Nr.367 prot. Tiranë më 15.02.2023

REKOMANDIM

Nr. 04, datë 15.02.2023

PËR KONTROLLUESIN "*EUROSIG" 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 *"Eurosig" SHA* (në vijim, *"Kontrolluesi"*),

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 198, 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, 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 14.04.2008 "*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 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*

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

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 agjentëve në të gjithë territorin e Republikës së Shqipërisë. Gjatë ushtrimit të aktivitetit, Kontrolluesi përpunon të dhëna personale për subjektet e të dhënave personale si: *"klientë*", "*individë*", "*përfitues apo shkaktarë të dëmeve të përfshirë në një aksident automobilistik*", "*punonjës*", "*aksionerë*", "*vizitorë*", *"ish-punëmarrësve"*, *"kandidatë për punë"* etj. Përpunimi i të dhënave kryhet në mënyrë elektronike dhe manuale.

2. Kontrolluesi përpunon dhe ruan 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 (*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 arkivën fizike dhe elektronike të Kontrolluesit. Përmbajtja e dosjeve personale të ish-punëmarrësve dhe kandidatë për punë, konsiston në dokumente të noterizuara dhe/ose të fotokopjuara të tilla si: jetëshkrim, kopje të kartës së identitetit, kopje e listës së notave, kopje e diplomës, etj., në kundërshtim me parimet e mbrojtjes së të dhënave personale, parashikuar në germën "*d*", të pikës 1, të nenit 5 të Ligjit, si dhe Udhëzimin nr. 11, datë 08.09.2011 të Komisionerit*"Për përpunimin e të dhënave të punonjësve në sektorin privat",* i ndryshuar (në vijim, *"Udhëzimi nr. 11"*).

   Zyra e Komisionerit vlerëson se, Kontrolluesi 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.

3. Kontrolluesi ka të instaluar një sistem video-survejimi (CCTV) të cilat mbikëqyrin korridoret, ambientet e jashtme dhe ambientet e brendshme të zyrave. Konstatohet se kamerat janë pozicionuar në ambientet e brendshme të zyrave, në kundërshtim me parashikimet e neneve 5 dhe 6 të Ligjit dhe Udhëzimit nr. 11 të Komisionerit.
   Në ambientet e brendshme të shoqërisë, oborrit etj., ka tabela informuese mbi prezencën e sistemit të video survejimit CCTV, por tabelat nuk përmbajnë elementët

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

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*").

Zyra e Komisionerit vlerëson se, një nga mjetet e rëndësishme të përpunimit të të dhënave personale është edhe sistemi i video/audio-survejimit (CCTV). Të dhënat e ruajtura në këto sisteme si *"imazhe"* dhe *"video"*, janë të dhëna personale, dhe përpunimi i tyre duhet të jetë në përputhje me parashikimet e Ligjit si dhe akteve të miratuara nga Komisioneri në lidhje me mbledhjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale, gjatë kryerjes së aktivitetit nga Kontrolluesit.

4. Kontrolluesi u mundëson klientëve të kërkojnë shpërblimin e dëmit të mjetit motorik në rast aksidenti duke plotësuar dokumentin "tip" për *"Kërkesë për dëmshpërblim dëmi".* Nëpërmjet dokumentit tip Kontrolluesi mbledh të dhëna personale të kategorive të ndryshme të tilla si, emër, mbiemër, datëlindje, vendlindje, numër telefoni, e-mail, targë automjeti, etj. Konstatohet se, në dokumentin "*tip*" nuk ka të parashikuar asnjë rubrikë në mënyrë që të informojë subjektet e të dhënave mbi përpunimin e të dhënave, në kundërshtim me parashikimet e nenit 18 të Ligjit.

   Zyra e Komisionerit vlerëson se, informimi i subjekteve të të dhënave personale është një nga detyrimet bazë të Kontrolluesit pasi u jep mundësinë subjekteve të të dhënave personale të njihen me të drejtat që gëzojnë dhe mundësinë e ushtrimit të tyre në praktikë. Mospërmbushja e këtij detyrimi nga ana e Kontrolluesit mund të sjellë pasoja të rënda sa i përket privatësisë dhe përpunimit të të dhënave personale të subjekteve të të dhënave.

5. 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 nëpërmjet agjentëve. Departamenti i shitjeve ofron shitjen e produkteve të 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 klientëve në sistem elektronik dhe në rrugë manuale nëpërmjet krijimit të dosjeve për policat vullnetare.

   Kontrolluesi, ndër të tjera, ofron, shitjen e policave të detyrueshme (*Policë për sigurimin e detyrueshëm të mbajtësve të mjeteve motorike për përgjegjësi ndaj palëve të treta (TPL), certifikatë ndërkombëtarë e sigurimit motorik (karton jeshil) dhe 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.

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

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*.".

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.eurosig.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, Storage Backup, 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 grupi 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 përdoruesi 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", "Raportim Jete", " Raportimi jo jetë".*

Ky sistem ndërvepron online nëpërmjet webservice me regjistrat e AMF-së, 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 nëpunësit apo agjentët e shitjeve të policave.

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

Agjenti në momentin e shitjes së 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 shitjen e policave në sistemin elektronik REOSH, të AMF-së.

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 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;
- 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);
- Nuk ka kryer raportime të përcaktuara sipas pikës 6.4 të *"Manualit të procedurave standarde të punës në dhomën e serverave",* miratuar me Urdhër nr. 246, datë 26.06.2020, të Drejtorit të Përgjithshëm.

Konstatohet se, politikat mbi gjurmët (*log*-et) në sistemin *"E-insure"* dhe infrastrukturën mbështetëse TIK, nuk zbatohen sipas një procedure të rregulluar, me risk në qasje të paautorizuar në të dhëna, kërcënim të sigurisë në fushën e teknologjisë së informacionit dhe mungesë transparence.

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

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:

- Në sistem rezultojnë si përdorues mbi 2161 *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

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

të jenë më pak se numri aktual i usera/përdorues të sistemit *"E-insure"* për kryerjen e detyrave funksionale;
- Në sistemin *"E-insure"*, nuk janë sistemuar përdoruesit.

Për sa më sipër, Zyra e Komisionerit vlerëson se, Kontrolluesi nuk ka marrë masa organizative dhe teknike të përshtatshme për të mbrojtur të dhënat personale nga shkatërrime të paligjshme, aksidentale, humbje aksidentale, për të mbrojtur aksesin ose përhapjen nga persona të paautorizuar, veçanërisht në këtë rast kur përpunimi i të dhënave kryhet nëpërmjet komunikimeve elektronike, në kundërshtim me parashikimet e nenit 27 të Ligjit, si dhe Udhëzimit nr. 47, datë 14.09.2018 të Komisionerit *"Për përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga subjektet përpunuese të mëdha"*, (në vijim*, "Udhëzimi nr.47"*).

6. Kontrolluesi i ka rregulluar marrëdhëniet për ofrimin e shërbimit për veprimtarinë e sigurimit dhe risigurimit me agjentët nëpërmjet një kontrate *"tip"*. Gjithashtu, Kontrolluesi ka lidhur një *"Kontratë Shërbimi Mirëmbajtje"* nr. 1717 prot., datë 09.04.2021, me shoqërinë me përgjegjësi të kufizuar *"Sinteza CO shpk"*, si palë të tretë.

   Nga shqyrtimi i kontratave të sipëcituara, rezulton se në përmbajtje të tyre 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"*).

   Zyra e Komisionerit vlerëson se, të gjitha detyrimet e sanksionuara në këtë nen duhet të jenë të përfshira në kontratën dhe/ose aneks kontratën e shkruar mes Kontrolluesit dhe Përpunuesit. Çdo kontratë përpunimi (*outsourcing*) që ka për qëllim delegimin e përpunimit të të dhënave personale duhet të përmbaj dispozita që vendosin rregulla për përpunimin e të dhënave personale, sipas legjislacionit në fuqi. Çdo kontratë e tillë duhet të parashikoj masat që duhet të marr përpunuesi për të siguruar/garantuar mbrojtjen e mjaftueshme të të dhënave, si dhe hapat që do të ndërmerren në rast cenimi të të dhënave, me qëllim që të sigurojë paprekshmërinë e tyre, në çdo hallkë të këtij përpunimi.

7. 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:

   - *Rubrika 1.2: Ndryshimi i personit të kontaktit;*
   - *Rubrika 3.1: Kategoritë e subjekteve të të dhënave personale që përpunohen;*

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

- *Rubrika 4.1 : Kategoritë e të dhënave personale që përpunohen.*

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.

8. Kontrolluesi me vendimin nr. 5416/1 prot., datë 31.10.2022, të Këshillit Mbikëqyrës ka miratuar Rregulloren "*Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale në shoqërinë Eurosig SH.A*".

   Konstatohet se, Rregullorja nuk parashikon qartë proceset, procedurat, masat teknike dhe organizative ku të parashikohen rregulla dhe procedura organizative specifike mbi mënyrën e përpunimit të të dhënave personale, sigurinë e të dhënave, konfidencialitetin, afatet e mbajtjes së të dhënave, etj., në kundërshtim me parashikimet e nenit 27 të Ligjit 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 të dhënash*), sigurinë e të dhënave, konfidencialitetin, afatet e mbajtjes së të dhënave, nivelet e aksesit etj., konsiderohet një detyrim shumë i rëndësishëm në zbatim të nenit 27 të Ligjit, pasi shmang pasojat e rënda që mund të vijnë për subjektet e të dhënave.

9. Kontrolluesi nuk ka ndërmarrë masa konkrete në kuadër të trajnimit të punonjësve që kanë akses dhe përpunojnë të dhëna personale lidhur me legjislacionin në fuqi për mbrojtjen e të dhënave personale. Grupi i kontrollit konstaton mosplotësim të detyrimeve në lidhje 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,

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

Kontrolluesi, është i detyruar të krijojë, mirëmbajë dhe administrojë SMSI në përputhje me parashikimet e Udhëzimit nr. 47.

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

Në përfundim të hetimit administrativ, referuar provave dhe konstatimeve në vend, grupi i hetimit administrativ hartoi procesverbalin përkatës, një kopje e të cilit i është 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.

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. 6363 prot., datë 21.12.2022, Kontrolluesi parashtroi argumentet si më poshtë:

- Në lidhje me pikën 2 të procesverbalit të konstatimit, Kontrolluesi shprehet se "*...përsa i përket "Dosjeve personale të ish-punëmarrësve" sqarojmë se, ruhen në arkivën fizike të shoqërisë Eurosig sha për një periudhë deri në 6 muaj, në respektim të afatit ligjor të përcaktuar në nenin 33, pika 4, të Kodit të Punës dhe nenit 29 të Rregullores "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale" në shoqërinë Eurosig sh.a (miratuar me vendimin nr. 18, datë 31.10.2022, të Këshillit Mbikëqyrës)...*"

  ..Ndërsa në lidhje me "kandidatët për punë", sqarojmë se në arkivën fizike mbahet vetëm Jetëshkrimi (CV) dhe asnjë dokument tjetër identifikues, të tilla si kopje të kartës së identitetit, kopje të listës së notave apo kopje të diplomës...

  Nga ana tjetër, sqarojmë se dosjet "Klientë të praktikave të dëmshpërblimit shëndetësor" ruhen, administrohen dhe përpunohen nga shoqëria Eurosig sh.a. në kuadër të përmbushjes së detyrimeve ligjore në fushën e sigurimeve, Rregullores "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale në shoqërinë Eurosig sh.a." dhe sipas afateve të miratuara me urdhrin nr. 575, datë 19.09.2022, të Drejtorit të Përgjithshëm, "Për miratimin e listës tip të dokumenteve, afateve e ruajtjes dhe kritereve për administrimin e dokumenteve dhe komunikimin në strukturat e Eurosig-ut".

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

Megjithatë, theksojmë se në disa raste është e pamundur të përcaktohet afati i ruajtjes, administrimit dhe përpunimit të të dhënave personale për klientë apo të dëmtuar, sidomos në rastet kur këta të fundit i drejtohen organeve gjyqësore për të kërkuar shpërblimin e dëmit apo një të drejte legjitime të pretenduar prej tyre (shih me poshtë pikën 7).

Nga sa më sipër, shoqëria Eurosig sh.a. nuk ka vepruar në kundërshtim me përcaktimet e nenit 5 dhe 6, të ligjit nr. 9887/2008..."

Lidhur me pretendimet e parashtruara nga Kontrolluesi se, afatet për ruajtjen e të dhënave në dosjet personale të ish punëmarrësve parashikohen në Rregulloren "*për mbrojtjen e të dhënave personale*" dhe në dispozitat e Kodit të Punës, Zyra e Komisionerit vlerëson se, pretendimet e Kontrolluesit nuk qëndrojnë për arsyet në vijim:

Së pari, dispozita e cituar nga Kontrolluesi në rregulloren *"Për mbrojtjen e të dhënave personale"* është e përgjithshme dhe parimore, pra nuk ofron asnjë rregullim konkret të proceseve përpunuese të Kontrolluesit lidhur me detyrimet për të mbajtur të dhënat personale 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. Së dyti, afati i parashikuar në pikën 4, të nenit 33, të Kodit të Punës, i cituar nga Kontrolluesi, aplikohet specifikisht për ato raste kur kontrata zgjidhet pa shkaqe të arsyeshme. Ndërsa, dokumentet e administruar nga grupi i hetimit në cilësinë e provës materiale i referohen një rasti ku marrëdhënia e punës është ndërprerë me konsensus dhe nuk gjen mbështetje në dispozitën e Kodit të Punës, për rrjedhojë Kontrolluesi duhet të marrë masa konkrete në përputhje me parashikimet e nenit 5 dhe 6, të Ligjit.

Lidhur me pretendimin se, për kategorinë "*kandidatët për punë*", mbahet vetëm Jetëshkrimi (CV) dhe asnjë dokument tjetër identifikues, Zyra e Komisionerit vlerëson se, jetëshkrimi i kandidatëve përmban një numër të konsiderueshëm të dhënash personale, të cilat bëjnë qartësisht të identifikueshëm subjektin e të dhënave. Gjithashtu, përveç parashikimeve ligjore për parimet dhe kriteret e përpunimit të të dhënave personale, Zyra e Komisionerit ka miratuar dhe akte nënligjore që rregullojnë përpunimin e të dhënave personale të kandidatëve për punë, konkretisht, Udhëzimin nr. 42, datë 22.07.2014 të Komisionerit "*Për përpunimin e të dhënave personale të kandidateve për punë*" (në vijim, "*Udhëzimi nr. 42*"). Në nenin 6, të këtij Udhëzimi, parashikohet midis të tjerave se, Punëdhënësi mund të përpunoj të dhënat personale të kandidatëve për punë, të cilat janë mbledhur gjatë periudhës së rekrutimit vetëm nëse plotësohen të gjitha kërkesat e mëposhtme: *a) të përdorë të dhënat vetëm nëse kandidati ka dhënë pëlqimin me shkrim për përdorimin e të dhënave edhe për qëllime të tjera; b) të hartojë politikën e privatësisë për të mbajtur të dhënat për këtë qëllim; c) të përcaktojë periudhën kohore të ruajtjes së këtyre të dhënave, etj*. Zyra e Komisionerit vlerëson se, Kontrolluesi nuk ka dokumentuar asnjë nga këto masa konkrete, përpara grupit të kontrollit në kundërshtim me parashikimet e nenit 5 dhe 6, të Ligjit, si dhe të Udhëzimit nr. 42 të Komisionerit.

Lidhur me pretendimin e Kontrolluesit sipas të cilit "*në disa raste është e pamundur të përcaktohet afati i ruajtjes, administrimit dhe përpunimit të të dhënave personale për*

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

klientë apo të dëmtuar" 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 përpunim, duhet të marrë masa për përcaktimin dhe rregullimin e afateve kohore për ruajtjen e të dhënave për secilën kategori të dhënash. Koha e ruajtjes së të dhënave duhet të përcaktohet nga Kontrolluesi, në përputhje me parashikimet ligjore specifike dhe qëllimin e përpunimit.

- Në lidhje me pikën 3 të procesverbalit të konstatimit, Kontrolluesi shprehet se, *"...gjetjet e grupit të inspektimit nuk janë në përputhje me provat e administruara gjatë hetimit administrativ dhe këto gjetje nuk ekzistojnë. Shoqëria Eurosig sh.a. nuk ka vepruar në kundërshtim me nenin 5 dhe 6, të ligjit nr. 9887/2008, si dhe me pikën 10.1 dhe 10.3, të Udhëzimit nr. 11, datë 08.09.2011, "Mbi përpunimin e të dhënave të punonjësve në sektorin privat", i ndryshuar, pasi kamerat e vëzhgimit gjenden vetëm në ambientet e jashtme dhe korridore".*

  Ndërsa lidhur me konstatimin se në dokumentin tip "Kërkesë për dëmshpërblim dëmi", nuk parashikohet asnjë rubrikë që të informojë subjektet e të dhënave mbi përpunimin e të dhënave nuk qëndron, pasi shoqëria Eurosig sh.a. ka vënë në dispozicion të grupit të inspektimit 3 modele tip "Kërkesë për dëmshpërblim" ku parashikohet rubrika përkatëse informuese".

  Pretendimi i Kontrolluesit, sipas të cilit gjetjet e grupit të kontrollit mbi vendosjen e kamerave të vëzhgimit në ambientet e brendshme të zyrave nuk ekzistojnë, është i pasaktë. Gjatë zhvillimit të hetimit administrativ të zhvilluar nga grupi i kontrollit janë administruar në cilësinë e provës materiale fotografi nga sistemi i video-survejimit CCTV. Argumenti i pretenduar nga ana e Kontrolluesit sipas të cilit, kamera e vendosur në sportelin e shitjeve është vendosur për arsye sigurie, pasi aty mbahen likuidime "*cash*" dhe ka arkëtar nuk qëndron pasi, fokusi i kamerës nuk është në sportelin ku bëhen transaksionet, por nga fotografitë dallohet qartë një kamer e vendosur në ambientet e brendshme të zyrës, e cila fokuson punonjësit në pozicionin e vendit ku ata punojnë.

  Njëkohësisht, sjellim në vëmendje se, përveç parashikimeve ligjore, Zyra e Komisionerit ka miratuar dhe akte nënligjore që rregullojnë përpunimin e të dhënave personale të punonjësve në sektorin privat, konkretisht, Udhëzimin nr. 11 të Komisionerit. Në pikën 10.2 të tij, parashikohet midis të tjerave se, "*Kamera e vëzhgimit nuk mund të përdoret për mbikëqyrjen e një punonjësi në vendin e punës*".

  Sa i përket pretendimit të dytë të kësaj pike, Zyra e Komisionerit vlerëson se nuk qëndron, pasi gjatë hetimit administrativ është administruar në cilësinë e provës materiale një kopje e "*Kërkesës për dëmshpërblim dëmi motorik TPL/REA*" më nr. 2495, datë 08.07.2022, i cili në përmbajtje nuk parashikonte asnjë rubrikë që të informojë subjektet e të dhënave mbi përpunimin e të dhënave në kundërshtim me parashikimet e nenit 18 të Ligjit.

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

Gjithashtu, lidhur me pretendimin e Kontrolluesit se, ka vënë në dispozicion të grupit të inspektimit 3 modele tip "*Kërkesë për dëmshpërblim*" të miratuar nga Eurosig sha, nga analiza e përmbajtjes së tyre, nuk rezulton se subjektet e të dhënave informohen mbi të drejtat që ata kanë, në lidhje me qëllimin për të cilin të dhënat personale janë deklaruar.

Nga ana tjetër, referuar *"Kërkesës për dëmshpërblim dëmi motorik TPL/REA, datë 08.07.2022 lidhur me kërkues subjektin A.J., kërkesave model "Për dëmshpërblim dëmi në pronë nga polica TPL ose vullnetare" dhe "Për dëmshpërblim për rastet me pasojë paaftësi e përkohshme/përhershme",* rezulton se në përmbajtje të këtyre kërkesave ekziston edhe rubrika *"Me nënshkrimin e kësaj kërkese për dëmshpërmblim, deklaroj se jap pëlqimin tim që të dhënat e deklaruara më sipër, të administrohen e përpunohen në përputhje me ligjin nr. 9887/2008 për mbrojtjen e të dhënave personale i ndryshuar".*

Referuar pretendimeve të Kontrolluesit si dhe rubrikës së sipërcituar në përmbajtje të "*Kërkesave për dëmshpërblim*", Zyra e Komisionerit vlerëson se, Kontrolluesi ka paqartësi sa i përket konstatimit në lidhje me informimin e subjekteve (neni 18 i Ligjit), nëpërmjet formularëve/kërkesave të sipërcituara.

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. Mos përmbushja e këtij detyrimi nga ana e Kontrolluesit, mund të sjellë pasoja sa i përket privatësisë dhe përpunimit të të dhënave personale të subjekteve të të dhënave. Kur mbledh të dhëna personale, Kontrolluesi duhet të informojë subjektin e të dhënave për fushën dhe qëllimin, për të cilin do të përpunohen të dhënat personale, mënyrën e përpunimit, të drejtën për akses, të drejtën për korrigjim të të dhënave të tij, etj.

Lidhur me pikën 4, të procesverbalit Kontrolluesi shprehet se, "*Për sistemin "E-insure" nuk ka plane specifike, por sigurisht që për teknologjinë e informacionit janë krijuar procedurat standarde të IT-së, në të cilat janë përshkruar masat që merren për sigurinë e të dhënave, procedurat e backup e tjerë.*

Gjatë hetimit administrativ të realizuar në ambientet e shoqërisë Eurosig sh.a. kemi njoftuar se në ambientin e grupit EUROSIG-INSIG është në përfundim të implementimi i një infrastrukture të re virtualizimi dhe paralelisht po ndërton edhe një "site" dytësor në Elbasan për DRS dhe BCP, për të cilën procedurat e implementimit pritet të përfundojnë brenda muajit Janar 2023.

Kontrata e lidhur me subjektin "Infosecurity", i cili do të implementojë dhe do të realizojë auditimin e brendshëm të këtij standardi. Procesi i implementimit ka startuar me 01.12.2022 dhe pritet të përfundojë në 3 (tre) mujorin e parë të vitit 2023.

Duke qenë se shoqëria Eurosig sh.a. është duke kryer procedurat e implementimit SMSI, ju informojmë se jemi duke punuar për mënyrën e kryerjes së raportimeve dhe ruajtjes së logeve sipas standardit ISO 27001. Nga ana tjetër theksojmë se, sistemi "E-insure" ofron

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

një strukturë të mirë organizuar të logeve, nëpërmjet të cilave evidentohet qasje drejt sistemit.

Aktualisht, shoqëria Eurosig ruan backup në fileserver (Strukturë fizike e ndryshme nga ajo e virtualizimit) dhe tape. Nëpërmjet këtij mekanizmi ulet probabiliteti i riskut që mund të vijë si pasojë e dëmtimeve të makinave primare edhe si pasojë e sulmeve kibernetike me enkriptim. Parë nga ana tjetër, ashtu siç është parashtruar edhe më sipër, shoqëria Eurosig është duke punuar për përfundimin e site-ve dytësore për DRS dhe BCS, nëpërmjet të cilave pritet të ofrohet një siguri maksimale.

Në lidhje me numrin e llogarive në "E-insure", për të cilat grupi i inspektimit ka konstatuar rreth 2161 user-a, ju sqarojmë se kjo shifër nuk tregon numrin e llogarive totale. Theksojmë sërish se numri 2161 tregon numrin total të llogarive të çelura që nga momenti që sistemi E-insure është vendosur në zbatim. Për më tepër, në rastet kur operatorët ndryshojnë pozicionin e punës, sistemi E-insure kërkon pezullimin e llogarisë së mëparshme dhe çeljen/hapje e një account të ri (sipas pozicionit të ri të punës), kjo pasi sistemi është ndërtuar në atë mënyrë që të ruajë integritetin e të dhënave. Sqarojmë se numri i llogarive active në E-insure është shumë herë më i vogël dhe përkon me numrin e operatorëve që shoqëria Eurosig sh.a. ka në organigramën e saj.

Njëkohësisht, kërkojmë të theksojmë se struktura aktuale e teknologjisë së informacionit e shoqërisë Eurosig sh.a. ofron një siguri të lartë për ruajtjen e të dhënave personale nga shkatërrime të paligjshme ose humbje aksidentale, me qëllim mbrojtjen e aksesit ose përhapjen e tyre nga persona të paautorizuar. Ndërkohë që edhe masa për sigurinë e të dhënave janë parashikuar edhe me aktet e brendshme të shoqërisë si Rregullorja "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale në shoqërinë Eurosig sh.a", Manuali i Procedurave standarde të Teknologjisë së informacionit, Manual të procedurave standarde të punës në dhomën e serverëve të shoqërisë..".

Sa i përket pretendimit të mësipërm, Zyra e Komisionerit vlerëson se ai nuk qëndron, krijimi i procedurave dhe politikave të përdorimit të infrastrukturës TIK dhe sistemeve elektronike nga Kontrolluesi si dhe zbatimit praktik i 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.

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

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

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

Lidhur me pikën 5, të procesverbalit Kontrolluesi shprehet se, *"...përsa i përket kontratës "tip" të agjentit, sqarojmë se veprimtaria e tyre është e parashikuar dhe e rregulluar me ligjin nr.52/2014 "Për veprimtarinë e sigurimit dhe risigurimit", ku ata licensohen dhe mbajnë përgjegjësi të drejtpërdrejtë për veprimtarinë e tyre dhe sot për sot agjentët me të cilët shoqëria "Eurosig" sh.a. ka marrëdhënie kontraktore janë persona fizik (pra jo një kompani tjetër që kryen përpunim të dhënash).*

Gjithashtu, shoqëria "Eurosig" sh.a. në respekt të ligjit nr. 9887/2008 ka rregulluar marrëdhëniet juridike me agjentët me kontrata të shkruara..."

"Ndërsa lidhur me konstatimin për kontratën me "SINTEZA CO shpk", sqarojmë se "Eurosig" sh.a. ka kontratë shërbimi mirëmbajtje hardware, e cila në asnjë rast nuk akseson sisteme operimi apo të dhëna në infrastrukturën tonë. Sinteza përgjigjet vetëm për gjendjen fizike të UPS dhe Serverave Fizik, ku në rast dështimi të një pjese përbërëse apo të gjithë serverit bëhet zëvendësim vetëm fizik sipas kontratës së nënshkruar. Megjithatë nëse ju e vlerësoni se edhe në këtë rast duhet të ketë një parashikim për mbrojtën e të dhënave, ne angazhohemi të rregullojmë veprimtarinë e mëtejshme mes palëve, duke hartuar një shtesë kontratë në përputhje me parashikimet e kërkesat ligjore dhe Udhëzimin nr. 19...".

Lidhur me pretendimet e ngritura nga ana e Kontrolluesit për kontratat me agjentët, Zyra e Komisionerit vlerëson se, 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.

Nga hetimi administrativ i ushtruar rezulton se agjentët përpunojnë të dhëna personale për llogari të Kontrolluesit. Në këtë kuadër, Kontrolluesi lidhur me kontratën me agjentët, duhet të sigurohet që përpunuesi të garantojë përpunim të ligjshëm dhe të sigurt të të

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

dhënave, në përputhje me nenin 20 të Ligjit dhe me parashikimet e Udhëzimit nr. 19. Nga shqyrtimi i përmbajtjes së kontratës me agjentët, rezulton se, nga ana e Kontrolluesit nuk janë përmbushur detyrimet e sanksionuara në këtë nen.

Lidhur me pretendimet për kontratën midis Kontrolluesit dhe subjektit "SINTEZA CO shpk", në pikën 4, të nenit 3, Ligjit nr. 10273, datë 29.4.2010 "*Për dokumentin elektronik*", parashikohet se, sistem kompjuterik është ai sistem, i cili përbëhet prej pajisjeve, grup pajisjesh apo pajisje të lidhura, ku njëra ose më shumë prej tyre janë vazhduese dhe që kryejnë një proces automatik të transmetimit të të dhënave. Sikurse është parashikuar në kontratë midis palëve, "SINTEZA CO shpk", ndër të tjera, përgjigjet për gjendjen fizike të pajisjeve *Uninteruptible power supply* (UPS) dhe Server-ave Fizik. Në rast të dështimit të njërit prej këtyre komponentëve apo të gjithë serverit është subjekti "SINTEZA CO shpk", në cilësinë e ofruesit të shërbimit, që kryen mirëmbajtjen respektive të këtyre komponentëve, çka rezulton se, është përgjegjës për garantimin e konfidencialitetit, integritetit dhe disponueshmërisë së sistemeve (si dhe të dhënave që ato përmbajnë) sipas proceseve të punës respektive. Për rrjedhojë, Zyra e Komisionerit vlerëson se pretendimet e Kontrolluesit nuk qëndrojnë.

Në lidhje me pikën 6 të procesverbalit të konstatimit, në të cilën janë ngritur pretendime për mangësi në deklarim sa i përket rubrikave të formularit, sqarojmë se: "*Për rubrikën 1.2 "Ndryshimi i personit të kontaktit", ju informojmë se ky detyrim është përmbushur nga ana jonë nëpërmjet shkresës nr. 6214 prot., datë 07.12.2022. Po ashtu, sipas ligjit aktual në fuqi, ligjit nr. 9887/2008, Personi i Kontaktit (DPO) nuk përbën një detyrim ligjor për kontrolluesin.*

Përsa i përket rubrikës 3.1, "Kategoritë e subjekteve të të dhënave personale që përpunohen", shoqëria Eurosig sha ka deklaruar se përpunon të dhëna personale për subjekte si: klientë, nëpunës, punëmarrës, aksionerë dhe anëtarë. Ndërsa në rubrikën 4.1 "Kategoritë e të dhënave personale që përpunohen" shoqëria ka deklaruar se përpunon të dhëna personale të tilla si: situata ekonomike financiare, të dhëna identifikimi, adresa, karakteristika të banesës, numri i sigurimit shoqëror, formimi-diplomat-medaljet, foto, numri personal identifikimit, jeta personale, imazhe ndërmjet kamerës CCTV. Aktualisht, shoqëria Eurosig sha vlerëson se këta subjekte përbëjnë kategorinë e personave për të cilët shoqëria përpunon të dhëna apo kategoritë e të dhënave personale janë të përmendura, megjithatë shoqëria Eurosig sh.a. mbetet e hapur ndaj sugjerimeve dhe propozime të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, për përmirësimin e këtyre dy pikave..."

Lidhur me pretendimet e Kontrolluesit mbi plotësimin e detyrimit për Njoftim dhe përditësimin e tij, Zyra e Komisionerit vlerëson se, për rubrikën 1.2 "*personi i kontaktit*", Kontrolluesi nëpërmjet emalit të datës 13.12.2022, ka njoftuar për ndryshimin e personit të kontaktit, ndërkohë që hetimi administrativ ndaj Kontrolluesit ka nisur në zbatim të Urdhrit nr. 198, datë 10.11.2022. Neni 21 i Ligjit parashikon se, "*Çdo kontrollues duhet të njoftojë Komisionerin për përpunimin e të dhënave personale, për të cilat është përgjegjës. Njoftimi duhet të bëhet para se kontrolluesi të përpunojë të dhënat për herë*

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

të parë ose kur kërkohet ndryshimi i gjendjes së njoftimit të përpunimit, sipas nenit 22 të këtij ligji, të njoftuar më parë".

Lidhur me pretendimet e Kontrolluesit se, *sipas ligjit aktual në fuqi, ligjit nr. 9887/2008, Personi i Kontaktit (DPO) nuk përbën një detyrim ligjor për kontrolluesin,* 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 për mbrojtjen e të dhënave personale. Formatet e miratuara nga autoriteti përgjegjës (*të tilla si: formularit të njoftimit*), janë të detyrueshme për tu zbatuar.

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 pretendimin e Kontrolluesit se *"...sa i përket rubrikës 3.1: "Kategoritë e subjekteve të të dhënave personale që përpunohen" dhe rubrikës 4. 1 "Kategoritë e të dhënave personale që përpunohen "shoqëria Eurosig vlerëson se këta subjekte përbëjnë kategorinë e personave për të cilët shoqëria përpunon të dhëna apo kategoritë e të dhënave personale janë të përmendura..."* Zyra e Komisionerit vlerëson se ky pretendim nuk qëndron, Kontrolluesi ka informuar për proceset përpunuese që kryen por, duhet që të njoftojë për të gjitha kategoritë e subjekteve dhe kategoritë e të dhënave, në referencë të aktivitetit që kryen.

Konkretisht, në rubrikën 3.1 të Formularit nuk është parashikuar kategoria "*vizitor*", të dhënat e të cilëve përpunohen nëpërmjet sistemeve të video-survejimit, ndërsa në rubrikën 4.1 të Formularit nuk është njoftuar për kategoritë e të dhënave që Kontrolluesi përpunon për këto subjekte, grupi i kontrollit ka siguruar prova që vërtetojë kryerjen e këtij përpunimi nga ana e Kontrolluesit.

Lidhur me pikën 7, të procesverbalit Kontrolluesi shprehet se, *"...përsa i përket konstatimeve në lidhje me rregulloren për mbrojtjen e të dhënave, vlerësojmë të sqarojmë se kjo rregullore, e miratuar në datë 31.10.2022, u realizua pas konstatimit të nevojës për përmirësim, dhe shoqëria "Eurosig" sh.a. ndërmori një proces të mirëfilltë konsultimi të brendshëm me strukturat dhe drejtoritë përkatëse të shoqërisë, pikërisht duke pasur në konsideratë se rregullorja duhet të ishte më e detajuar e konkrete, sipas Udhëzimeve dhe kërkesave të Zyrës së Komisionerit (konstatuar nga gjetjet/shkeljet e konstatuara në subjekte të tjera të kontrolluara nga vendimet e Zyrës së Komisionerit). Në këtë kuadër, shoqëria "Eurosig" sh.a. ka parashikuar një sërë ndryshimesh në këtë rregullore (të tilla si: procedura organizative specifike; deklarata e konfidencialitetit; masa konkrete për sigurinë e të dhënave, etj., në nenet 6,7,8,9,10,12,13,16 e vijues..").*

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

Zyra e Komisionerit vlerëson se, dispozitat e cituara nga Kontrolluesi në Rregulloren "*Për mbrojtjen e të dhënave personale*" janë të përgjithshme dhe parimore por nuk ofron asnjë rregullim konkret të proceseve përpunuese të Kontrolluesit lidhur me detyrimet e ligjit. Konkretisht, në nenin 8 të Rregullores parashikohen kriteret e përpunimit të të dhënave personale. Megjithatë në pikën 1 të kësaj dispozite është dhënë një përcaktim i përgjithshëm për punonjësit e strukturave të Eurosig sha, ndërkohë që është detyrim që të bëhet një ndarje, në përgjegjësi të kategorive të punonjësve të cilët kanë detyrime konkrete lidhur më këtë pikë. Në nenin 9 të Rregullores parashikohet përpunimi i të dhënave sensitive. Në pikën 1 të kësaj dispozite u njihet si atribut i përpunimit të të dhënave personale për çdo punonjës të Eurosig sha, pa parashikuar si do të rregullohet ky përpunim. Në pikën 2, të nenit 9 të Rregullores parashikohet përpunimi i të dhënave sensitive të tilla si, "*jeta seksuale*", ndërkohë që nuk kuptohet se kujt të dhëne personale i referohet konkretisht Kontrolluesi, duke marrë në konsideratë faktin se një deklarim i tillë nuk është parashikuar në rubrikën e të dhënave sensitive të Formularit të Njoftimit dhe as është përmendur apo dokumentuar një përpunim i tillë nga ana e Kontrolluesit gjatë zhvillimit të hetimit administrativ. Në nenin 10 të Rregullores parashikohen procedurat për transferimin ndërkombëtar të të dhënave personale.

Në nenin 19 të Rregullores janë parashikuar rregulla për Drejtorinë e Teknologjisë së Informacionit. Në pikën dy të kësaj dispozite pretendohet se drejtoria e IT-së mban në gatishmëri sisteme dytësore (*disaster recovery*), megjithatë nga hetimi administrativ i ushtruar pranë Kontrolluesit nuk u dokumentua një procedurë e tillë. Në nenin 20 të Rregullores pretendohet se, përdorim i pajisjeve elektronike që përpunojnë të dhëna personale kryhet nga personel i trajnuar, dhe se trajnimi i personelit bëhet nga specialistët e IT me strukturën përgjegjëse, ndërkohë që një pretendim i tillë nuk u arrit të dokumentohet nga Kontrolluesi. Madje, grupi i kontrollit e ka konstatuar shkelje faktin e mungesës së trajnimit të stafit lidhur me mbrojtjen e të dhënave personale. Në nenin 23 të Rregullores trajtohet mbrojtja e dokumenteve dhe procedura e ndjekur për sekretimin e tyre. Përmbajta e kësaj dispozite është e paqartë duke marrë në konsideratë faktin se klasifikimi i dokumenteve bëhet sipas parashikimeve të një legjislacioni specifik dhe ka një autoritet kompetent të ngarkuar më këtë detyrë.

Për sa më sipër, Zyra e Komisionerit vlerëson se, mangësitë e përmendura (*të cilat nuk janë shteruese pasi nga ana e grupit të kontrollit janë konstatuar edhe të tjera*) provojnë qartësisht se, masat e parashikuara në Rregullore janë fiktive, të paqarta, të pa dokumentuara dhe të pamjaftueshme, për rrjedhojë kjo Rregullore konsiderohet në kundërshtim me parashikimet e nenit 27 të Ligjit dhe Vendimin nr. 6 të Komisionerit.

Lidhur me pikën 8, të procesverbalit Kontrolluesi shprehet se, ..."*Eurosig" sh.a. ka kohë që ka ndërmarrë një fushatë dhe hapa konkrete për përmirësimin e gjithë standardeve dhe politikave të saj të brendshme lidhur me mbrojtjen e të dhënave personale dhe sigurinë e sistemeve. Sikundër kemi sqaruar shoqëria "Eurosig" sh.a. ka marrë masa konkrete lidhur me sigurinë e informacionit, duke angazhuar edhe ekspertë të jashtëm. Po ashtu, ka ngritur grup pune pikërisht për sigurinë e informacionit (Urdhri nr. 560, datë 12.09.22 "Për ngritjen e grupit të punës për hartimin e procedurave për sigurinë e*

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

Informacionit në shoqërinë "Eurosig" sh.a.", bashkëlidhur). Pra, shoqëria ka ndërtuar strukturën për SMSI dhe nga fillimi i dhjetorit 2022 sipas kontratës me "INFOSECURITY" ka filluar implementimi dhe trajnimi i stafit për këtë proces (kontrata bashkëlidhur).

Në përfundim, vlerësojmë të theksojmë se shoqëria ka predispozitën dhe angazhohet për përmirësimin e standarteve që aplikon me qëllim mbrojten sa më të mirë të të dhënave personale, ndaj kërkojmë edhe bashkëpunimin e Zyrës së Komisionerit për të na asistuar në vijimësi (veçanërisht kur të miratohet projektligji i ri), duke qenë se jo vetëm është struktura më e specializuar, por ka treguar gatishmëri dhe qasje transparente, mendje-hapur dhe bashkëpunuese...".

Lidhur më këtë pretendim rezulton se, që nga momenti i fillimit të hetimit administrativ, Kontrolluesi nuk ka provuar se ka ndërmarrë masa konkrete në kuadër të trajnimit të punonjësve që kanë akses dhe përpunojnë të dhëna personale lidhur me legjislacionin në fuqi për mbrojtjen e të dhënave personale. Grupi i kontrollit konstaton mosplotësim të detyrimeve në lidhje me ngritjen, administrimin dhe mirëmbajtjen e sistemit të menaxhimit së sigurisë së informacionit (SMSI) lidhur me mbrojtjen e të dhënave personale, të parashikuara në Udhëzimin nr. 47.

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:

Sa më sipër, në zbatim të neneve 5, 6, 18, 20, 21, 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, për të gjitha proceset e përpunimit në përputhje me germën *"d"*, të pikës 1, të nenit 5 të Ligjit;

2. Kontrolluesi, në zbatim të neneve 5 dhe 6 të Ligjit, Udhëzimit nr. 3 dhe Udhëzimit nr. 11 të Komisionerit, të marrë masa për ripozicionimin e planit të monitorimit përmes sistemit CCTV;

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

3. 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.;

4. Kontrolluesi, të marrë masa për të rishikuar kontratat me përpunuesit duke specifikuar detyrimet midis palëve, dhe të monitorojë në vijimësi zbatimin e detyrimeve të përcaktuara në marrëveshjet me përpunuesit, sipas dispozitave të parashikuara në nenin 20 të Ligjit dhe Udhëzimin nr. 19 të Komisionerit;

5. 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;

6. 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, mënyrat e përpunimit të të dhënave, të drejtat e subjekteve të të dhënave, garantimin e konfidencialitetit etj., në funksion të aktivitetit të tij, për çdo proces përpunimi;

7. 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;

8. 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;

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

(i) Menjëherë, detyrimet e treguara në pikën 2 më sipër;

(ii) brenda 15 (pesëmbëdhjetë) ditëve, detyrimet e përcaktuara në pikat 1, 3, 4 dhe 5;
(iii) brenda 30 (tridhjetë) ditëve, detyrimet e përcaktuara në pikën 6 më sipër;

(iv) brenda 45 (dyzetë e pesë) ditëve, detyrimet e përcaktuara në pikën 7 më sipër.

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

10. Kontrolluesi të njoftojë Komisionerin për masat e marra;

11. 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

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

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 15.02.2023.

KOMISIONERI

Besnik Dervishi

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