adresohet nga strukturat përgjegjëse të Kontrolluesit me qëllim sigurinë dhe garantimin e funksionimit të sistemit të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të shërbimit.

Kontrolluesi duhet të marrë masa teknike të nevojshme që të dhënat që përpunohen në ambientin *"test",* të mos jenë reale dhe të ndërlidhura me ambientet e sistemit *"production",* me qëllim minimizimin e riskut të sigurisë së informacionit dhe integritetin e të dhënave.

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

Gjithashtu, menaxhimi i përdoruesve të sistemit "*E-Insure"* nga ana e administratorëve, duhet të jetë koherent me çdo ndryshim të funksionalitetit të punës apo në rastet e largimeve nga pozicionet e punës. Llogaritë e përdoruesve në sistem të tipit *"guest/user",* nuk duhet të jenë aktive dhe më të drejta funksionale, pasi veprimet e këtyre përdoruesve nuk mund të identifikohen dhe si rrjedhojë përbëjnë risk.

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 nga nëpunësit e caktuar të Kontrolluesit, gjatë procesit të hetimit administrativ.

- Lidhur me pikën 5, të procesverbalit Kontrolluesi shprehet se; "*Agjentët nuk mund të trajtohen si përpunues të punësuar pranë INSIG sh.a. Logjika rregulluese dhe interpretuese e nenit 20 të Ligjit, ka të bëjë vetëm me rregullimin ligjor që ligjvënësi i ka bërë këtij pozicioni që quhet punonjës përpunues pranë Kontrolluesit*".

  Zyra e Komisionerit vlerëson se pretendimet e Kontrolluesit nuk qëndrojnë pasi, sipas parashikimit të pikës 7, të nenit 3 të Ligjit "*Përpunues*" është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër që përpunon të dhëna personale në emër të Kontrolluesit. Parashikimet e nenit 20 të Ligjit nuk kanë të bëjnë me detyrimet që kanë punëmarrësit e punësuar pranë Kontrolluesit, por me detyrimet ligjore të cilat duhet të jenë të përfshira në kontratën dhe/ose aneks kontratën e shkruar mes Kontrolluesit dhe subjektit përpunues.

  Nga hetimi administrativ i ushtruar rezulton se agjentët (*jo si individ, por në cilësinë e personit fizik ose juridik të regjistruar pranë QKB-së*) përpunojnë të dhëna personale për llogari të Kontrolluesit. Në këtë kuadër, është plotësisht përgjegjësi e Kontrolluesit të përmbush detyrimet e sanksionuara në nenin 20 të Ligjit dhe Udhëzimit nr. 19.

- Lidhur me pikën 6, të procesverbalit Kontrolluesi shprehet se "*Të dhënat e subjektit kontrollues janë të deklaruara, Lidhur me personin e kontaktit, përditësimi i tij nuk është detyrim ligjor për të cilin duhet të shprehet Kontrolluesi, ndërsa fusha e veprimtarisë rezulton të jetë e plotësuar* ".

  Zyra e Komisionerit vlerëson se, pretendimi i Kontrolluesit nuk qëndron pasi të gjitha rubrikat e formularit të njoftimit janë të detyrueshme për tu plotësuar dhe përditësuar nga Kontrolluesi sipas Vendimit nr. 66, datë 01.10.2009 të Komisionerit, me anë të të cilit është miratuar modeli standard i *"Formularit të Njoftimit"* si dhe Udhëzuesi për plotësimin e tij, bazuar në Ligjin nr. 9887, datë 10.03.2008 *"Për mbrojtjen e të dhënave personale"*, i ndryshuar. Formatet e miratuara nga autoriteti përgjegjës (*të tilla si: formulari i njoftimit*), janë të detyrueshme për tu zbatuar.

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

Përditësimi i të dhënave të personit të kontaktit, ka për qëllim mbarëvajtjen e procesit të njoftimit dhe përditësimit të njoftimit. Ndryshimi i vetëm është që të dhënat e personit të kontaktit, të deklaruara në rubrikën 1.2 të formularit të njoftimit nuk pasqyrohen në regjistrin e hapur për publikun.

Lidhur me pikën 7, të procesverbalit Kontrolluesi shprehet se; "*Lidhur me konstatimet mbi Rregulloren nr. 14 "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale", përveç faktit që nuk ka të përcaktuar një afat për ruajtjen e të dhënave, pretendimet e tjera nuk qëndrojnë, pasi proceset, procedurat, masat teknike dhe organizative specifike mbi mënyrën e përpunimit të të dhënave personale, sigurinë e të dhënave, konfidencialitetin, janë të përcaktuara konkretisht nenet 8, 9, 10, 13, 19, 20, 25 të kësaj rregullore.*

Lidhur me ketë pretendim Zyra e Komisionerit vlerëson se, rregullorja e vendosur në dispozicion të grupit të kontrollit nuk parashikon proceset, procedurat, masat teknike dhe organizative, ku të parashikohen rregulla dhe procedura organizative specifike mbi mënyrën e përpunimit të të dhënave personale (për çdo kategori të dhënash) që përpunon, sigurinë e të dhënave, konfidencialitetin, afatet e mbajtjes së të dhënave, etj., në kundërshtim me parashikimet e nenit 27 të Ligjit, dhe Vendimin nr. 6 të Komisionerit.

- Lidhur me pikën 8, të procesverbalit Kontrolluesi shprehet se "*...nuk ka aftësi profesionale dhe njohuri të posaçme apo persona të kualifikuar në fushën e trajnimit të punonjësve të saj për sa i përket legjislacionit në fuqi për mbrojtjen e të dhënave personale. Në këto kushte ju bëjmë me dije se INSIG sh.a është dhe do të jetë gjithmonë e hapur për të marrë pjesë në trajnime të cilat ka detyrim dhe duhet ti realizojë Komisioneri".*

  Sa i përket këtij argumenti, Zyra e Komisionerit vlerëson se, bazuar në parashikimet e 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 punëmarrësit të trajnohen për mbrojtjen e të dhënave personale. Sipas parashikimeve të ligjit Komisioneri është autoriteti përgjegjës i pavarur, që mbikëqyr dhe monitoron, në përputhje me ligjin, mbrojtjen e të dhënave personale, duke respektuar e garantuar të drejtat dhe liritë themelore të njeriut, dhe nuk është përgjegjës për realizimin e trajnimeve të punonjësve të Kontrolluesve si publikë dhe privatë.

  Gjithashtu, sa i takon verifikimit në lidhje me detyrimet e rekomandimeve të mëparshme të dhëna nga Zyra e Komisionerit rezulton se, Kontrolluesi nuk ka marrë masa për plotësimin e detyrimeve ligjore. Konkretisht në zbatim të detyrimeve të lëna

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

në Vendimin nr. 10, datë 29.12.2014 të Komisionerit, rezulton se Insig Sha, nuk ka marrë masa sa i takon detyrimeve të parashikuara në nenet 18, 20, 27 dhe 28 të Ligjit.

Si përfundim, shkeljet e konstatuara gjatë ushtrimit të hetimit administrativ në kuptim germave "*a", "b", "ç", "d" dhe* "*dh"* dhe 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 të ripërsëritura 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 teknike-organizative për sigurinë e të dhënave personale.

PËR KËTO ARSYE:

Sa më sipër, në zbatim të neneve 5, 18, 20, 21, 27, 28, 29, 30, 39 (pika 1, germat *"b", "ç" dhe "dh"),* si dhe nenet 40 dhe 41 të Ligjit,

V E N D O S A:

1. Dënimin e Kontrolluesit me gjobë në vlerën 100 000 (njëqind mijë) lekë, për shkelje të detyrimit të përcaktuar në nenin 18 të Ligjit;

2. Dënimin e Kontrolluesit me gjobë në vlerën 150 000 (njëqind e pesëdhjetë mijë) lekë, për shkelje të detyrimit të përcaktuar në nenin 20 të Ligjit;

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

3. Dënimin e Kontrolluesit me gjobë në vlerën 120 000 (njëqind e njëzetë mijë), për shkelje të detyrimit të përcaktuar në nenin 27 dhe 28 të Ligjit;

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

5. Kontrolluesi, në zbatim të nenit 18 të Ligjit, të marrë masa konkrete, për përmbushjen e detyrimit për informimin e subjekteve të të dhënave personale mbi qëllimin dhe mënyrën e përpunimit të të dhënave, etj.;

6. Kontrolluesi, të marrë masa të përfshij detyrimet e secilës palë në kontratë, sipas parashikimeve të nenit 20 të Ligjit dhe Udhëzimit nr. 19 të Komisionerit;

7. Kontrolluesi, në zbatim të neneve 21 dhe 22 të Ligjit, të kryej përditësimin e "*Njoftimit*" në lidhje me ndryshimin e gjendjes së njoftimit të përpunimit të të dhënave personale, të cilat përpunon;

8. Kontrolluesi, në zbatim të nenit 27 të Ligjit, të përfshijë në Rregulloren "*për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*", 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;

9. 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;

10. 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;

11. 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 pikën 4 më sipër;
    (ii) brenda 15 (pesëmbëdhjetë) ditëve, detyrimet e përcaktuara pikat 5, 6 dhe 7 më sipër;
    (iii) brenda 30 (tridhjetë) ditëve, detyrimet e përcaktuara në pikën 8 më sipër;
    (iv) brenda 45 (dyzetë e pesë) ditëve, detyrimet e përcaktuara në pikën 9 më sipër.

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

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

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

13. 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;

14. 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 15.02.2023.

KOMISIONERI

Besnik Dervishi

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