R E P U B L I K A E S H Q I P Ë R I S Ë

KOMISIONERI PËR TË DREJTËN E INFORMIMIT DHE MBROJTJEN E TË DHËNAVE PERSONALE

DREJTORIA E PËRGJITHSHME PËR MBROJTJEN E TË DHËNAVE PERSONALE

DREJTORIA E HETIMIT SEKTORIAL DHE SIGURISË SË TË DHËNAVE

Nr.1135/3 prot. Tiranë më 24.11.2022

VENDIM

Nr. 52, datë 24.11.2022

PËR KONTROLLUESIN "DREJTORIA E PËRGJITHSHME E TATIMEVE"

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 *"Drejtoria e Përgjithshme e Tatimeve"* (në vijim, *"Kontrolluesi"* dhe/ose *"DPT"*),

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 203, datë 22.12.2021 të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim, *"Komisioneri"*), u krye hetimi administrativ pranë Kontrolluesit, me objekt:

- Verifikim lidhur me ligjshmërinë e përpunimit të të dhënave personale të subjekteve të të dhënave *"nëpunës/punëmarrës",* nisur nga informacionet e publikuara në median elektronike.

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

1. Më datë 22.12.2021, media të ndryshme publikuan një lajm me titull *"Skandal me të dhënat private, pagat e mbi 637 mijë shqiptarëve dalin në publik"*, (lajmi gjendet në lidhje të ndryshme në internet), nëpërmjet të cilit bëjnë me dije se qarkullon në aplikacionin *Whatsapp* një databazë (bazë të dhënash) me të dhënat personale të mbi 637 mijë subjekteve të të dhënave, nëpunës/punëmarrës të sektorit publik dhe atij privat.

Zyra e Komisionerit administroi një kopje të bazave të të dhënave (RROGAT-JANAR2021.xlsx, RROGAT-PRILL2021.xlsx), në të cilat rezultojnë të përpunuara të dhënat personale të 637,139 (*gjashtëqind e tridhjetë e shtatë mijë e njëqind e tridhjetë e nëntë*) dhe 694,470 (*gjashtëqind e nëntëdhjetë e katër mijë e katërqind e shtatëdhjetë*) subjekteve të të dhënave (në vijim, *"Baza e të Dhënave*"). Këto Baza të Dhënash rezultojnë të kenë qarkulluar nëpërmjet kanaleve të ndryshme komunikimi.

Nga të dhënat e materialeve elektronike të Bazës së të Dhënave, konstatohet se materiali elektronik RROGAT JANAR 2021.xlsx është krijuar më datë 24.02.2021, ora 10:33 AM, me përmasa 47,859,991 *bytes*, ndërsa materiali elektronik RROGAT-PRILL2021.xlsx është krijuar më datë 26.04.2021, ora 11:08 AM, me përmasa 134,714,708 *bytes*.

Baza e të Dhënave për materialin elektronik *"RROGAT-JANAR2021.xlsx"* përbëhet nga kategori me të dhëna si vijon:

1. Numër rendor (Nr.);
2. Nr. i identifikimi (NID) subjekti të dhënash;
3. Emër;
4. Mbiemër;
5. Emër Mbiemër, i plotë;
6. Nr. i identifikimit (NUIS) subjekti tregtar / publik;
7. Emri i subjektit tregtar/privat;
8. Qyteti;
9. Paga e nëpunësit;
10. Pozicioni i punës;
11. Koha e punës.

Baza e të Dhënave për materialin elektronik *"RROGAT-PRILL2021.xlsx"*, është e organizuar në dy faqe (*"sheet1"* dhe *"sheet2"*) dhe përmban kategoritë me të dhënat si vijon:

1. Numër rendor (Nr.);
2. Nr. i identifikimit (NID) subjekti të dhënash;
3. Emër;
4. Mbiemër;
5. Emër Mbiemër, i plotë;
6. Nr. i identifikimit (NUIS) subjekti tregtar / publik;
7. Emri i subjektit tregtar/privat;
8. Qyteti;
9. Paga e nëpunësit;
10. Pozicioni i punës;
11. Koha e punës;
12. Nr. telefoni.

Nga kërkimet e ekspertëve të teknologjisë së informacionit dhe komunikimit (TIK) të Zyrës së Komisionerit, rezulton e pamundur të identifikohet, në të dhënat elektronike të Bazës së të Dhënave, krijuesi dhe/ose origjina elektronike e këtij dokumenti.

Në vijim, është konstatuar një përhapje masive e paligjshme e Bazës së të Dhënave, ndër të tjera nëpërmjet aplikacionit Whatsapp dhe faqeve të ndryshme të internetit dhe medias audiovizive, shkak për të cilin Zyra e Komisionerit i është drejtuar Autoritetit të Komunikimeve Elektronike dhe Postare (AKEP) dhe AMA për bllokimin e menjëhershëm të tyre, si dhe fillimin e procedimit ligjor të personave që zotërojnë/posedojnë këto faqe interneti, në të cilat rezulton të publikohen të dhënat personale të shtetasve që supozohen të jenë marrë nga Baza e të Dhënave.

Rezulton e qartë se Baza e të Dhënave përmban të dhëna personale të subjekteve të të dhënave, siç përkufizohen në pikën 1 të nenit 3 të Ligjit, sipas së cilës e dhënë personale është çdo informacion në lidhje me një person fizik, të identifikuar ose të identifikueshëm, direkt ose indirekt, në veçanti duke iu referuar një numri identifikimi ose një a më shumë faktorëve të veçantë për identitetin e tij fizik, fiziologjik, mendor, ekonomik, kulturor apo social.

Përhapja e të dhënave, si formë e posaçme përpunimi (sipas përkufizimit në pikën 12 të nenit 3 të Ligjit), duhet të realizohet në përputhje me parimet dhe kriteret e neneve 5 dhe 6 të ligjit në fjalë.

Referuar pikës 20 të nenit 3 të Ligjit, përhapja e të dhënave nënkupton komunikimin e informacionit për të dhënat personale palëve të papërcaktuara, në çfarëdo forme, edhe përmes vënies në dispozicion ose për konsultime.

Sa më sipër, nisur nga shkalla jashtëzakonisht e gjerë e përpunimit të të dhënave në Bazën e të Dhënave, në kundërshtim me parimet dhe kriteret e përpunimit të të dhënave personale, Zyra e Komisionerit vlerëson se përhapja masive e saj, përbën cenim të rëndë të jetës private dhe të drejtës së shtetasve për mbrojtjen e të dhënave të tyre personale, që në fjalorin ligjor ndërkombëtar njihet si "*personal data breach*".

2. Hetimi administrativ pranë Kontrolluesit është iniciuar kryesisht nga Zyra e Komisionerit bazuar në sa më sipër. Gjatë hetimit është Konstatuar se, detyrat funksionale të administratës tatimore, të kryesuar nga DPT, përfshijnë, ndër të tjera, mbledhjen e të ardhurave tatimore, si dhe kontributeve të sigurimeve shoqërore dhe shëndetësore, mbajtjen e Regjistrit Qendror të Llogarive Bankare, etj.

   Kontrolluesi administron detyrimet tatimore në Republikën e Shqipërisë në nivel qendror për tatimet dhe taksat e përcaktuara në ligjin nr. 9920, datë 19.05.2008 *"Për procedurat tatimore në Republikën e Shqipërisë"* i ndryshuar, si dhe kontributet e sigurimeve shoqërore e shëndetësore të përcaktuara në ligjin nr. 9136, datë 11.09.2003 *"Për mbledhjen e kontributeve të detyrueshme të sigurimeve shoqërore e shëndetësore në Republikën e Shqipërisë"* i ndryshuar.

Gjithashtu, DPT përgatit dhe miraton planin strategjik të objektivave dhe synimeve kryesore të administratës tatimore qendrore për një periudhë afatshkurtër, afatmesme dhe afatgjatë si edhe monitoron zbatimin rigoroz të tij nga të gjitha drejtoritë e Drejtorisë se Përgjithshme të Tatimeve dhe nga të gjitha Drejtoritë Rajonale Tatimore.

3. Kontrolluesi mbledh dhe përpunon të dhëna personale për kategoritë e subjekteve të të dhënave:
   a) tatimpagues, nëpunës të administratës tatimore, agjentë tatimorë, agjentë të mbajtjes së tatimit në burim, si dhe persona të tjerë të përcaktuar nga legjislacioni tatimor;
   b) personat e ngarkuar për të paguar, mbajtur, deklaruar dhe transferuar në Buxhetin e Shtetit kontributet për sigurimet shoqërore dhe shëndetësore;
   c) personat që paguajnë kontributet për sigurimet shoqërore dhe shëndetësore, për sa i përket pagesës dhe mbledhjes së kontributeve;
   ç) personat që paguajnë taksa dhe tarifa vendore, për aq sa nuk rregullohen me ligjin nr. 9632, datë 30.10.2006, *"Për sistemin e taksave vendore"* i ndryshuar, etj.

   Përpunimi i të dhënave kryhet në mënyrë manuale dhe elektronike. Sistemi elektronik i tatimeve, shërben si një sistem i automatizuar për ofrimin e shërbimeve për administratën tatimore dhe tatimpaguesit, duke i ardhur në ndihme këtyre të fundit për të përmbushur detyrimet ligjore sipas legjislacionit në fuqi.

   Nga krahasimi i kryer me të dhënat që DPT përpunon nëpërmjet sistemit elektronik për kategorinë e subjekteve të të dhënave *"nëpunës/punëmarrës",* me ato të Bazës së të Dhënave që kanë rrjedhur dhe janë publikuar në platformat e ndryshme teknologjike, rezulton se të dhënat përkojnë me 10 kategori, të cilat janë:

   1. Nr. i identifikimit (NID) të subjektit të të dhënave;
   2. Emër;
   3. Mbiemër;
   4. Emër Mbiemër, i plotë;
   5. Nr. i identifikimit (NUIS) të subjektit tregtar/publik;
   6. Emri i subjektit tregtar/privat;
   7. Qyteti;
   8. Paga e nëpunësit;
   9. Pozicioni i punës;
   10. Koha e punës.

4. Veprimtaria e institucionit realizohet, ndër të tjera, nëpërmjet sistemit elektronik *"e-Taxation".* Nga verifikimi rezulton se baza e të dhënave e këtij sistemi përbëhet nga:
   - Baza e të dhënave të sistemit *"e-Taxation",* e cila është ndërtuar me qëllim regjistrimin e të dhënave të tatimpaguesve në Republikën e Shqipërisë, për individ apo biznese;

- Baza e të dhënave të sistemit *"e-Taxation"* është e ndërtuar në SQL Server;
- Emri i databazës është *"e-Taxation"*;
- Aksesimi i databazës nga përdoruesit e jashtëm, kryhet nëpërmjet një lidhje me VPN;
- VPN ofron konfidencialitet të të dhënave pasi ato enkriptohen gjatë transmetimit;
- Të dhënat nuk mund të lexohen pa pasur çelësin përkatës të dekriptimit;
- VPN përdor protokollin SSL e cila e bën atë të sigurt për tu përdorur;
- OS Microsoft Windows Server 2012;
- Apache tomcat;
- Infinica Process Engine ;
- Microsoft SQL Server 2012 me karakteristikat e mëposhtme:
    - ✓ database Engine Services (Shërbimet për motorin e databazës);
    - ✓ analysis services;
    - ✓ integration services;
    - ✓ reporting services;
    - ✓ SQL Server Data Tools and Client Tools Connectivity.
- Kjo bazë të dhënash përdor modelin Full Recovery, në mënyrë që çdo veprim i kryer mbi databazën të ruhet në log.

Sistemi tatimor *"e-Taxation"* përbëhet nga elementet CORE, PUBLIC, Integration Services & WebServices & Replication Services dhe FTP.

CORE: është sistemi i brendshëm i cili menaxhohen bazën kryesore të të dhënave. Ky sistem është përgjegjës për të gjitha veprimet, si menaxhimi i deklaratave, procesimi i pagesave, kontabiliteti, regjistrimi, menaxhimi i çështjeve, kontrollin, menaxhimin e riskut, menaxhimi i dokumenteve, menaxhimi i sigurisë, etj.

PUBLIC: është portali që përdoret nga tatimpaguesit për të deklaruar detyrimet dhe për të menaxhuar të dhënat e tyre. Ky sistem komunikon me sistemin CORE nëpërmjet Integration Services, *Web* Services, dhe Replication Services. Nëpërmjet shtresës integruese, sisteme të tjera furnizohen me të dhëna, duke përfshirë, platformën raportuese, sistemin "*m-Tax"*, dhe sistemin e kasave fiskale.

DIS*:* është Departament Integration Server që shërben për të ofruar dhe konsumuar shërbime sipas koncepteve të Service Oriented Architecture (SOA) për palët e treta si Drejtoria e Përgjithshme e Gjendjes Civile (DPGJC), Qendra Kombëtarë e Biznesit (QKB), Instituti i Sigurimeve Shoqërorë (ISSH), Doganat, portali e-Albania.

Sistemi *"e-Taxation"* (site primar dhe site dytësor) hostohet në ambientet e Agjencisë Kombëtare të Shoqërisë së Informacionit (AKSHI), dhe të gjitha Drejtoritë Rajonale kanë mundësi që ta aksesojnë nëpërmjet një lidhje me VPN.
Zgjidhja teknike ndërtohet sipas modelit të tipit *"dështimit"* të sistemit (Failover), i cili është implementuar nëpërmjet pajisjeve *"load balancer Server".* Nëpërmjet këtij *"clusteri"* garantohet disponueshmëri e lartë (High Avaibility) për të gjitha shërbimet

që hostohen në të. Sistemi konsiston në makina virtuale, me disponueshmëri të lartë, të mbështetura në modelin *"Hyper-V Failover Cluster-in"*.

Serverët janë të konfiguruar sipas modelit "*Microsoft për Virtualizim*" dhe *"Failover"*. Komponentët përbërës të infrastrukturës mbështetëse TIK përfshijnë: Firewall , Hardware Load Balancer , Core Switches, Aggregation Switches etj.

Duke qenë së niveli i kërkuar i sigurisë duhet të përcaktohet në përputhje me objektivat e sigurisë së informacionit nëpërmjet parametrave të integritetit, konfidencialitetit dhe disponueshmërisë, rezulton që *"e-Taxation"* duhet të ketë një nivel të lartë sigurie të nivelit L-D2I3K2, referuar dhe ofertës teknike të cituar në kontratën e mirëmbajtjes së sistemit *"e-Taxation"*.

Në sistemin *"e-Taxation"* kryhen ndërveprime të të dhënave personale me sisteme të tjera nëpërmjet web service-ve si: me sistemet e Drejtorisë së Përgjithshme të Gjendjes Civile (DPGJC), Qendrës Kombëtarë të Biznesit (QKB), Institutit të Sigurimeve Shoqërorë (ISSH), portalit unik qeveritar e-Albania dhe me sistemin e Fiskalizimit, nëpërmjet platformës qeveritare të ndërveprimit.

Të dhënat parësore që krijohen në sistemin *"e-Taxation"* nga Kontrolluesi, janë si më poshtë vijon:

Nr.	Sipas Kategorisë
1	Menaxhimi i çështjeve për administratën tatimore
2	Statistika
3	Regjistrimi
4	Borxhet
5	Listë pagesat
6	Parapagimet
7	Librat
9	Ndihma Financiare
10	Rikalkulim
11	Risk
12	Vlerësimi Alternativ
13	Deklaratat
14	Diva
18	Performanca e aplikimit
19	Raporte Thesari (mbledhje te ardhurash)

Infrastruktura e sigurisë së sistemit është parashikuar sipas niveleve të roleve dhe të drejtat dhe politikat e aksesimit të të dhënave, për të përcaktuar dhe kontrolluar se çfarë veprimesh mund të kryejnë përdoruesit në sistemin *"e-Taxation"*. Dhënia e të

drejtave një përdoruesi, ndër të tjera, duhet të lejojë kontrollin e aksesit në ndërfaqe ose në funksionalitete të ndryshme, duke dhënë mundësitë për të përshtatur strukturën e *menu*-ve për secilin përdorues. Menaxhimi i përdoruesve të sistemit është planifikuar të kryhet nga përdoruesit me rol *"Administrator"*. Gjatë krijimit të një përdoruesi të ri, përcaktohet edhe roli i tij. Roli në sistem lidhet me një profil të caktuar sipas funksionaliteteve të punës. Kur një përdoruesi i caktohet një rol, automatikisht i jepen të drejta mbi profilin e këtij roli.

Përdoruesit e sistemit elektronik të tatimeve janë të gjithë përdoruesit e identifikueshëm nga ky sistem, të cilët aksesojnë funksionalitetet e tij, me anë të llogarisë së tyre *"Single Sign On"*, me qëllim kryerjen e funksioneve të avancuara si mbledhja, inspektimi dhe kontrolli i detyrimeve tatimore, krijimi i deklaratave të përgjegjësive të ndryshme tatimore, dorëzimi i listëpagesave, etj. Ky grup përbëhet nga nëngrupet e mëdha si më poshtë:

1. **Tatimpagues** - janë përdoruesit të cilët në bazë të legjislacionit në fuqi duhet të deklarojnë përgjegjësitë e tyre tatimore dhe të paguajnë detyrimet lidhur me të, duke ngarkuar në sistem dokumentacionin përkatës.
2. **Administrata Tatimore** - janë përdoruesit të cilët duke zbatuar legjislacionin tatimor në fuqi, duhet të monitorojnë, vlerësojnë dhe kur është e nevojshme të verifikojnë, çdo sjellje të çdo tatimpaguesi, që nuk zbaton ose keq zbaton me dashje apo jo, përmbushjen e detyrimeve ligjore.

Rolet e sistemit kanë nivele të ndryshme aksesi, në varësi të specifikave dhe të drejtave që ata kanë në sistem. Më poshtë shpjegohen rolet që kanë përdoruesit për të aksesuar sistemin (informacioni i dërguar me postë elektronike nga punonjësit e Njësisë së Teknologjisë së Informacionit e të Komunikimit pranë DPT - NJTIK):

Përdorues total të sistemit *"e-Taxation"*.

	Nr	Nr Users	Nr Active Users
C@TS	CATS UI	2,146	1,445
	CATS DB	52	43
	SubTotal	***2,198***	**1,488**
eFILING	eFILING UI	525,292	524,939
	eFILING DB	20	15
	SubTotal	***525,312***	524,954
	Total	**527,510**	**527,930**

Rolet sipas kategorive në sistem janë si më poshtë (dërguar me postë elektronike nga punonjësit e NJTIK pranë DPT):

ExportFile
RiskExportData
Administrator TIK
VAT_REFUND_COPY_EXPORT
ShikoRaportetMbledhjaTeArdhurave
VAT_Refund_Deputy_Director_General
VAT_Refund_Deputy_General_Director
VAT_REFUND_OFFICE_INSPECTOR
VAT Refund - Tirane Audit Director PROT
VAT Refund - Tirane Audit Director SIPT
VAT_REF_INVESTIGATION_inspector
vat_refund_Drejtor risku
VAT_Refund_Director
VAT_Refund_Risk_Inspector
VAT Refund - Audit Director DRT
BKH
eTax_Support_Staff
FinancialAid2020
DPD Users
AuditVieë
Dpppp Users
AspVieëData
DebtRegionalAgreement
HetimiDrtDirector
HetimiDptDirector
RiskPerformance
RiskAnalise
PaymentDpt
HetimiTatimor
AuditMgmtDpt
TaskForceChief
TaskForce
VieëTaxpayer
CaseAdmin
CaseManagementAdmins
CourtInspector
CourtChief
RefundApproveDptFinal
RefundApproveDpt2
RefundApproveDpt1
Registraton GDT
AdminDPT
RefundAprovelFinal

RefundAprovel2
RefundAprovel1
Administrator DRT
ReturnsheetsGeneration
AuditKLSH
HelpDesk
CaseTaxpayerServiceDirector
AppealsChief
DebtRegionalInspector
DebtRegionalChief
SpotVerificationChief
SpotVerification
TP_Registration_Checks
TP_Registration_Final
TP_Registration_Approval
VieëData
Registration_Amendment
TaxpayerService
CaseTaxpayerService
RegionalDirector
AuditDirector
AuditChief
AuditInspector
DebtMgmtRegional
AssessmentRegional
AuditRegional
AccountingRegional
Legal
Investigations
Appeals
Assessment
Technical
Debt Management
Audit
Risk Management
Accounting
Return Sheets
Reports
TaxpayerRegistration
Administrators

Konstatohet se në dokumentacionin e ofertës teknike të operatorit ekonomik mbi mirëmbajtjen e sistemit *"e-Taxation",* të kontratës së shërbimit me nr. 3339 prot.,

datë 12.05.2021, me objekt *"Mirëmbajtja e sistemit e-Taxation, për DPT",* janë planifikuar disa veprime teknike në rast se ka dështime të serverit / sistemit / aplikacioneve dhe bazës së të dhënave, kur kalojnë në një gjendje jo konsistente. Për të shmangur këto situata është parashikuar të ndiqet një veprimtari aktive dhe proaktive në vazhdimësi, si dhe automatizim periodik të backup-it/recover-it.

Kur krijohet një *backup* i ri, *backup*-et e mëparshme presupozohet të jenë të disponueshëm dhe mund të përdoren për procedurat e rikthimit të të dhënave në rast dështimi. Sidoqoftë, në varësi të madhësisë së skedarëve të *backup*-eve dhe kapacitetit të disponueshëm për ruajtjen e tyre, duhet të procedohet me rutina të përditshme për mirëmbajtjen e tyre. Këto rutina duhet të synojnë ruajtjen e backup-eve të vjetra në hapësira të veçanta ose fshirjen e backup-eve të vjetra të papërdorura, për të krijuar hapësira të lira. Backup-et duhet të ruhen në një vend që ofron siguri fizike dhe akses të kontrolluar. Mjedisi i ruajtjes së backup-it të mediave si *"hard drive", "disk-s"* apo *"tape-s/ storage",* duhet të jetë në një arkiv të organizuar elektronik. Për menaxhimin e hapësirës së alokuar nga backup-et, ripërdorimin apo shkatërrimin e tyre, duhet të ndiqen procedura të mirë përcaktuara, të ndjekura nga protokollet që do të nënshkruhen.

Gjithashtu, siguria e aplikacionit të sistemit në lidhje me *logimet*, sipas projektit teknik, duhet të zgjidhet teknikisht nëpërmjet:

1. IIS Logging (për çdo veprim të përdoruesit nga ndërfaqja);
2. Error Logging (në databazë);
3. Tabela Historike në databazë për të gjurmuar ndryshimet në të dhëna;
4. Loge të ekzekutimeve të raporteve;
5. Loge SQL Audit mbi veprimet e përdoruesve në nivel databaze (select statement);
6. Windows Logging në Event Viewer;
7. Transaction Logs të SQL Server (Full Recovery Mode).

Shtresa e integrimeve/ndërveprimeve nëpërmjet shërbimit web-service është një komponent i rëndësishme i sistemit *"e-Taxation".* Kjo shtresë ofron mundësi integruese midis komponentëve të sistemit dhe në të njëjtën kohë, edhe me sisteme të tjera të palëve të treta. Duke qenë së "*e-Taxation*" është i integruar në Government Gateway (GG), ai mund të komunikojë me sisteme të tjera për të marrë dhe për të dhënë informacione. Integrimet me sistemet e jashtme janë të rëndësishme pasi gjatë popullimit të sistemit me të dhëna, një nga hapat është marrja e të dhënave nga sistemet e jashtme. Integrimi me sisteme të tjera si DPGJC, QKB, ISSH, Doganat, e-Albania etj., bën të mundur ndërveprimin e të dhënave në formën hyrëse/dalëse (parësor dhe dytësor). Në këtë mënyrë, bëhet e mundur lidhja e shtresës së prezantimit me shtresën e bazës së të dhënave. Përveç integrimeve me sistemet e tjera, ka dhe web-service të cilat kryhen midis vetë komponentëve të sistemit "*e-Taxation*".

Nga kontrata e mirëmbajtjes rezulton se sistemi është ndërtuar mbi bazë të moduleve/nënsistemeve kryesore. Modulet kryesore të sistemit listohen si më poshtë:

- Modulet e Regjistrimit, Amendimit, Rivlerësimit;
- Modulet e Deklaratave;
- Modulet e Menaxhimit të Borxhit;
- Modulet e Kontabilitetit;
- Modulet e Proceseve të Pagesave;
- Modulet e Menaxhimit të Rasteve;
- Modulet e Menaxhimit të Kontrollit;
- Modulet e Menaxhimit të Analizës së Riskut;
- Modulet e Hedhjes së Deklarimeve;
- Modulet e Librave të Shitjes dhe Blerjes;
- Modulet e Listë pagesave dhe Bilanci;
- Modulet e Menaxhimit te Përdoruesve dhe Aksesit;
- Modulet e Shërbimeve Publike;
- Modulet e Komunikimit me bankat Komunikimet me palët e treta;
- Sistemi i Raportimit;
- Sistemi i Integruar i Mesazheve;
- Sistemi i Gjurmimit.

Rezulton se: Komponentët e sistemit të ndërveprimit përbëhen nga:

- Web Aplikimi C@TS;
- Web Aplikimi *eFiling*;
- *Web Service* (të brendshme);
- Shërbimet e raportimit (SSRS);
- Shërbime Integruese SQL Server (paketa SSIS);
- Komunikimi me palët e treta nëpërmjet platformës qeveritare të ndërveprimit (DIS);
- Shërbimet elektronike në e-Albania (*web service* për palë të treta);
- Komponenti Vlerësim Rrisku për Tatimpaguesit (DB + SSIS);
- Komponent për gjenerimin e dokumenteve në masë (Infinica).

Kategoritë e të dhënave që shkëmbehen nëpërmjet komponentëve të *web-service*-ve janë:

- Të dhënat e regjistrimit të tatimpaguesit (*cats-efiling*);
- Të dhënat e deklaratave bosh (*cats-efiling*);
- Deklaratat e dorëzuara (*efiling-cats*);
- Listë pagesat e krijuara (*cats-efiling*);
- Listë pagesat e dorëzuara (*efiling-cats*);
- Gjendja e detyrimeve te tatimpaguesit (*cats-efiling*);
- Çështjet e krijuara (*efiling-cats*);
- Përditësimit të statuseve të çështjeve (*cats-efiling*);
- Librat e shitjes & blerjes së dorëzuara (*efiling-cats*);
- Bilancet e dorëzuara (*efiling-cats*);
- Dokumente të gjeneruara nga sistemi (*cats-efiling*).

Konkretisht të dhënat personale që shkëmbehen nëpërmjet komponentëve janë:

1. Të dhëna rreth punonjësve:

Nr.	Të dhëna
1	NID
2	Emër
3	Mbiemër
4	*MiddleName*
5	Datëlindja
6	Gjinia
7	Kombësia

2. Të dhëna rreth personave të lidhur, ndër të tjera, kombësia, nr. pasaporte, nr. telefoni, adresë emaili, etj., (sipas procesverbalit të hetimit administrativ).

Nr.	Të dhëna
1	NID
2	Emër
3	Mbiemër
4	MiddleName
5	Datëlindja
6	Gjinia
7	Kombësia
8	Atësia
9	Mëmësia
10	Nr. pasaportë
11	Status Gjendje Civile
12	Marrëdhënia me kryefamiljarin
13	Lloji i personit të lidhur
14	Qyteti
15	Bashkia
16	Rruga

17	Kodi postar
18	Nr. telefoni
19	Adresë email

3. Të dhëna rreth Individëve Privat dhe Personave Fizik:

Nr.	Të dhëna
1	NID
2	Emër
3	Mbiemër
4	MiddleName
5	Datëlindja
6	Gjinia
7	Kombësia
8	Atësia
9	Mëmësia
10	Vendlindja
12	Marrëdhënia me Kryefamiljarin
13	Qyteti
14	Bashkia
15	Rruga
16	Kodi Postar
17	Nr. Telefoni
18	Adresë Email

4. Të dhëna rreth Llogarive Bankare:

Nr.	Të dhëna
1	Emër Banke
2	IBAN
3	Tatimpaguesi (NIPT që lidhet me të)

5. Të dhënat mbi Raportet SSRS:

Nr.	Moduli
1	Menaxhimi i çështjeve
2	Statistika
3	Regjistrimi
4	Borxhet
5	Listë pagesat
6	Parapagimet
7	Librat
8	Raporte DPT
9	Ndihma Financiare
10	Rikalkulim
11	Risk
12	Vlerësimi Alternativ
13	Deklaratat
14	Diva
15	Raporte fund viti
16	Dogana
17	ISSH
18	Performanca e aplikimit
19	Raporte Thesari (mbledhje te ardhurash)

Nga verifikimi i kërkesave teknike të parashikuara në dokumentacionin teknik si dhe verifikimi në vend mbi statusin aktual, rezulton se Kontrolluesi:

- Nuk ka të identifikuar sistemet ose pjesët e tyre të cilat janë kritike për ofrimin e shërbimit 24 orë, në 7 ditë të javës;
- siguria e aplikacionit të sistemit në lidhje me Log-imet (gjurmueshmëria e veprimeve dhe të funksionimit të sistemit *"e-Taxation*"), edhe pse është e planifikuar teknikisht në projekt, nuk u arrit të provohet nga Kontrolluesi se realizohet specifikisht sipas projektit teknik;
- Edhe pse ka plane të dokumentuara për menaxhimin e riskut, teknikat e menaxhimit dhe të performancës së tij, rezulton se ato nuk zbatohen nga ana e njësive përgjegjëse. konkretisht, referuar rregullores nr. 12445/1, datë 03.07.2020 *"Për sigurinë e Informacionit në DPT",* mbi detyrat dhe përgjegjësitë e njësive përgjegjëse;
- Nuk janë kryer auditime të brendshme me qëllim garantimin e mirë funksionimit të këtyre teknikave për menaxhimin e riskut (ose në mungesë të teknikave, identifikim të riskut);
- Konstatohen mangësi në hartimin dhe dokumentimin e planit të rimëkëmbjes nga katastrofa, i cili duhej të përmbante masa dhe procedura të mirë dokumentuara për

rivendosjen në funksionim të sistemit në rastet e emergjencave. Në këto procedura duhej të ishin përcaktuar koha e rivendosjes në funksionim, disponueshmëria e burimeve njerëzore, mënyrat e informimit dhe personat përgjegjës të cilët do të ndjekin këto procedura;

- 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;
- Edhe pse ka të formalizuar një procedurë zyrtare të sigurisë së informacionit, dhe menaxhimit ndaj incidenteve të teknologjisë së informacionit (*Manuali për Politikat dhe Procedurat e Drejtorisë së Teknologjisë së Informacionit dhe Komunikimit*), nuk u arrit të dokumentohet nga ana e Kontrolluesit që kjo procedurë të jetë zbatuar sa i takon sigurisë së infrastrukturës TIK;
- Mbledhja e të dhënave sipas tabelës nr. 2, si më sipër rreth personave të lidhur, nuk u provua/dokumentua se realizohet në përputhje me parimet dhe kriteret ligjore të parashikuara në nenet 5 dhe 6 të Ligjit.

Në vijim, u konstatua se Politikat mbi gjurmët (log-et) në sistemin *"e-Taxation"* dhe infrastrukturën mbështetëse TIK, nuk zbatohen sipas modulariteteve të Rregullores për Sigurinë e Informacionit, çka rezulton në cenim të sigurisë në fushën e teknologjisë së informacionit dhe mungesë transparence.

Gjithashtu u konstatua 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 rikuperimit (DRP), në kundërshtim kjo me aktet ligjore apo nënligjorë në fuqi. Konstatohet se backup-i tek mjediset e AKSHI-t kryhet automatikisht, por nga ana e përfaqësuesve të Kontrolluesit, nuk u arrit të dokumentohej testimi i backup-ve. Kopjet (backup) e të dhënave nuk testohen rregullisht për t'u siguruar që mund të përdoren në raste të nevojshme. Kopjet e këtyre backup janë marrë si efektive nga DPT dhe janë kaluar në storage/arkivim. Procedurat e rikrijimit (restore) të të dhënave nuk testohen për t'u siguruar që ato janë të efektshme dhe që ato mund të ekzekutohen brenda kohës së lejuar. Këto procedura duhet të testohen rregullisht, sistematikisht dhe vazhdimisht.

Nga kontrolli i përdoruesve të sistemit dhe përgjegjësive që kanë në sistemin *"e-Taxation"*, u konstatuan disa problematika me ndikim/impakt në sigurinë e të dhënave, si vijon:

- Në sistem rezultojnë përdorues me status *"aktiv"* edhe punonjësit të cilët kanë ndërprerë marrëdhëniet e punës;
- Këto Atribute mbi rolet nuk rezultojnë të dokumentuara, duke krijuar një konfuzion në menaxhimin e përdoruesve;
- Data e mbarimit të përgjegjësisë që i është caktuar një përdoruesi, mungon në të gjithë përdoruesit edhe nëse punonjësi mund të ketë ndryshuar pozicionin e detyrimisht edhe profilin në sistem;

- në sistemin *"e-Taxation"*, sipas përgjigjes së përfaqësuesit të Kontrolluesit rezultojnë si përdorues c@ts mbi 2,198 *"usera"* nga ku 1,488 janë aktiv, e-filing mbi 527,510 *"user"*, nga ku janë aktiv 527,930, përfshirë edhe *"usera"* që janë përdorur për testimin dhe implementimin e sistemit, apo përdorues të krijuar me të dhëna jo të plota për emrin, të tilla si tipi *"guest"*.

Baza e të dhënave të sistemit *"e-Taxation"* rezulton se nuk është e regjistruar si bazë të dhënash shtetërore në Autoriteti Rregullator Kombëtar për bazat shtetërore (ARK), referuar ligjit nr. 10325, datë 23.09.2010 "*Për bazat e të dhënave shtetërore*" dhe VKM nr. 945, datë 02.11.2012 *Për miratimin e rregullores "Administrimi i sistemit të bazave të të dhënave shtetërore"*. Regjistrimi i bazës së të dhënave është i nevojshëm për standardizimin dhe sigurimin e saj.

Zyra e Komisionerit vlerëson se, Kontrolluesi duhet të kryejë auditime të vazhdueshme mbi hedhjen e të dhënave dhe logim-et në sistem. Log-et, të cilat gjenerohen nga sistemi duhet të analizohen përmes një ndërfaqeje aplikative të posaçme, e cila të mundësojë një shfletim në kohe reale të tyre. specialistët IT duhet të kenë akses në mënyrë të shpejtë për të bërë kërkime si: tentativat e dështuara për log-in, nr. e login nga një PC, etj., 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 rreziku që ngjarje të tilla të verifikohen dhe lokalizon problemin.

Krijimi i procedurave të backup dhe vazhdimësisë së punës për Sistemet e Informacionit për sistemin *"e-Taxation",* duhet të jetë në përputhje me VKM Nr. 945, datë 02.11.2012 *"Për miratimin e rregullores "Administrimi i sistemit të bazave të të dhënave shtetërore"* si dhe VKM nr. 710, dt. 21.08.2013 *"Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit"*.

Menaxhimi i përdoruesve të sistemit *"e-Taxation"* nga ana e administratorëve, duhet të jetë koherent me çdo ndryshim të funksionalitetit të punës apo në rastet e largimet nga pozicionet e punës. Llogaritë në sistem *"e-Taxation"* të tipit *"guest/user"* nuk duhet të jenë aktive dhe më të drejta funksionale, pasi veprimet e këtyre përdoruesve nuk mund të identifikohen dhe përbejnë risk.

zbatimi rregulloreve dhe procedurave të miratuar nga Kontrolluesi përfshirë dhe rregulloren nr. 12445/1, datë 03.07.2020 "*Për Sigurinë e Informacionit në DPT*", mbi detyrat dhe përgjegjësitë e njësive përgjegjëse, duhet të jetë periodik dhe i vazhdueshëm. Analizimi periodik i veprimeve/gjurmëve të përdoruesve apo të funksionimit të sistemit nëpërmjet logeve, minimizon riskun dhe lokalizon problemin. Zyra e Komisionerit vlerëson se, Kontrolluesi nuk ka marrë masa organizative dhe teknike të përshtatshme për të mbrojtur të dhënat personale nga shkatërrime të paligjshme, aksidentale, humbje aksidentale, për të mbrojtur aksesin ose përhapjen nga persona të paautorizuar, veçanërisht në këtë rast kur përpunimi i të dhënave kryhet

nëpërmjet komunikimeve elektronike, në kundërshtim me parashikimet e nenit 27 të Ligjit dhe Udhëzimit nr. 47, të Komisionerit, datë 14.09.2018 *"Për përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga subjektet përpunuese të mëdha*" (në vijim, *"Udhëzimi nr. 47"*).

Përgjegjësia për të garantuar sigurinë dhe konfidencialitetin e të dhënave personale qëndron për çdo kontrollues, bashkëkontrollues apo përpunues që ka akses në të dhënat në këtë sistem. Një nga masat kryesore për garantimin e sigurisë së të dhënave personale dhe konfidencialitetit të të dhënave është edhe gjurmueshmëria e veprimeve përpunuese dhe verifikimi i vazhdueshëm i tyre, në zbatim të neneve 27, 28 të Ligjit dhe Udhëzimit nr. 47.

5. Në kuadër të detyrimeve ligjore të funksionimit të institucioneve të tjera shtetërore, DPT ofron mundësinë e aksesit dhe ndërveprimit të të dhënave në sistemin *"e-Taxation".*

   Referuar kontratës së shërbimit të mirëmbajtjes së sistemit, në ofertën e specifikimeve teknike të sistemit *"e-Taxation",* rezulton se janë parashikuar ndërveprime me palë të treta si Instituti i Statistikave (INSTAT), DPGJC, Drejtoria e Përgjithshme e Thesarit (DPTH), QKB, ISSH, DPD, Fiskalizimi dhe e-Albania, për të patur akses/shërbim në këtë bazë të dhënash nëpërmjet GG.

   Nga verifikimi i kryer, rezulton se ka më shumë institucione publike të cilat kanë akses në sistemin elektronik, nga sa është parashikuar në termat teknik. Ndërveprimi i sistemit me sisteme të tjera kryhet në dy mënyra, që janë:

   a) Aksesi nëpërmjet *web-service*-ve:
   Referuar termave teknike rezulton se janë parashikuar pesë institucione për të patur akses/shërbim në të dhënat e kësaj baze të dhënash. Nga verifikimet e marrëveshjeve të vendosura në dispozicion të grupit të hetimit administrativ rezulton se ka më tepër institucione të cilët ndërveprojnë në sistemin elektronik nëpërmjet shërbimit *web-service* (shërbime ndërlidhëse të automatizuara midis sistemeve).

   Gjithashtu, bazuar në pikën 7 të Vendimit nr. 673, datë 22.11.2017, të Këshillit të Ministrave *"Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit"* i ndryshuar (në vijim, *"VKM nr. 673"*), AKSHI mundëson ekspozimin e web service-ve të bazave të të dhënave me qëllim aksesimin e të dhënave parësore për subjektet e interesuara për ndërveprimin në platformën qeveritare të ndërveprimit, konkretisht të *"e-Taxation"*, me qëllim aksesimin e të dhënave parësore nëpërmjet portalit unik qeveritar e-Albania, etj., për subjektet e interesuara të cilat kanë detyrime ligjore për ndërveprimin në platformën qeveritare.

   b) Aksesi në mënyrë të drejtpërdrejtë për punonjësit administrativ të cilët identifikohen në sistem nëpërmjet *"emrit të përdoruesit"* dhe *"fjalëkalimit përkatës"*, nëpërmjet VPN.

Bazuar në pikën 10, të VKM nr. 673, në përbërje të AKSHI-t, pranë çdo institucioni dhe organi të administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave, krijohen dhe funksionojnë Njësitë e Teknologjisë së Informacionit e të Komunikimit (NJTIK), si strukturë organizativo-teknike për projektimin, zbatimin dhe administrimin e qeverisjes elektronike në institucion, nëpërmjet teknologjisë së informacionit e të komunikimit (TIK). Pranë DPT funksionon struktura NJTIK me emërtim *"Drejtoria e TIK",* e cila administron sistemin *"e-Taxation"* së bashku me komponentët e tjerë të teknologjisë dhe informacionit.

Nga verifikimi i aktiveve të Kontrolluesit, rezulton se pajisjet TIK si dhe infrastruktura e sistemit *"e-Taxation",* janë pjesë e inventarit të DPT. Si rrjedhojë DPT është zotërues i pajisjeve sipas përcaktimit të ligjit nr. 10 296, datë 08.07.2010 *"Për menaxhimin financiar dhe kontrollin",* i ndryshuar, dhe për pasojë mbart çdo detyrim që lind nga ky ligj.

Referuar pikës 1, të nenit 4, të ligjit Nr. 10325, datë 23.9.2010 *"Për bazat e të dhënave shtetërore",* rezulton se, *"Baza e të dhënave shtetërore krijohet me ligj ose me VKM"*. Gjithashtu, neni 7 i këtij ligji, parashikon se, *"Baza e të dhënave shtetërore përmban të dhënat parësore dhe të dhënat dytësore":*

a) *Të dhënat parësore të një baze të dhënash shtetërore janë informacione specifike, të mbledhura nga institucioni administrues, në përputhje me aktin e krijimit.*
b) *Të dhënat dytësore janë të dhënat që merren nga një bazë tjetër të dhënash, ku ato janë parësore.*

Të dhënat që popullojnë sistemin *"e-Taxation"* mblidhen dhe përpunohen në zbatim të ligjit nr. 9920, datë 19.05.2008 *"Për procedurat tatimore në Republikën e Shqipërisë"* i ndryshuar, si dhe ligjit nr. 9136, datë 11.09.2003 *"Për mbledhjen e kontributeve të detyrueshme të sigurimeve shoqërore e shëndetësore në Republikën e Shqipërisë",* i ndryshuar.

Zyra e Komisionerit vlerëson se, në bazë të pikës 5 të nenit 3 të Ligjit, "*Kontrollues*" *është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër që, vetëm apo së bashku me të tjerë, përcakton qëllimet dhe mënyrat e përpunimit të të dhënave personale, në përputhje me ligjet dhe aktet nënligjore të fushës, dhe përgjigjet për përmbushjen e detyrimeve të përcaktuara në këtë ligj"*.

Ndërsa, "*Përpunues*" *është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër që përpunon të dhëna personale në emër të kontrolluesit* (pika 7).

Sipas këtyre përkufizimeve, cilësia e kontrolluesit i vishet subjektit që përmbush kushtet si vijon:

a. Përcakton vetëm apo së bashku me të tjerë, qëllimet dhe mënyrat e përpunimit; dhe,
b. Përgjigjet për përmbushjen e detyrimeve që burojnë nga Ligji (parimi i përgjegjësisë, i parashikuar në pikën 2 të nenit 5 të Ligjit).

Në cilësinë e kontrolluesit, DPT rezulton se përcakton qëllimet dhe mënyrat e përpunimit të të dhënave personale duke përmbushur, kushtet e germës "*a*", më sipër. Rrjedhimisht, DPT është e detyruar të përgjigjet për përmbushjen e detyrimeve që burojnë nga Ligji (germa *"b"*, më sipër).

Bazuar në nenet 27 dhe 28 të Ligjit, në cilësinë e kontrolluesit, DPT ka detyrimin të garantojë sigurinë dhe konfidencialitetin e të dhënave personale, të cilat ky Kontrollues përpunon.

Sa më sipër, konstatohet se, sa i përket aksesit nga palët e treta nëpërmjet *web-service*-ve, Kontrolluesi nuk ka marrë masa të përshtatshme për formalizimin dhe dokumentimin e politikave dhe procedurave lidhur me mënyrën e dhënies së të drejtës së aksesit. Përhapja e të dhënave, si formë e posaçme përpunimi (sipas përkufizimit në pikën 12, të nenit 3 të Ligjit), duhet të realizohet në përputhje me parimet dhe kriteret ligjore të parashikuara në nenet 5 dhe 6 të Ligjit.

Edhe pse, bazuar në VKM nr. 673, AKSHI (në cilësinë e bashkëkontrolluesit) bart detyrimin për të garantuar sigurinë dhe pacenueshmërinë e sistemeve të infrastrukturave kritike të përdorura nga institucionet shtetërore, si në rastin e DPT, dispozitat e Ligjit në lidhje me aspektet e sigurisë së të dhënave nuk përjashtojnë nga përgjegjësia ligjore institucionet në fjalë, të cilat, në cilësinë e kontrolluesit, kanë detyrimin të demonstrojnë përputhshmëri me Ligjin, si dhe mbajnë përgjegjësi, për realizimin e proceseve përpunuese në përputhje me dispozitat e nenit 5 të Ligjit.

Kontrolluesi nuk mund të justifikojë anomalitë dhe cenimet eventuale në sigurinë e të dhënave, me faktin se për këtë qëllim është përgjegjës AKSHI, në përputhje me dispozitat e VKM-së nr. 673.

Zyra e Komisionerit vlerëson se angazhimi i përpunuesve/bashkëkontrolluesve të tjerë (të përcaktuar me akt nënligjor) nuk çliron Kontrolluesin nga përgjegjësitë për të mbikëqyrur dhe monitoruar aspektet e sigurisë dhe konfidencialitetit të të dhënave që Kontrolluesi është i autorizuar (me ligj) të përpunojë dhe administrojë;

6. Në lidhje me palët e treta tek të cilat përhapen të dhëna personale, si dhe bazën ligjore përkatëse, konstatohet se kontrolluesi ka lidhur Marrëveshje (dhe/ose të ngjashme), në kuadër të bashkëpunimit institucional dhe shkëmbimit të informacionit, ndër të tjera, me:

- Marrëveshje Bashkëpunimi ndërmjet Drejtorisë së Policisë së Shtetit dhe DPT (nr.28640, datë 10.08.2016).

Konstatohet se referencat ligjore të cituara në këtë marrëveshje referohen ligjeve organike (dhe jo vetëm) të dy institucioneve respektive dhe nuk identifikojnë saktë kuadrin ligjor rregullator që dikton nevojën e shkëmbimit të informacionit midis palëve dhe/ose dhënien e aksesit, duke mos identifkuar rrjedhimisht një kriter ligjor për përpunimin e të dhënave, në kundërshtim me nenin 6 të Ligjit.

- Marrëveshje Bashkëpunimi ndërmjet Inspektoratit të Lartë të Deklarimit dhe Kontrollit të Pasurive dhe Konfliktit të Interesave (ILDKPKI) dhe DPT (nr. 3456 Prot., datë 30.03.2009).
  Konstatohet se dispozita e cituar si referencë ligjore (neni 17/ç, ligjit nr.9049, datë 10.4.2003 "Për deklarimin dhe kontrollin e pasurive, të detyrimeve financiare të të zgjedhurve dhe të disa nëpunësve publikë", i ndryshuar, për procesin e bashkëpunimit dhe bashkërendimin e aktiviteteve të palëve në këtë memorandum) në nenin 1 "*Qëllimi*" është e pasaktë dhe nuk identifikon saktë kuadrin ligjor rregullator që dikton nevojën e shkëmbimit të informacionit midis palëve dhe/ose dhënien e aksesit, duke mos identifkuar rrjedhimisht një kriter ligjor për përpunimin e të dhënave, në kundërshtim me nenin 6 të Ligjit.

AKSHI është institucioni i cili ofron infrastrukturën TIK të ndërveprimit midis sistemeve elektronike të institucioneve shtetërorë nëpërmjet GG. Qëllimi i ndërtimit të GG është që të sigurohet ndërveprimi i sistemeve elektronike të ndryshme, pavarësisht teknologjisë së përdorur. Bazuar në arkitekturën GG, integrohen të gjitha sistemet elektronike të brendshme të Qeverisë.

Nëpërmjet kësaj arkitekture mund të integrohet dhe mundësohet ndërveprimi midis sistemeve të brendshme, të ndryshme qeveritare. Këto sisteme të brendshëm mund të ekspozojnë funksionalitetet e tyre nëpërmjet portalit unik qeveritar e-Albania. Referuar VKM nr. 673, AKSHI ka për qëllim, ndër të tjera, të krijojë kushtet teknike të ndërveprimit të sistemeve elektronike.

Zyra e Komisionerit vlerëson se, dhënia nga Kontrolluesi e aksesit për palë të tjera, legjitimohet vetëm nëse është e parashikuar me ligj, në përputhje me parimet dhe kriteret ligjore të përpunimit të të dhënave, të parashikuara në nenet 5 dhe 6 të Ligjit.

7. Nga verifikimi i kryer në regjistrin elektronik të subjekteve kontrolluese, si dhe në protokollin e Zyrës së Komisionerit, rezulton se Kontrolluesi ka njoftuar mbi përpunimin e të dhënave personale, për të cilat është përgjegjës por në zbatim të pikës 1, të nenit 21 të Ligjit, konstatohet se njoftimi nuk është i plotë dhe i saktë.

   Gjatë hetimit administrativ të ushtruar, është konstatuar se *"Njoftimi"* ka mangësi në deklarim, sa i përket rubrikave të formularit si vijon:

   i. Deklarimin në rubrikën 2, të formularit të njoftimit *"personi i kontaktit ngarkuar nga subjekti"*;

ii. Deklarimin në rubrikën 3, të formularit të njoftimit *"kategoritë e subjekteve të të dhënave personale që përpunohen"*;
iii. Deklarimin në rubrikën 4, të formularit të njoftimit "*kategoritë e të dhënave personale që përpunohen*";
iv. Deklarimin në rubrikën 5, të formularit të njoftimit *"të dhënat sensitive që përpunohen*";
v. Deklarimin në rubrikën 6, të formularit të njoftimit "*qëllimi i përpunimit"*;
vi. Deklarimin në rubrikën 7, të formularit të njoftimit "*Marrësit e të dhënave personale"*.

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

8. Kontrolluesi ka lidhur me palë të treta Kontratë nr. 3339 Prot., datë 12.05.2021, me objekt: *"Mirëmbajtja e sistemit e-Taxation, për DPT"* midis palëve AKSHI dhe *"IkubINFO shpk",* me përfitues DPT.

   Nisur nga parashikimet e kontratës së sipërcituar si dhe konstatimeve në vend, rezulton se operatori ekonomik *"IkubINFO shpk"*, ka akses të drejtpërdrejtë në nivel administratori në sistemin *"e-Taxation"* dhe bazën e të dhënave. Në këto kushte, referuar pikës 7, të nenit 3 të Ligjit, operatori ekonomik gëzon cilësinë e përpunuesit.

   Referuar kontratës së sipërcituar, rezulton se nuk janë reflektuar detyrimet sipas parashikimeve në nenin 20 të Ligjit dhe Udhëzimin nr. 19 të Komisionerit, datë 03.08.2012 *"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 delegim*i*"*, i ndryshuar (në vijim, *"Udhëzimi nr. 19"*).

   Zyra e Komisionerit vlerëson se, në rastet e delegimit të përpunimit të të dhënave dhe/ose një shërbimi, Kontrolluesi duhet të sigurohet që përpunuesi të garantojë përpunim të ligjshëm dhe të sigurt të të dhënave. Detyrimet e përpunuesit, për përpunimin e të dhënave personale, parashikohen në nenin 20 të Ligjit dhe rregullohen me aplikimin e Udhëzimit nr.19.

9. Grupi i hetimit administrativ i kërkoi Kontrolluesit, ti vihen në dispozicion një kopje e logeve të sistemit *"e-Taxation",* konkretisht kopje të logeve që paraqesin gjurmueshmërinë e veprimeve të punonjësve të NJTIK për periudhën Janar-Mars 2021, si dhe periudhën Prill-Qershor 2021. Në përgjigje të kërkesës së grupit të hetimit, u vendos në dispozicion nëpërmjet postës elektronike datë 01.03.2022, në formatin *"loge.rtp",* një kopje e Historikut të *"Log-eve"* të sistemit *"e-Taxation".*

Nga verifikimi rezulton se përmbajtja e logeve është e kufizuar në përmbajtje dhe në role dhe jo sipas kërkesës së grupit të hetimit, çka ka pamundësuar identifikimin dhe gjurmueshmërinë e rrjedhjes apo incidenteve të ndryshme që mund të kenë ndodhur.

Nga shqyrtimi i eventeve të logeve *"loge.rtp"* të vëna në dispozicion, konstatohet se event-i i *log*-eve përmban vetëm të dhëna si mëposhtë vijon:

Fillimi i eventit: 2021-01-03 19:28:39.3873101|SL
EventID|event_time,
[Subjekti]
Agjensia
DRT]
Taksa]
Data Vleresimit]
Periudha
Kredi e paperdorur]
detyrimi]
gjoba]
interesa]
detyrimi]+[interesa]+[gjoba]) [Balanca]
Statusi]
Gjurmë të tjera:
*Shitje të përjashtuara],0)) +
sum(isnull([(10) Shitje pa TVSH],0)) +
sum(isnull([(11) Eksporte mallrash],0)) +
sum(isnull([(12) Furnizime me shkallë 0%],
distinct t.UniqueIdentificationNumber NIPT,*
*t.name Subjekti,
trl.CodeDescription [DRT],
ll.codedescription [Forma Ligjore],
tsl.codedescription [Statusi],
t.registrationdate [Dt Fillimit],
"lloji.[Pershkrimi Kodi ekonomik" 1]*
* sektoret.sektori
,sektoret.nensektori
,sektoret.Risku
,sektoret.pronesia
,sektoret.[type]
,sektoret.kodi
,sektoret.pershkrimi
,case*
.....
Mbarimi i eventit: 2021-02-26 12:28:37.9035467|SL

Kontrolluesi nuk ka vënë në dispozicion informacionin e plotë të eventeve, të veprimtarisë së kryer në sistem nga punonjësit, sipas periudhës së kërkuar.

Kontrolluesit i'u kërkua të vendosë në dispozicion backup-e të kompjuterëve të punonjësve NJTIK të atashuar pranë DPT si dhe qasje në arkivën e mail-box të Exchange qeveritar (GovNET) të punonjësve të po kësaj njësie, me qëllim verifikimin e veprimeve të kryera nga këta punonjës, sipas dispozitave të parashikuara në Rregullore nr. 12445/1 datë 03.07.2020 *"Për Sigurinë e Informacionit në DPT".* Nga ana e përfaqësuesve të Kontrolluesit, nuk është vënë në dispozicion informacioni i kërkuar nga grupi i hetimit administrativ, edhe pse një gjë e tillë është kërkuar disa herë në formë elektronike dhe verbale.

Përfaqësuesve të Kontrolluesit i'u kërkua të mundësojë aksesin/demonstrimin on-site të sistemit *"production",* për verifikimin *"live"* të moduleve/kategorive të të dhënave, etj. Gjithashtu, është kërkuar të dokumentohet e plotë praktika e ndërtimit të sistemit *"e-Taxation"* (termat e referencës, TOR-set, etj.). Ndër të tjera, Grupi i hetimit kërkoi ti mundësohet qasja në loget e sistemit *"e-Taxation",* me qëllim verfikimin e gjurmueshmërisë (event-log) të veprimeve të punonjësve, konkretisht atyre të NJTIK pranë DPT.

Zyra e Komisionerit vlerëson se, Kontrolluesi ka dëshmuar një qasje pjesërisht jobashkëpunuese, e cila, shoqëruar me mosadresimin e kërkesave të parashtruara në lidhje me dhënien e dokumentacionit dhe mundësimin e aksesit/demonstrimit të funksionimit të sistemit *"eTaxation",* sipas kërkesave të grupit të hetimit, ka pamundësuar zhvillimin e gjerë të hetimit administrativ, konkretisht për zbatimin e objektit të planit të hetimit, në kundërshtim me nenet 30, 32 të Ligjit për Mbrojtjen e të Dhënave Personale, si dhe nenin 77 të Kodit të Procedurave Administrative.

10. Kontrolluesi ka të miratuar një rregullore dhe manual në funksion të sigurisë së informacionit, në të cilat janë specifikuar rregullat e përgjithshme për sigurinë e informacionit dhe përgjegjësitë për veprimet që lidhen me sigurinë e informacionit në DPT.

    Konstatohet se nuk ka norma specifike që rregullojnë ruajtjen, mbrojtjen dhe sigurinë e të dhënave personale, gjatë proceseve përpunuese që zhvillon Kontrolluesi, në përmbushjen e detyrave funksionale.

    Gjithashtu, nuk janë konstatuar procese monitorimi të standardizuara dhe periodike sipas rregulloreve të hartuara për mbrojtjen e aseteve dhe informacionit, për ruajtjen, integritetin, disponueshmërinë dhe konfidencialitetin e të dhënave.

    Kontrolluesi nuk ka të miratuar rregullore specifike *"Për mbrojtjen e të dhënave personale"*, dhe si rrjedhojë, mungojnë procedurat mbi masat teknike dhe organizative sipas parashikimeve të nenit 27 të Ligjit, me qëllim garantimin e

përpunimit të ligjshëm dhe sigurisë së të dhënave, në përputhje me proceset përpunuese të Kontrolluesit.

Zyra e Komisionerit vlerëson se hartimi i një *"Rregulloreje 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 subjekti të dhënash), sigurinë e të dhënave, konfidencialitetin, afatet e mbajtjes së të dhënave, etj., konsiderohet një detyrim shumë i rëndësishëm në zbatim të nenit 27 të Ligjit dhe Vendimit nr. 6 të Komisionerit, datë 05.08.2012 *"Për përcaktimin e rregullave të hollësishme për sigurimin e të dhënave personale"* (në vijim, *"Vendimi nr. 6"*).

11. Në faqen zyrtare https://www.tatime.gov.al të institucionit, Kontrolluesi ka të publikuar një rubrikë të emëruar "*politikë privatësie*". Nga verifikim i përmbajtjes së saj, konstatohet se në këtë rubrikë, subjektet e të dhënave nuk informohen plotësisht mbi qëllimin dhe mënyrën e përpunimit të të dhënave personale, personin që do t'i përpunojë të dhënat, të drejtat ligjore që gëzojnë, afatin e mbajtjes së të dhënave, masat e sigurisë, etj., në kundërshtim me parashikimet e nenit 18 të Ligjit.

    Zyra e Komisionerit vlerëson se informimi i subjekteve të të dhënave personale është një nga detyrimet bazë të kontrolluesit pasi u jep mundësinë subjekteve të të dhënave personale të njihen me të drejtat që gëzojnë 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.

12. Kontrolluesi nuk ka ndërmarrë masa konkrete në kuadër të trajnimit të punonjësve që kanë akses dhe përpunojnë të dhëna personale lidhur me legjislacionin në fuqi për mbrojtjen e të dhënave personale. Rezulton mosplotësim i detyrimeve në lidhje me ngritjen, administrimin dhe mirëmbajtjen e Sistemit të Menaxhimit së Sigurisë së Informacionit (SMSI) për sa i takon mbrojtjes së të dhënave personale, të parashikuar në Udhëzimin nr. 47.

    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 standartin ndërkombëtar ISO/IEC 27001, siç parashikohet në nenin 5 të Udhëzimit nr. 48, datë 14.09.2018, të Komisionerit "*Për certifikimin e sistemeve të sigurisë së informacionit, të dhënave personale dhe mbrojtjes së tyre*" (në vijim, "*Udhëzimi nr. 48*"), si dhe duhet të jetë një sistem i certifikueshëm, për qëllime përputhshmërie me standardin e

sipërpërmendur, vetëm nga organizma të akredituar dhe autorizuar sipas parashikimeve të Udhëzimit nr. 48 të Komisionerit.

13. Kontrolluesi nuk ka marrë masa në lidhje me zbatimin e detyrimeve të përcaktuara në Vendimin nr. 41, datë 23.08.2021 të Komisionerit, për Kontrolluesin *"Drejtoria e Përgjithshme e Tatimeve".*

    Zyra e Komisionerit vlerëson se, mungesa totale e angazhimit të Kontrolluesit, për të marrë masa për zbatimin e rekomandimeve dhe detyrave të lëna në Vendimin e sipërcituar, rëndon pozitën e tij si Kontrollues, në raport me zbatimin e detyrimeve të sanksionuara në Ligj.

Në përfundim të hetimit administrativ, referuar provave dhe konstatimeve në vend, grupi i hetimit administrativ hartoi procesverbalin përkatës, një kopje e të cilit i është dërguar Kontrolluesit me rrugë postare nëpërmjet shkresës nr. 1135/1 prot., datë 06.06.2022.

Në respektim të së drejtës për t'u dëgjuar, në zbatim të neneve 87-89 të Kodit të Procedurave Administrative, Kontrolluesi është ftuar të marrë pjesë në seancë dëgjimore, përpara marrjes së vendimit përfundimtar nga ana e Komisionerit.

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

1. *Lidhur me faktin që pajisjet TIK si dhe infrastruktura e sistemit "e-Taxation" janë pjesë e inventarit të DPT-së dhe rrjedhimisht DPT është zotërues i pajisjeve, bëjmë me dije se: "Pavarësisht faktit që procedura e kalimit kapital të aseteve nga DPT në AKSHI nuk është finalizuar për shkak të disa problematikave të cilat po diskutohen dhe shqyrtohen ndërmjet anëtareve të grupeve respektive të punës të ngritur për këtë qëllim, AKSHI është struktura e specializuar, për administrimin, menaxhimin e informacionit në të gjithë infrastrukturën hardware dhe software në Administratën Tatimore."*
   Referuar VKM 673/2017, institucioni i cili përfaqëson pronarin shtet dhe administron çdo sistem dhe infrastrukture hardware dhe software në fushën TIK, për institucionet dhe organet e administratës buxhetore nën përgjegjësinë e Këshillit të Ministrave, si dhe institucionet jo buxhetorë, është AKSHI.
   ... pavarësisht faktit se procedura e kalimit kapital të aseteve nga DPT të AKSHI, në zbatim të kësaj VKM-je nuk është finalizuar për arsye objektive, administruesi dhe menaxhuesi faktik i sistemeve është AKSHI, si njësia e vetme e specializuar dhe aksesi i çdo punonjësi te Administratës Tatimore ne sistem, administrohet dhe mundësohet vetëm nga Drejtoria TIK që ndodhet në DPT, e cila është në varësinë funksionale të AKSHI-t.

2. ***Së dyti,*** *për sa i përket konstatimit të mangësive në hartimin dhe dokumentimin e planit të rimëkëmbjes nga katastrofa, bëjmë me dije se: "Çdo software dhe hardware,*

është në ambientet e AKSHIT dhe është nën autoritetin e këtij të fundit të marrë të gjitha masat në këtë drejtim. Administrata Tatimore nuk disponon asnjë hardware ku ruhen këto të dhëna dhe nuk ka ekspertizë në staf për të marrë masa për planin e rimëkëmbjes nga katastrofa."

3. ***Se treti**, theksojmë se në Ligjin nr.9920/2008, në aktet nënligjore dalë në zbatim të tij, si dhe në një sërë aktesh të tjera të brendshme të institucionit, ndër të tjera, janë përcaktuar rregullime specifike për sa i përket detyrimit që kanë punonjësit e Administratës Tatimore Qendrore, për ruajtjen e konfidencialitetit të të dhënave, për të cilat vihen në dijeni për shkak të funksioneve të tyre, detyrim i cili mbetet në fuqi edhe në rastet e mos ushtrimit më të këtyre funksioneve, si rezultat i largimit nga puna. Në DPT, aplikohen një sërë masash në funksion të ruajtjes dhe mbrojtjes së informacionit (të dhënave), të parashikuara në Rregulloren nr.12445/ 1, datë 03.07.2020, "Për sigurinë e informacionit në Drejtorinë e Përgjithshme të Tatimeve", të ndryshuar, e hartuar në përputhje me praktikat me të mira sipas standardit të sigurisë ISO 27001:*

- *Çdo person i autorizuar për të aksesor sistemet e DPT-se, për identifikimin e tij ka një llogari përdoruesi unike...;*
- *Dhënia e të drejtave të aksesimit në sisteme bazohet në pozicionin e punës të punonjësit të DPT-së duke marrë parasysh detyrat e tij funksionale...;*
- *Funksionimi i Komitetit përgjegjës për sigurinë- anëtaret e të cilët, ndër të tjera kujdesen për: rishikimin e vazhdueshëm të masave të sigurisë ndaj ofruesve të shërbimeve te jashtme, veçanërisht te personelit qe punon me kontrate ne ambientet e DPT-se; rishikimin e rregullt te privilegjeve për aksesimin e sistemeve te kompjuterëve; kontrollin për mbylljen e menjëhershme të llogarive të përdoruesve që japin dorëheqjen ose qe largohen nga puna për arsye të tjera; koordinimin e kontrolleve të sigurisë, përfshire këtu organizimin e rregullt të kontrolleve të jashtme për të siguruar përputhjen me rregullat dhe standardet e sigurisë;*

  Komiteti përgjegjës për sigurinë dhe Nëpunësi Zbatues i DPT-së kryejnë një analizë vjetore zyrtare të riskut për asetet e informacionit, sipas procedurave qe rekomandohen në standardet ndërkombëtare.
- *Përgjegjësia për sigurinë përcaktohet që në fazën e marrjes në punë, ku çdo punonjës i Administratës Tatimore nënshkruan një dokument që quhet "Deklarata e sigurisë dhe konfidencialitetit".*
- *Të gjithë punonjësit e rekrutuar rishtazi në Administratën Tatimore në bashkëpunim me QTA TD dhe ASPA i nënshtrohen ciklit të trajnimeve për përfitimin e njohurive baze për legjislacionin tatimor në tërësi, si dhe për tema specifike të cilat trajtojnë parimet kryesore si: ruajtja e informacionit dhe konfidencialitetit, e drejta e informimit dhe mbrojtja e të dhënave personale.*
- *Nga ana e DPT janë ndërmarre edhe masa të tjera shtese në kuadër të zbatimit të rregullores "Për sigurinë e informacionit në Drejtorinë e Përgjithshme të Tatimeve", si dhe në zbatim të praktikave ndërkombëtare për sigurinë e*

informacionit, konkretisht në kompjuterat fundore të punonjësve të DPT-së dhe DRT-së është bllokuar përdorimi i USB për transferimin e materialeve; aksesi në web i punonjësve të DPT është kufizuar, duke u limituar vetëm në aksesimin e faqeve/linkeve që lidhen me detyrat dhe kompetencat e Administratës Tatimore, si dhe janë marrë masat që të gjithë punonjësit e institucionit të behën pjesë e Active Directory të AKSHI-t.

- *Theksojmë se rasti i cili është bërë precedent për nisjen e këtij hetimi administrative tashme është në faze të avancuar në prokurorinë e Tiranës e cila ka identifikuar qe përgjegjësit e këtij veprimi të paligjshëm janë ish specialiste të Drejtorisë TIK atashuar nga AKSHI në DPT, dhe asnjë punonjës i Administratës Tatimore nuk ka rezultuar të jetë i përfshire në këtë akt. Gjithashtu nga konkluzionet e Prokurorisë ka rezultuar që informacioni nuk ka rrjedhur nga sistemi, por nga veprime të pastra të paligjshme të këtyre individëve.*

  Bazuar sa më sipër, Administrata Tatimore e konsideron çështjen në hetim nga ana juaj si një çështje përtej, jo vetëm përgjegjësisë së saj, po edhe kapaciteteve të mundshme që kjo administratë ka për të ndikuar në procesin e ruajtjes së informacionit, duke qenë thjesht një administratë e pastër përdoruese e informacionit dhe jo administruese e saj.

Sa i përket këtyre argumenteve, Zyra e Komisionerit vlerëson se, DPT në cilësinë e Kontrolluesit, i cili vetëm apo së bashku me të tjerë, përcakton qëllimet dhe mënyrat e përpunimit të të dhënave personale, në përputhje me ligjet dhe aktet nënligjore të fushës, është përgjegjës për përmbushjen e detyrimeve të përcaktuara në Ligj, pavarësisht mënyrës së përpunimit të të dhënave dhe mekanizmave të përdorur.

Gjithashtu, sa i përket administrimit të sistemit *"eTaxation"* nga NJTIK (e AKSHI-t), Zyra e Komisionerit vlerëson se Kontrolluesi (DPT), duhet të jetë në gjendje të demonstrojë kontrollin dhe të garantojë përdorimin e ligjshëm dhe të sigurt të të dhënave, në mënyrë që përpunimi i tyre të kryhet vetëm në përputhje me udhëzimet e tij.

Bazuar në VKM nr. 673, AKSHI në cilësinë e institucionit përgjegjës për ofrimin e sigurisë për institucionet nën varësinë e Këshillit të Ministrave, bart detyrimin për të garantuar sigurinë dhe pacenueshmërinë e sistemeve të infrastrukturave kritike të përdorura nga institucionet shtetërore, si në rastin e DPT. Dispozitat e legjislacionit për mbrojtjen e të dhënave personale në lidhje me aspektet e sigurisë së të dhënave, nuk përjashtojnë nga përgjegjësia ligjore Kontrolluesin, i cili ka detyrimin të demonstrojnë përgjegjshmëri, si dhe mbajë përgjegjësi, për realizimin e proceseve përpunuese në përputhje me dispozitat e nenit 5 të Ligjit.

Kontrolluesi, nuk mund të justifikojë anomalitë dhe cenimet eventuale në sigurinë e të dhënave, me faktin se për këtë qëllim është përgjegjës AKSHI, bazuar në dispozitat e VKM nr. 673.

Zyra e Komisionerit vlerëson se angazhimi i përpunuesve të tjerë (qoftë edhe të përcaktuar me akt nënligjor), nuk çliron Kontrolluesin nga përgjegjësitë për të mbikëqyrur dhe monitoruar aspektet e sigurisë dhe konfidencialitetit të të dhënave që Kontrolluesi është i autorizuar (me ligj) të përpunojë dhe administrojë.

Si përfundim, shkeljet e konstatuara gjatë ushtrimit të hetimit administrativ në kuptim germave *a, b, ç, d, dh, dh/1* të pikës 1 dhe pikës 2, 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;

dh/1) kontrolluesit dhe përpunuesit, që veprojnë në kundërshtim me pikën 2 të nenit 32 të këtij ligji, dënohen me 100 000 deri në 1 000 000 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 se shkeljet e konstatuara dhe pasojat janë serioze. Ato lidhen në veçanti me zbatueshmërinë e masave teknike dhe organizative në proceset përpunuese dhe me garantimin e parimeve dhe përpunimin e ligjshëm të të dhënave personale.

Gjithashtu, Vendimi i Komisionerit bazohet edhe në faktin që, në vitin 2021 ky kontrollues është sanksionuar me gjobë në rrethana rënduese (për shkelje të detyrimeve të parashikuara në nenin 32 të ligjit, konkretisht për mungesë bashkëpunimi me Zyrën e Komisionerit) dhe nuk ka marrë masa për plotësimin e rekomandimeve të lëna nëpërmjet këtij Vendimi.

PËR KËTO ARSYE:

Në zbatim të neneve 5, 6, 18, 20, 21, 22, 27, 28, 32, 39 pika 1, germat *"a", "b", "ç", "d", "dh", "dh/1"* dhe 39 pika 2, të Ligjit,

V E N D O S A:

1. Dënimin e kontrolluesit me gjobë në vlerën 300 000 (treqind mijë) Lekë, për shkelje të detyrimeve të përcaktuara në Kreun II të Ligjit;

2. Dënimin e Kontrolluesit me gjobë në vlerën 150 000 (njëqind e pesëdhjetë mijë) Lekë, për shkelje të detyrimeve të përcaktuara në nenin 18 të Ligjit;

3. Dënimin e Kontrolluesit me gjobë në vlerën 480 000 (katërqind e tetëdhjetë mijë) Lekë, për shkelje të detyrimeve të përcaktuara në nenin 20 të Ligjit;

4. Dënimin e Kontrolluesit me gjobë në vlerën 250 000 (dyqind e pesëdhjetë mijë) Lekë, për shkelje të detyrimeve të përcaktuara në nenet 21 dhe 22 të Ligjit;

5. Dënimin e Kontrolluesit me gjobë në vlerën 240 000 (dyqind e dyzetë mijë) Lekë, për shkelje të detyrimeve të përcaktuara në nenet 27 dhe 28 të Ligjit;

6. Dënimin e Kontrolluesit me gjobë në vlerën 1 600 000 (një milion e gjashtëqind mijë) Lekë, për shkelje të detyrimeve të përcaktuara në nenin 32 të Ligjit;

7. Kontrolluesi, të marrë masa për përpunimin e të dhënave personale në përputhje me dispozitat e parashikuara në nenet 5 dhe 6 të Ligjit;

8. Kontrolluesi, të përcaktojë në mëyrë të qartë databazat në të cilat legjitimohet të ketë akses dhe kategoritë e të dhënave që duhet të aksesoj në secilën databazë si dhe të marrë masa të menjëhershme në drejtim të ndalimit të aksesit të paligjshëm, në ato databaza, aksesi në të cilat, është në tejkalim të parimit të mjaftueshmërisë së të dhënave, sipas parashikimit në germën "c" të pikës 1, të nenit 5 të Ligjit;

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

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

11. Kontrolluesi, në zbatim të nenit 27 të Ligjit, të hartojë "*Rregulloren për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale*", duke parashikuar masa konkrete teknike dhe organizative për mbrojtjen e të dhënave personale, mënyrat e përpunimit të të dhënave, të drejtat e subjekteve të të dhënave, etj.

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

13. 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 7, më sipër;
    (ii) menjëherë, detyrimet e treguara në pikën 8, më sipër;
    (iii) brenda 15 (pesëmbëdhjetë) ditëve, detyrimet e treguara në pikat 9 dhe 10, më sipër;
    (iv) brenda 30 (tridhjetë) ditëve, detyrimet e treguara në pikën 11, më sipër;
    (v) brenda 45 (dyzetë e pesë) ditëve, detyrimet e përcaktuara në pikën 12, më sipër.

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

14. Kontrolluesi të njoftojë Komisionerin për masat e marra;

15. 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;

16. 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 24.11.2022.

KOMISIONERI

Besnik Dervishi