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.381/2 prot. Tiranë më 24.11.2022

VENDIM

Nr. 51, datë 24.11.2022

PËR KONTROLLUESIN "DREJTORIA E PËRGJITHSHME E SHËRBIMEVE TË TRANSPORTIT RRUGOR"

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 Shërbimeve të Transportit Rrugor"* (në vijim, *"Kontrolluesi"* dhe/ose *"DPSHTRR"*),

KONSTATOVA SE:

Në zbatim të Urdhrit nr. 208, datë 28.12.2021 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 *"pronar automjetesh",* 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 24.12.2021, media të ndryshme publikuan një lajm me titull *"Pas pagave, dalin edhe targat e makinave të shqiptarëve",* i cili gjendet në lidhjen 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 530 mijë subjekteve të të dhënave, pronarë automjetesh.

Zyra e Komisionerit administroi një kopje të bazës së të dhënave në të cilën rezultojnë të përpunuara të dhënat personale të 530,452 (pesëqind e tridhjetë mijë e katërqind e pesëdhjetë e dy) subjekteve të të dhënave (në vijim, *"Baza e të Dhënave"*).

Nga të dhënat e materialit elektronik të Bazës së të Dhënave në formatin *Microsoft Exel*, konstatohet se ajo është krijuar më datë 09.02.2021, ora 01:04 PM, me përmasa 29.5 MB. Materiali elektronik është i organizuar në dy faqe (*"sheet1" dhe "sheet2"*).

"Sheet1" i materialit elektronik konsiston në një informacion të organizuar, me mundësi filtrimi sipas kategorive (shtyllave) *"targa e mjetit", "marka e mjetit", "modeli i mjetit", "ngjyra e mjetit", "Numër identifikimi (NID) i subjektit të të dhënave (zotëruesit)", "emër", "mbiemër",* dhe përmban 530,452 regjistrime (targa/mjete).

"Sheet2" i materialit elektronik konsiston në një informacion të organizuar, me mundësi filtrimi sipas kategorive (shtyllave) *"Targa e mjetit", "marka e mjetit", "modeli i mjetit", "ngjyra e mjetit", "numër identifikimi (NUIS) i personit fizik tregtar ose personit juridik",* dhe përmban 61,513 regjistrime (targa/mjete).

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.

Nga konstatimet rezulton se, Baza e të Dhënave qarkulloi nëpërmjet kanaleve të ndryshme të komunikimit, të tilla si platforma *WhatsApp*, faqe 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 Autoritetit të Mediave Audiovizive (AMA) për bllokimin e menjëhershëm të tyre, si dhe fillimin e procedimit ligjor të personave që zotërojnë/posedojnë këto faqe interneti, në të cilat rezultonin të publikuara të dhënat personale të shtetasve që supozohen të jenë marrë nga Baza e të Dhënave.

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 ligjore të përpunimit, sipas parashikimeve në nenet 5 dhe 6 të Ligjit.

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

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 ligjore të përpunimit të të dhënave personale, Zyra e Komisionerit vlerëson se përhapja masive e saj, përbën cënim 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 ndërmarrë kryesisht nga Zyra e Komisionerit, bazuar në sa është parashtruar në pikën 1 më sipër. Kontrolluesi është institucion shtetëror, i krijuar me Vendim të Këshillit të Ministrave Nr. 343, datë 21.07.1999, në zbatim të Ligjit nr. 8378, dt. 22 07.1998 *"Kodi Rrugor i Republikës së Shqipërisë"* i ndryshuar, me vetëfinancim, me kapital tërësisht shtetëror, mbi bazën e pasurisë dhe kapitalit të Ndërmarrjes së Shërbimeve të Transportit Rrugor. Kontrolluesi ofron shërbim përmes 13 Drejtorive Rajonale dhe zyrave të shërbimit të transportit rrugor. Kontrolluesi ka në objektin e veprimtarisë së tij: "*Shërbimet për mjetin", "Leje Drejtimi dhe Autoshkolla", "Dëshmi, Certifikata dhe Licenca", "Kontrolli Teknik i Mjeteve", "Regjistri Kombëtar i Mjeteve dhe Drejtuesve të tyre", "Agjent Tatimor për Taksat e Mjeteve", "Prodhim i Targave dhe Shtypshkrimeve", "Siguria Rrugore", "Retro"* .

Kontrolluesi mbledh dhe përpunon të dhëna personale, për kategoritë e subjekteve të të dhënave: *"pronar automjetesh", "subjekte që pajisen me leje drejtimi", "subjekte që pajisjen me dëshmi mbi kategoritë e mjeteve", "subjekte që përfshihen në regjistrin e mjeteve", "subjektet e taksave vjetore të mjeteve", "subjekte që përfshihen në regjistrin e mjeteve historike RETRO",* etj. Përpunimi i të dhënave kryhet në mënyrë manuale dhe elektronike. Sistemi elektronik i Kontrolluesit, shërben si një sistem i automatizuar për veprimtarinë e administratës, për të përmbushur detyrimet ligjore sipas legjislacionit në fuqi.

Nga krahasimi i kryer me të dhënat që DPSHTRR ka në sistemin elektronik të pronësisë së automjetit, me ato të "*Bazë*s së të Dhënave", që kanë rrjedhur në platformat e ndryshme teknologjike, rezulton se përkojnë me 7 kategori të dhënash. konkretisht:

1. Emër;
2. Mbiemër;
3. Numri i targës së automjetit;
4. Numri personal NID;
5. Tipi i markës;
6. Tipi i modelit të markës;
7. Ngjyra e automjetit.

3. Nga verifikimi i kryer rezulton se Kontrolluesi ka ndërtuar sisteme elektronike mbi të cilat kryen aktivitetin funksional për shërbimet e cituara më sipër. Veprimtaria e institucionit realizohet, ndër të tjera, nëpërmjet sistemit elektronik *"eDPSHTRR"*.

Referuar dokumentit elektronik *"TORs-Upgrade i sistemit eDPSHTRR"*, baza ligjore për ushtrimin e veprimtarisë së DPSHTRR për shërbimet e ofruara në sistemin *"eDPSHTRR"* mbështetet në:

- Ligjin nr. 8378, datë 22.07.1998 *"Kodi Rrugor i Republikës së Shqipërisë",* i ndryshuar, dhe aktet nënligjore të Këshillit të Ministrave të dala në bazë dhe zbatim të ligjit;
- Ligji nr. 8308, datë 18.03.1998 *"Për transportet rrugore",* i ndryshuar;
- Ligjin nr. 9975, datë 28.07.2008 *"Për taksat kombëtare",* i ndryshuar dhe aktet nënligjore të Këshillit të Ministrave dhe/ose Ministrisë së Financave të dala në bazë dhe zbatim të ligjit;
- Ligjin nr. 10325, datë 23.09.2010 *"Për bazat e të dhënave shtetërore",* si dhe VKM nr.945, datë 02.11.2012 Për miratimin e Rregullores *"Administrimi i sistemit të bazave të të dhënave shtetërore"* .

Të dhënat teknike të sistemit *"eDPSHTRR"* konsistojnë si më poshtë:

- Baza e të dhënave të sistemit "*eDPSHTRR*" është ndërtuar me qëllim regjistrimin e të dhënave të mjeteve që qarkullojnë në Republikën e Shqipërisë nga qytetarë apo biznese, si dhe marrjen e shërbimeve të ndryshme në lidhje me mjetin;
- Baza e të dhënave të sistemit *"eDPSHTRR"* është e ndërtuar në SQL Server 2012;
- Emri i bazës së të dhënave është *"eDPSHTRR"*;
- Aksesimi i bazës së të dhënave nga Drejtoritë Rajonale dhe/ose palë të treta, kryhet nëpërmjet një lidhjeje me VPN;
- VPN ofron konfidencialitet të të dhënave pasi ato duhet të 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 t'u përdorur;
- Kjo bazë të dhënash përdor modelin *"Full Recovery"*, në mënyrë që çdo veprim i kryer mbi databazën të ruhet në log të përgjithshëm.

Sistemi "*eDPSHTRR*" hostohet në ambientet e DPSHTRR dhe të gjitha Drejtoritë Rajonale kanë mundësi që ta aksesojnë, nëpërmjet një lidhje VPN.

Zgjidhja teknike sipas modelit *"Failover"* është implementuar nëpërmjet pajisjeve *Rendundante Server*. Nga *Cluster*-i, garantohet disponueshmëri e lartë (*High Avaibility*) për të gjithë shërbimet që hostohen në të. Shtresa e aplikimit, *Domain Controller*-i sekondar, sistemi i raporteve, si edhe sistemi *"test"*, konsistojnë në makina virtuale, *Highly Available*, nga dy për secilin rol, të mbështetura mbi këtë *Hyper-V Failover Cluster*.
Një server fizik luan rolin e *Domain Controller*-it primar. Janë dy servera të konfiguruar në *High Available* sipas metodave të Microsoft për Virtualizim dhe *Failover*. Shtresa e bazës së të dhënave konsiston në makina fizike të dedikuara, mbi të cilat është krijuar një *Cluster* për të siguruar vazhdueshmërinë e shërbimit në rast dështimi *"fail"* të njërës nyje (*node*) të komunikimit. Komponentet e infrastrukturës

së rrjetit përfshijnë: *Firewall Solution, Hardware Load Balancer, Core Switches, Aggregation Switches*.

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 *"eDPSHTRR"* duhet të ketë një nivel të lartë sigurie, të nivelit D2l2Kl.

Në sistemin *"eDPSHTRR"* ka dy dhënës informacioni me të cilët popullohet baza e të dhënave. Më konkretisht, dhënësit e informacionit për sistemin *"eDPSHTRR"* janë Qendra Kombëtare e Biznesit (QKB) dhe Drejtoria e Përgjithshme e Gjendjes Civile (DPGJC). Nëpërmjet tyre, sistemi *"eDPSHTRR"* popullon bazën e të dhënave me informacionin bazë të aplikantëve, të cilët mund të jenë individë ose biznese.

Të dhënat parësore që krijohen nga DPSHTRR, për sistemin *"eDPSHTRR",* janë si më poshtë vijon:

- Të dhëna për shërbimet si emri i shërbimit, kodi që shërben për identifikimin e tij pasi është unik, kategoria e shërbimit, tarifa e shërbimit etj.
- Të dhëna për aplikimin, përfshin të dhënat për aplikimin që kanë bërë qytetarët/bizneset për të marrë një shërbim të caktuar.
- Të dhënat për regjistrimin e mjeteve, përfshin Regjistrin Kombëtar të të gjithë mjeteve që janë regjistruar në Republikën e Shqipërisë.

Në tabelën e mëposhtme jepen më të detajuara të dhënat parësore të sistemit *"eDPSHTRR"*.

Shërbimet	**Aplikimet**	**Regjistër Mjeti**
1. Emërtimi i shërbimit	1. Numri i aplikimit	1. Nr. Shasie
2. Përshkrimi i shërbimit	2. Data e aplikimit	2.Markë
3. Kategoria e shërbimit	3. Dokumentet e aplikimit	3. Model
4. Lloji i aplikimit (qytetarë / biznese)	4. Formulari i aplikimit	4. Vit Prodhimi
5.Kodi i shërbimit (automatik / manual)	5. Numri i protokollit	5. Nr. i Dyerve
6. Tarifa e shërbimit	6. Mënyra e njoftimit	6. Cilindrat Motori
7. Ditët e procesimit	7. Mënyra e marrjes së përgjigjes	7. Pesha Maksimale
8.Dokumentet e shërbimit ligjor	8.Dokumentet e aplikantit	8. Pronari i mjetit
	9. Statusi i aplikimit	9. Targë
	10.Data e marrjes së përgjigjes	10. Nr. Leje Qarkullimi

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 *"eDPSHTRR".* Dhënia e të drejtave një përdoruesi, 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 dhe për të shfaqur vetëm *links*/butona me të cilat përdoruesi është i autorizuar të ndërveprojë. 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 (menu, nyje dhe funksionalitete). Kur një përdoruesi i caktohet një rol, automatikisht i jepen të drejta mbi profilin e këtij roli.

Subjektet e interesuara në sistemin "*eDPSHTRR*" duhet të jenë të organizuara në role sipas funksioneve të punës. Rolet e sistemit kanë nivele të ndryshme aksesi në varësi të specifikave dhe të drejtave që ata kanë në sistem. Më poshtë shpjegohen të drejtat për secilin rol që do të aksesojë sistemin:

- Administrator Sistemi - Roli me të drejta të plota në të gjithë sistemin. Merret me menaxhimin e përdoruesve dhe përcaktimin e të drejtave, menaxhon të dhënat e referencës, etj.;
- Arkëtar - Roli i cili ka të drejtën e gjenerimit të taksave, gjobës KTV (kontrolli teknik vjetor) dhe arkëtimin e tyre, si dhe arkëtimin e faturave të shërbimeve në arkë. Kryen anulimin e faturave të papaguara;
- Ekonomist Taksa - Roli i cili pasqyron në sistem pagesat e kryera nëpërmjet bankës;
- Inspektori i Identifikuesit Teknik të Mjetit - Roli që ka të drejtë të krijojë aplikime për kontroll fizik të mjetit dhe të regjistrojë masat administrative për mjetet me ndryshim të karakteristikave konstruktive dhe funksionale pa miratim paraprak;
- Përgjegjës Regjistrimi Mjeti - Roli që ka të drejtë të krijojë aplikime për shërbimet që janë pjesë e modulit të regjistrimit të mjetit dhe të kryejë korrigjime në të dhënat e lejes, mjetit, pronësisë;
- Operator Mjeti - Roli që ka të drejtë të kontrollojë të dhënat e arkivit të mjeteve, taksave, gjobave dhe të regjistrojë vendimet e bllokimit dhe zhbllokimit te veprimeve me mjetet;
- Informacioni - Roli që ka të drejtë të kontrollojë të dhënat e arkivit të mjeteve, taksave, gjobave;
- Specialist Finance - Roli që ka të drejtë të kontrollojë të dhënat e arkivit të mjeteve, taksave, gjobave të autorizimit në sistem, pagesat e kryera nëpërmjet bankës si dhe të anulimit të pagesave të kryera;
- Specialist Interpoli - Roli që ka të drejtë të plotësojë regjistrin e mjeteve të cilët lejohen të kryejnë veprime pavarësisht statusit në Interpol;
- Specialist Shërbimi Mjeti - Roli që ka të drejtë të krijojë aplikime për shërbimet që janë pjesë e modulit të regjistrimit të mjetit;
- Inspektor i Kontrollit në Rrugë - Roli që ka të drejtë të krijojë gjoba të *Task Force*-s, të japë vendim për gjoba dhe të parashkruajë gjoba;

- Jurist - Roli që ka të drejtë të krijojë aplikime për shërbimet që janë pjesë e modulit të regjistrimit të Kontratave të Shit-Blerjes;
- Specialist Licence - Roli që ka të drejtë të krijojë aplikime për shërbimet që janë pjesë e modulit të liçencave;
- Arkiva - Roli që ka të drejtë të shikojë cilat dosje janë pjesë e drejtorisë së atij përdoruesi, të konfirmojë Dosjet Hyrje, Dosjet Dalje, të shikojë historikun e transferimit të një dosje nga një Drejtori Rajonale në një tjetër;
- Komisioner DPSHTRR - Roli i cili ka të drejtë të japë vendim për Kërkesat për Ndryshime Konstruktive të Mjetit;
- Magazina DTSH - Roli i cili administron magazinën e targave të DTSH. Ka mundësi të regjistrojë targa, të konfirmojë Urdhër - Stampime për targat, të konfirmojë/anulojë kërkesa për targa, të shikojë historikun e një targe, të ndryshojë kategorinë e një targe nga LUX në SIMPLE, të shikojë rezervimet online të targave;
- Magazina e Drejtorisë Rajonale - Roli i cili administron magazinën e targave të Drejtorisë Rajonale. Ka mundësi të dërgojë kërkesa për targa, të shikojë historikun e një targe, të shikojë targat hyrje dhe targat dalje, të marrë kërkesa nga drejtoritë e tjera rajonale.

Në dokumentacionin e hartimit të termave teknik janë parashikuar dhe dështimet e serverit të bazës së të dhënave (dështim fizik), kur kjo e fundit kalon në një gjendje jo konsistente. Për të shmangur këto situata është menduar të ndiqet një plan dhe një model *backup*-i/*recover*-i.
Gjithashtu, është planifikuar të ndërtohet një plan për mirëmbajtjen e bazës së të dhënave, konkretisht sipas modelit *full recovery*, me *backup*-e diferenciale çdo 4 orë dhe *backup*-e *log*-esh çdo 15 minuta, për t'u siguruar që humbja e të dhënave është e minimizuar. Sipas punës duhet të veprohet me *tape-backup* të *backup*-eve të plota për të siguruar rikthimin e të dhënave kur është e nevojshme ose për qëllime auditimi.
Po ashtu, përveç *backup*-eve të bazës së të dhënave, duhet të kryhen edhe *backup*-e të skedareve të sistemit *"eDPSHTRR"* si dhe *backup*-e në nivel të sistemit të operimit (në baza javore).

Referuar dokumentacionit teknik, skedarët e *backup*-eve duhet të krijohen në *"clite"* të ndryshme. Kur krijohet një *backup* i ri, *backup*-et e *"clites"* së mëparshme duhet 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 disponushëm 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 do të ruhen në një vend që ofron siguri fizike dhe akses të kontrolluar. Mjedisi i ruajtjes së *backup*-it si *hard drive/storage, disk-s* apo tape-s, duhet të jetë në një arkiv të organizuar. Për menaxhimin e hapësirës së alokuar nga *backup*-et, ripërdorimin apo shkatërrimin e tyre, duhet të ndiqen procedura të mirëpërcaktuara, të ndjekura nga protokollet që do të nënshkruhen.

Shtresa e integrimeve/ndërveprimeve nëpërmjet shërbimit *web-service* është një komponent i rëndësishëm i sistemit *"eDPSHTRR"*. Kjo shtresë ofron mundësi integruese midis komponentëve të sistemit *"eDPSHTRR"* dhe në të njëjtën kohë midis *"eDPSHTRR"* dhe sistemeve të tjera të palëve të treta. Duke qenë se sistemi *"eDPSHTRR"* është i integruar në Government Gateway (GG), ai mund të komunikojë me sisteme të tjera për të marrë dhe/ose dhënë (*In/Out*) të dhëna. Integrimet me sistemet e jashtme duhet të jenë shumë të rëndësishme pasi gjatë regjistrimit të aplikimit, një nga hapat e përdoruesit është *marrja e të dhënave nga sistemet e jashtme* (thirrja e të dhënave dytësore nga sistemet e tjera). Më poshtë paraqiten thirrjet e të dhënave dytësore që përdor sistemi *"eDPSHTRR",* si:

- **Integrimi me QKB** - përdoruesi përcakton NUIS-in në formën përkatëse si të dhëna hyrëse dhe merr si përgjigje të dhënat e biznesit si psh: emrin, formën ligjore, adresën e biznesit etj.
- **Integrimi me DPGJC** - përdoruesi përcakton NID-in në formën përkatëse si të dhëna hyrëse dhe merr si përgjigje të dhënat e individit si psh: emrin, mbiemrin, ditëlindjen, adresën e individit etj.

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 komponentëve të *"eDPSHTRR".*

Sistemi është ndërtuar mbi bazë të moduleve/nënsistemeve kryesore. Modulet kryesore të sistemit listohen si më poshtë:

- Moduli i hyrjes në sistem;
- Moduli i roleve dhe përdoruesve të sistemit;
- Moduli i menaxhimit të konfigurimeve;
- Moduli i shërbimeve të mjetit;
- Moduli i faturimit dhe i pagesave;
- Moduli i administrimit të targave;
- Moduli i administrimit të licencave të transportit;
- Moduli i administrimit të gjobave;
- Moduli i administrimit të taksave;
- Moduli i raporteve të sistemit;
- Moduli për kërkimet dinamike;
- Moduli për regjistrin e aksidenteve.

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

- Nuk ka formalizuar një procedurë zyrtare të raportimit dhe menaxhimit ndaj incidenteve të teknologjisë së informacionit;
- Nuk ka të identifikuar sistemet ose pjesët e tyre të cilat janë kritike për ofrimin e shërbimit 24 orë në 7 ditë të javës;
- Nuk ka plane të dokumentuara për menaxhimin e riskut, teknikat e menaxhimit dhe të performancës së tij;

- Nuk janë 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 të hartuar planin e politikave të vazhdueshmërisë së biznesit si dhe një plan për ruajtjen e informacionit, dokumente këto që do të duhet të përmbanin politikat dhe objektivat që sigurojnë vazhdueshmërinë e punës së sistemeve;
- Konstatohen mangësi në hartimin dhe dokumentimin e planit të rimëkëmbjes nga katastrofa, i cili duhej të përmbante masa dhe procedura të mirëdokumentuara për rivendosjen në funksionim të sistemit në rastet e emergjencave. Në këto procedura duhet të ishte 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;
- Konstatohet se në ambientin *"test"* të *"eDPSHTRR",* punohet me të dhëna reale.

Gjatë inspektimit u konstatua se, politikat mbi gjurmët (*log*-et) në sistemin *"eDPSHTRR"* dhe infrastrukturën TIK mbështetëse, nuk zbatohen sipas një procedure të rregulluar, me risk në qasje të paautorizuar në të dhënat, kërcënim të sigurisë në fushën e teknologjisë së informacionit dhe mungesë transparence. Nga verifikimi i kontrolleve të loge-ve në hedhjen e të dhënave dhe *"login-et"* në sistem, të cilat gjenerohen nga sistemi i *"eDPSHTRR",* konstatohet që *log*-et nuk analizohen nëpërmjet një ndërfaqe aplikative të posaçme, e cila të mundësojë një shfletim në kohe reale të tyre. Në këtë mënyrë specialisti përgjegjës nuk ka akses në mënyrë të shpejtë për të bërë kërkime si: tentativat e dështuara për *"login"*, numrin e *"login"* nga një PC, etj., me qëllim monitorimin dhe funksionimin e sistemit.

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 rimëkëmbjes nga katastrofa (DRP), në kundërshtim kjo me aktet ligjore apo nënligjorë në fuqi. U konstatua se procedura e *backup*-it për Sistemet e Informacionit në DPSHTRR nuk janë në përputhje me VKM nr. 945, datë 2.11.2012 *"Për Miratimin e Rregullores "Administrimi i Sistemit të Bazave të të Dhënave Shtetërore""* i ndryshuar, dhe VKM nr. 710, datë 21.08.2013 *"Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit"*, të cilat kanë për qëllim përcaktimin e procedurave standarde të politikave të administrimit dhe funksionimit të sistemeve. Nga verifikimi rezulton se *backup*-et tek AKSHI kryhet automatikisht pa u mbështetur në procedurat e parashikuara nga VKM-të e sipër cituara. Nuk u gjetën procedura të testimit të *backup*-it. Kopjet (*backup*) e të dhënave nuk testohen rregullisht për t'u siguruar që mund të përdoren në raste të nevojshme. Kopjet e këtyre *backup*-eve janë marrë si të mirëqena nga DPSHTRR 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 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 *"eDPSHTRR"*, janë konstatuar disa problematika me ndikim/impakt në sigurinë e të dhënave, si vijon:

- Në sistem rezultojnë si përdorues me status aktiv edhe punonjësit të cilët kanë ndërprerë marrëdhëniet e punës;
- Data e përfundimit të përgjegjësisë (largimi nga funksioni) 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 sistem rezultojnë si përdorues mbi 1900 *user*-a, plus *user*-at që janë përdorur për testimet e implementimit të sistemit, apo përdorues të krijuar me të dhëna jo të plota për emrin. Referuar organigramës, rezulton se duhet të jenë përafërsisht 600 usera/përdorues të sistemit *"eDSHPTRR"* për kryerjen e detyrave funksionale në të gjithë Drejtoritë Rajonale përfshirë edhe administratën qendrore të DPSHTRR;
- Administratorët e sistemit, nuk i kanë sistemuar përdoruesit në *"eDPSHTRR"*, duke populluar për çdo rast të dhëna mbi datën e fillimit dhe të drejtat e tyre në sistem.

Baza e të dhënave të sistemit *"eDSHPTRR"* është e regjistruar si bazë të dhënash shtetërore në Autoritetin Rregullator Kombëtar (ARK) që prej datës 17.12.2015, me emërtimet *"Regjistri Kombëtar i Personave të Aftësuar për Drejtimin e Mjeteve"* si dhe *"Regjistri Kombëtar i Mjeteve",* por nuk ka vijuar me përditësimin e bazave të të dhënave të regjistruara, në kundërshtim me dispozitat e VKM-së nr. 945 datë 02.11.2012 *"Për miratimin e rregullores "Administrimi i sistemit të bazave të të dhënave shtetërore*". Regjistrimi dhe përditësimi i bazës së të dhënave është i nevojshëm për standardizimin dhe sigurinë e saj.

Zyra e Komisionerit vlerëson se, krijimi i procedurave dhe politikave të përdorimit të infrastrukturës TIK dhe sistemeve elektronike (konkretisht sistemit *"eDSHPTRR"*) është një ndër masat kryesore që duhet të ndërmarrë Kontrolluesi, në lidhje me sigurinë dhe funksionimin e sistemeve të teknologjisë së informacionit.

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 riskun dhe lokalizon problemin.

Krijimi i procedurave të *backup*-it dhe vazhdimësisë së punës për Sistemet e Informacionit në sistemin *"eDSHPTRR",* duhet të jetë në përputhje me VKM nr. 945/2012 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"*.

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

Menaxhimi i përdoruesve të sistemit "*eDPSHTRR"* 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 *"eDPSHTRR"* 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.

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"*).

4. Në kuadër të detyrimeve ligjore të funksionimit të institucioneve të tjerë shtetëror, DPSHTRR ofron për këta të fundit, mundësinë e aksesit në të dhënat e sistemit *"eDPSHTRR",* në tre mënyra, që janë:

a. Aksesi nëpërmjet web-service:
Referuar termave teknike, rezulton se janë parashikuar 4 institucione (Prokuroria, Autoriteti i Mbikëqyrjes Financiare, Ministria e Shëndetësisë dhe Mbrojtjes Sociale dhe Policia e Shtetit) për të pasur akses/ndërveprime në të dhënat e kësaj baze të dhënash, por nga verifikimet në sistem rezulton se janë më shumë se 4 institucione publike të cilët kanë akses/ndërveprime në sistemin elektronik, nëpërmjet shërbimit *"web-service"* (shërbime ndërlidhëse të automatizuara midis sistemeve).
Pavarësisht parashikimeve të termave teknikë, rezulton se ka një numër institucionesh publike të cilave iu është dhënë akses në sistemin elektronik mbi bazën e marrëveshjeve të bashkëpunimit ose të ngjashme me to. Kontrolluesi ka të planifikuar në projektin teknik edhe *web-service* me qëllim ndërveprimin nëpërmjet Government Gateway (GG) dhe portalit unik qeveritar e-Albania.

Bazuar në pikën 7 të VKM nr. 673, datë 22.11.2017 *"Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit"* i ndryshuar (në vijim, *"VKM nr. 673"*), Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI) është përgjegjës për krijimin e kushteve të nevojshme për ekspozimin e *web-serviceve* të ndryshme të bazave të të dhënave, konkretisht të *"eDPSHTRR",* me qëllim aksesimin e të dhënave parësore nëpërmjet portalit unik qevertiar 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 e administratës të cilët identifikohen në sistem nëpërmjet *"emrit të përdoruesit"* dhe *"fjalëkalimit përkatës",* nëpërmjet VPN.

c. Aksesi në mënyrë manuale i cili konsiston në nxjerrjen e të dhënave dhe vënien në dispozicion të palëve të treta në mënyrë manuale në *"hard copy"*.

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). Kontrolluesi nuk ka strukturë NJTIK sipas përcaktimeve të VKM-së të sipërcituar.

Pranë Kontrolluesit ekziston struktura me emërtim *"Drejtoria e Administrimit dhe Monitorimit"*, e cila administron sistemin *"eDPSHTRR"* së bashku me komponentët e tjerë të teknologjisë dhe informacionit. Gjithashtu, Në aktivet e Kontrolluesit rezulton se pajisjet TIK si dhe të sistemit primar janë pjesë e inventarit të DPSHTRR. Si rrjedhojë DPSHTRR është zotërues i pajisjeve/aktiveve, sipas përcaktimit të ligjit nr. 10296, 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.

DPSHTRR mbledh dhe përpunon të dhëna personale në zbatim të ligjit Nr. 8378, datë 22.07.1998 *"Kodi Rrugor i Republikës së Shqipërisë"*, si institucion me vetëfinancim, me kapital tërësisht shtetëror, mbi bazën e pasurisë dhe kapitalit të Ndërmarrjes së Shërbimeve të Transportit Rrugor. Të dhënat parësore që popullojnë sistemin

"eDPSHTRR", përpunohen për përmbushjen e detyrimeve të këtij ligji. Referuar pikës 5, të nenit 3 të Ligjit, DPSHTRR gëzon 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, dhe përgjigjet edhe për përmbushjen e detyrimeve të përcaktuara në Ligj.

Sa më sipër, konstatohet se, sa i përket aksesit nga palët e treta nëpërmjet web service-ve dhe qendrës së ndërveprimit GG, Kontrolluesi nuk ka marrë masa të përshtatshme për formalizimin dhe dokumentimin e politikave dhe procedurave të mënyrës së dhënies së të drejtës së aksesit.

Përhapja e të dhënave, si formë e posaçme përpunimi (siç përkufizohet 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.

Gjithashtu, bazuar në nenet 27 dhe 28 të Ligjit, DPSHTRR mbart detyrimin kryesor për marrjen e masave tekniko-organizative, për të garantuar sigurinë dhe konfidencialitetin e të dhënave personale.

Nga përgjigjet/pretendimet e DPSHTRR, aspektet e sigurisë së të dhënave dhe marrëdhëniet me përpunues të tjerë (përfshirë mirëmbajtës) mbulohen nga AKSHI.

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.

Bazuar në dispozitat e Udhëzimit nr. 47, Kontrolluesit janë përgjegjës për krijimin, administrimin dhe mirëmbajtjen e Sistemeve të Menaxhimit të Sigurisë së Informacionit (SMSI) për mbrojtjen e të dhënave personale, qoftë kur përpunojnë të dhënat me kapacitetet e tyre teknike dhe njerëzore, edhe kur për ruajtjen e sigurisë dhe konfidencialitetit të të dhënave angazhohen subjekte të tjera, rast në të cilin Kontrolluesi është i detyruar të veprojë edhe në përputhje me dispozitat e nenit 20 të Ligjit dhe Udhëzimin nr. 19, datë 03.08.2012, të Komisionerit *"Për 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"*).

5. Kontrolluesi, nëpërmjet shkresës nr. 6357 Prot., datë 11.03.2022, vendosi në dispozicion të grupit të hetimit administrativ, loget e sistemit me referenca:

- **Log_30_12_2021_Server30:**
  i. Loget për eventin Loge_DB përmbajnë informacion mbi gjurmushmërinë e eventeve të kryera në databazën e sistemit *"eDPSHTRR"* për periudhën 1 vjeçare dhjetor 2020 – dhjetor 2021 të server 30. Të dhënat mbi eventet e database ku ngrihet sistemi *"eDPSHTRR"* përbëhet nga evente

(gjurmueshmëri): AHCEvent, AMFEvent, ArchiveEvent, AX_AuditTrail, AX_EventLog, AX_UserEvents, BillingEvent, CoreEvent, eDPSHTRR_event mbi lejen e qarkullimit, eDPSHTRR_event mbi të dhënat e automjeteve, eTransport event, event, FineEvent, invoice event, Idf, MahaEvent, MMSR Event, Police Event, Reservation event, search event, SGSEvent, SQLServerLogs, TaxEvent, etj.,

ii. Reporting Services: përmban informacion të tipit Microsoft ReportingServices Portal WebHost (raporte mbi serviset e SQL).

- **Log_30_12_2021_Server31**:
  i. Reporting Services: përmban informacion të tipit Microsoft ReportingServices Portal WebHost (raporte mbi serviset e SQL).

- **Log_30_12_2021_Server32**:
  i. Loget për eventin AppData përmbajnë informacion mbi gjurmushmërinë e eventeve të kryera në databazën e sistemit *"eDPSHTRR"* për periudhën 2019 dhe në vazhdim të server 32. Të dhënat mbi eventet e aplikacioneve të ndryshme që janë në funksion të sistemit *"eDPSHTRR"*.
  ii. Loget për logFiles paraqesin gjurmueshmërinë mbi identifikimin e proceseve të niveleve të aplikacioneve që ngrihen mbi sistemin *"eDPSHTRR"*.

- **Log_30_12_2021_Server33**:
  i. Loget për eventin AppData përmbajnë informacion mbi gjurmushmërinë e eventeve të kryera në databazën e sistemit *"eDPSHTRR"* për periudhën 2019 dhe në vazhdim të server 33. Të dhënat mbi eventet e aplikacioneve të ndryshme që janë në funksion të sistemit *"eDPSHTRR"*.
  ii. Loget për logFiles paraqesin gjurmueshmërinë mbi identifikimin e proceseve të niveleve të aplikacioneve që ngrihen mbi sistemin *"eDPSHTRR"*.

Nga shqyrtimi i eventeve të logeve të vëna në dispozicion, konstatohet se nuk dokumentohen të gjithë loget sipas akt-marrëveshjeve të ndryshme që DPSHTRR ka me palë të treta, në lidhje me ndërveprimin e tyre në sistemin *"eDPSHTRR"* si dhe veprimeve të kryera nga vet nëpunësit e Kontrolluesit, pjesë e sistemit. Gjithashtu, Kontrolluesi nuk arrin të provojë dhe dokumentojë veprimtarinë që ka kryer secili rol që ka akses në sistemin *"eDPSHTRR"* dhe që ka atribute në të dhënat e plota të automjeteve. Dokumentimi duhet të përmbajë Urdhërat nga eprorët, kërkesa me shkrim procese periodike të punës sipas përshkrimit të punës së punonjësit, etj. Në këtë situatë, kur Kontrolluesi, ndër të tjera, është në pamundësi për dokumentimin e veprimtarisë së punonjësve, në mungesë të një politike rregullatore specifike për sistemin *"eDPSHTRR"* mbi proceset e punës, bëhet i pamundur identifikimi i rrjedhjes së të dhënave.

Sa më sipër, Kontrolluesi është në pamundësi të demonstrimit të masave teknike dhe organizative të ndërmarra, në kundërshtim të dispozitave të parashikuara në nenin 27 të Ligjit.

Zyra e Komisionerit vlerëson, se mos dokumentimi i plotë i logeve/eventeve, të cilat identifikojnë veprime të përdoruesve dhe/ose funksionalitete të sistemit, pengon një analizim të gjerë të sistemit.

Kontrolluesi duhet të jetë në gjendje të analizojë dhe të dokumentojë në çdo kohë veprime të përdoruesve që kanë llogari dhe atribute sipas funksionaliteteve përkatëse në sistemin elektronik *"eDPSHTRR"*. Gjithashtu, për çdo ndërveprim që kryhet me sisteme të tjera elektronike nga palë të treta, duhet të mundësohet gjurmueshmëria e veprimeve për çdo proces përpunimi.

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:

a. Akt-Marrëveshje për bashkëpunim dhe shkëmbim informacioni me Drejtorinë e Policisë së Shtetit, për strukturën OFL, me nr. 11333/2, datë 26.06.2020;

Konstatohet se në nenin 3 të kësaj Marrëveshje, përcaktohen detyrimet e DPSHTRR-së. Në pikën 3 të këtij neni, përcaktohet ndër të tjera se, komunikimi midis institucioneve do të jetë në formën shkresore ose nëpërmjet postës elektronike (*e-mail*). Gjithashtu, Në nenin 5 të saj, janë parashikuar detyrimet e përbashkëta ku, ndër të tjera, janë caktuar si pika kontakti nga dy përfaqësues (punonjës) të secilit institucion.
Konstatohet se 28 specialistë të strukturës OFL në Policinë e Shtetit, kanë nënshkruar deklaratat e konfidencialitetit për shkak të qasjes në të dhënat personale të administruara nga DPSHTRR. Në pikën 1 të deklaratës së konfidencialitetit citohet ndër të tjera se: *"me anë të kësaj deklarate marr përsipër të mos përdor dhe të mos i transmetoj personave të paautorizuar të dhëna personale apo informacione konfidenciale në lidhje me ose të marra nga* webservisi *dhe informacionet /dokumentacionet që shkëmbehen..."*.

Sa më sipër rezulton se, përtej sa është parashikuar në Marrëveshjen midis dy institucioneve, nuk janë respektuar parashikimet sa i përket mënyrës së komunikimit/aksesit, duke mundësuar gjithashtu komunikim elektronik nëpërmjet *web-servisit*, si dhe duke iu mundësuar akses rreth 28 specialistëve të Strukturës OFL në Policinë e Shtetit.

b. Në aneksin 1 të Memorandumit të Mirëkuptimit midis Institutit të Statistikave dhe DPSHTRR me nr. 16864 Prot., datë 28.08.2017, bashkëlidhet tabela me informacionet të cilat do t'i vihen në dispozicion Institutit të Statistikave. Konstatohet se veç të tjerave, në tabelë rezulton e përshirë e dhëna *"numri i shasisë së automjetit",* e cila është një e dhënë unike dhe mund të identifikojë pronarin e makinës, në kundërshtim parimin e mjaftueshmërisë sipas germës *"c"* të pikës 1, të nenit 5 të Ligjit.

c. Në marrëveshjen e përbashkët midis AMF dhe DPSHTRR me nr. 7747 prot., datë 16.06.2012, me objekt *"Bashkëpunimit dhe shkëmbimit të informacionit për sigurimin e detyrueshëm në sektorin e transportit*", datë 31.03.2021, përcaktohet, ndër të tjera, në pikën 4.6 detyrimet e AMF: *"AMF do të ruajë informacionin e marrë nga DPSHTRR për përdorim të brendshëm të shoqërive të sigurimit sipas dispozitave ligjore të identifikuara në pikën 1.1".* Qasja në të dhënat personale të DPSHTRR, nga palët e treta (shoqëri të sigurimeve) nëpërmjet kësaj marrëveshje (midis DPSHTRR dhe AMF), është në kundërshtim me parimet dhe kriteret ligjore të përpunimit, parashikuar në nenet 5 dhe 6 të Ligjit. Gjithashtu, referenca ligjore e përdorur në marrëveshjen e përbashkët, pika 14, e nenit 14, të ligjit nr. 9572/2006 *"Për Autoritetin e Mbikëqyrjes Financiare"* i ndryshuar, nuk mund të përdoret për të legjitimuar procesin e shkëmbimit të informacionit që përmban të dhëna personale, pasi nuk identifikon saktë kuadrin ligjor rregullator në të cilin mund të bazohet shkëmbimi i informacionit midis palëve, pasi në këtë referencë, janë parashikuar detyrat e bordit sa i takon parashikimit të buxhetit të autoritetit (AMF).

d. Në Marrëveshjen e Bashkëpunimit nr.26026/2 Prot., datë 15.01.2020, midis DPSHTRR dhe Regjistrit të Barreve Siguruese (RBS), nuk është evidentuar qartë baza ligjore që legjitimon procesin e shkëmbimit të informacionit, pasi konstatohet se referenca ligjore e cituar në Marrëveshje (nenet 659 e vijues të Kodit Civil), nuk identifikon saktë detyrimin ligjor në të cilin mund të bazohet shkëmbimi i informacionit midis palëve.

AKSHI është institucioni i cili ofron infrastrukturën TIK të ndërveprimit midis sistemeve elektronike të institucioneve shtetërorë nëpërmjet Government Gateway (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 ndër të tjera për qëllim 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 në ligj, në përputhje me parimet dhe kriteret ligjore të përpunimit të të dhënave, të parashikuara në nenet 5 dhe 6 të Ligjit.

7. Kontrolluesi është përfitues i shërbimit të mirëmbajtjes së sistemit *"e-DPSHTRR"*, *sipas* Kontratës nr. 4721 prot., datë 06.08.2019, me objekt *"Upgrade i sistemit qendror të "eDPSHTRR", pajisjet HP dhe aplikimit eDPSHTRR. Ridizenjim i infrastrukturës HP dhe ndërtimi i sistemit të menaxhimit".* AKSHI është nën cilësinë e Autoritetit kontraktues për këtë kontratë, ndërsa Infosoft System shpk, IkubINFO shpk janë operatoret ekonomik që në bashkëpunim, ofrojnë shërbimin sipas objektit të kontratës, nën cilësinë e përpunuesit.

Nisur nga parashikimet e kontratës së sipërcituar, termat teknike (TORs), si dhe konstatimeve në vend, rezulton se bashkimi i operatorëve Infosoft System shpk me IkubINFO shpk, ka akses të drejtpërdrejtë në nivel administratori në sistemin *"eDPSHTRR"* dhe bazën e të dhënave. Në këto kushte, referuar pikës 7, të nenit 3 të Ligjit, bashkimi i operatorëve 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.

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.

8. Nga verifikimi i formave të ndryshme të kontaktit (të tilla si, por pa u kufizuar: denonco akte korruptive apo abuzive nga punonjësit, denonco ndotje/anomali në transportin rrugor, pyetësor për cilësinë e shërbimit në sportel, kontakto institucionin, etj.) në faqen zyrtare https://www.dpshtrr.al, konstatohet se subjektet e të dhënave nuk informohen qartësisht, 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, dhe masat e sigurisë, në kundërshtim me parashikimet në nenin 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.

9. Në formularët e aplikimeve për shërbime të ndryshme, të paraqitur në sportelet e Drejtorive Rajonale, konstatohet se në fund të çdo formulari, ndodhen klauzolat deklarative me përmbajtje:

"KLAUZOLA DEKLARATIVE
Unë i/e nënshkruari/a _____, në dijeni të përgjegjësive penale që rrjedhin nga deklarimi dhe paraqitja e të dhënave e rrethanave të rreme, nën përgjegjësinë time personale deklaroj se të dhënat e paraqitura në këtë formular janë të vërteta dhe në respektim të ligjit nr.9887 "Për mbrojtjen e të dhënave personale" të ndryshuar, autorizoj me vullnetin tim të lirë institucionin, të përpunojë dhe të përdorë të dhënat e mia personale për qëllime statistikore dhe të shqyrtimit të aplikimit.

Njoftojmë se autorizimi i mëposhtëm është vullnetar.
Autorizoj institucionin të përpunojë të dhënat e mia personale (emër, mbiemër, numër telefoni ose email) të mbledhura më sipër, me qëllim zhvillimin e sondazheve të automatizuara për marrjen e opinionit tim, në lidhje me cilësinë e ofrimit të shërbimit."

Në formularë nuk qartësohen se cilat të dhëna janë të detyrueshme për t'u paraqitur, për të përfituar shërbimin e kërkuar nga ana e subjektit të të dhënave dhe cilat të dhëna nuk janë të detyrueshme, përpunimi i të cilave do të kërkonte *"pëlqimin"* e subjektit të të dhënave në përputhje me qëllimin e përpunimit specifik, sipas parimeve dhe kritereve ligjore të përpunimit të të dhënave të parashikuara në nenet 5 dhe 6 të Ligjit.

Sa i përket pjesës së parë deklarative mbi përgjegjësitë për deklarimin e saktë të të dhënave (për shkak të detyrimit ligjor për të përfituar shërbime nga DPSHTRR), konstatohet se në përbërje të saj përshihet edhe autorizimi/pëlqimi i subjektit mbi përpunimin e të dhënave personale nga DPSHTRR.

Zyra e Komisionerit vlerëson se *"Pëlqimi"*, është një nga 6 kriteret ligjore për përpunimin e të dhënave personale, parashikuar në pikën 1, të nenit 6 të Ligjit. Në rastin kur Kontrolluesi fillon një përpunim të dhënash, ai duhet të konsiderojë se cila është baza e përshtatshme ligjore për vazhdimin e përpunimit. Në përgjithësi, *"pëlqimi"* mund të jetë një kriter ligjor i përshtatshëm, nëse subjektit të të dhënave i është ofruar kontroll, si dhe i është ofruar mundësi e qartë për të pranuar apo refuzuar termat e ofruara, ose mundësia e pakushtëzuar e refuzimit të përpunimit.

Kur kërkon *"pëlqimin",* Kontrolluesi duhet të vlerësojë nëse ai i plotëson të gjithë kriteret për të garantuar një *"pëlqim"* të vlefshëm. Nëse është marrë në përputhje me ligjin, *"pëlqimi"* është një mjet që i mundëson subjektit të të dhënave kontroll nëse të dhënat personale të tij do të përpunohen apo jo. Në rast se jo, kontrolli i subjekteve mbi përpunimin e të dhënave, do të ishte imagjinar dhe *"pëlqimi"* do të ishte një kriter ligjor jo i saktë për përpunimin, duke e bërë procesin e përpunimit të paligjshëm.

10. Nga verifikimi i kryer në Regjistrin Elektronik të Subjekteve Kontrolluese, në protokollin e Zyrës së Komisionerit, rezulton se Kontrolluesi ka *"Njoftuar"* mbi përpunimin e të dhënave personale për të cilat është përgjegjës. Gjatë hetimit administrativ të ushtruar, është konstatuar se *"Njoftimi"* ka mangësi në deklarim, sa i përket rubrikave të formularit si vijon:

i. Deklarimin në rubrikën 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"*.

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

Zyra e Komisionerit vlerëson se përmbushja e detyrimit për ndryshimin e gjendjes së njoftimit të përpunimit të 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.

11. Kontrolluesi disponon rregullore *"Për mbrojtjen e të dhënave personale",* por konstatohet se Rregullorja nuk parashikon proceset, procedurat, 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, 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 Udhëzimit nr. 47, duke mundësuar shmangien e pasojave të rënda që mund të vijnë për subjektet e 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 mospërmbushje e 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 standardin 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.

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.

Përfaqësuesit e Kontrolluesit janë paraqitur në seancë dëgjimore dhe nëpërmjet shkresës nr. 14885/1 prot., datë 20.06.2022 kanë paraqitur pretendimet e tyre, nëpërmjet të cilave argumentohet si vijon:

1. *Mënyra e ndërtimit, mbajtjes dhe azhurnimit të këtyre sistemeve informatike është bërë sipas përshkrimeve teknike në përputhje me përmbajtjen e neneve 368 dhe 369 të VKM nr.153/2000 "Për miratimin e rregullores në zbatim të Kodit Rrugor të Republikës së Shqipërisë", i ndryshuar. Këto sistemе janë ndërtuar nga AKSHI i cili konform legjislacionit në fuqi, ngre, mirëmban dhe administron sistemet dhe aplikacione të teknologjisë së informacionit dhe komunikimit, infrastrukturën e qendërzuar dhe infrastrukturën TIK, përfshirë edhe ato të klasifikuara si "sekret shtetëror", për institucionet dhe organet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave.*

2. *Sa i përket konstatimit në lidhje me krahasimin e kategorive të të dhënave të listës së publikuar (targat) me ato të bazës së të dhënave në sistemin "eDPSHTRR", ... sqarojmë se: "Sistemi "eDPSHTRR" është i integruar në Government Gateway (GG) dhe kategoritë të dhënave të mësipërme janë të dhëna që ndwrveprohen në këtë platformë dhe nga institucione të tjera sipas legjislacionit dhe marrëveshjeve në fuqi."*

3. *Sa i përket konstatimit: "... se në ambientin "test" të "eDPSHTRR", punohet me të dhëna reale", sqarojmë që DPSHTRR për kryerjen e testeve në afrimitet me sistemin live nuk përdor të dhëna fiktive sepse ndërvepron me sisteme live të cilat shkëmbejnë të dhëna reale.*

4. *Sa i përket konstatimit që " ... nga verifikimi i kontrolleve të logeve në hedhjen e të dhënave dhe loget në sistem të cilat gjenerohen nga sistemi "eDPSHTRR" konstatohet që nuk analizohen nëpërmjet një ndërfaqe aplikative të posaçme e cila të mundësojë një shfletim në kohë reale të tyre" ... sqarojmë se, TORs-e për ndërtimin e sistemit eDPSHTRR janë hartuar sipas parashikimeve në VKM 673/2017 "Për organizimin e AKSHI" i ndryshuar.*

5. *Sa i përket konstatimit në lidhje me problematikat e konstatuara nga kontrolli i përdoruesve të sistemi dhe përgjegjësive që kanë në sistemin "eDPSHTRR", sqarojmë se, në sistemet e punës që DPSHTRR përdor, hapja/mbyllja e përdoruesve,*

ndryshimi i rolit të përdoruesit, kryhet në zbatim të Urdhrave të Drejtorit të Përgjithshëm. Për çdo përdorues në sisteme, ka rekorde që ruajnë informacion mbi hapjen/mbylljen/ndryshimin e rolit, ndryshimin e drejtorisë (foto I dhe foto2). Sistemi i vjetër "eDPSHTRR" (në përdorim në periudhën 24.10.2011 deri ne 29.11.2020) dhe sistemi i ri "eDPSHTRR" (në përdorim prej 02.12.2020), kanë ruajtur informacion mbi përdoruesin në skema të ndryshme, por në çdo rast evidentohet hapja e përdoruesve/mbyllja e përdoruesve/ndryshimi i rolit të përdoruesve.

Për sa citohet në lidhje me përdoruesit e përdorur për testim dhe implementimin e sistemit, theksojmë se DPSHTRR që në momentin që e konstatoi i kërkoi kompanisë që kryen mirëmbajtjen pastrimin e ambientit "live" nga rekordet e përdoruesve të përdoruara në ambientin test të cilat u kaluan pa konfirmim të DPSHTRR. Në modulin "Të gjithë përdoruesit" të sistemit "eDPSHTRR" shfaqen të dhënat e përdoruesve, përdorues aktual/ish përdorues/rekorde "Migruar pasi mungonin në sistemin e vjetër" për të siguruar migrimin gjithë rekordeve të sistemit të vjetër dhe integritetin e tyre në db (të cilat janë invalidur që në procesin e migrimit).
Në datën 13.06.2022 numri total i përdoruesve te sistemit edpshtrr është 1939. Një përdorues ka akses në ndërfaqen e sistemin "eDPSHTRR" nëse plotësohen kushtet: Invalidated= Jo, IsApproved = Po, IsLockedOut = Jo
Që një përdorues të aksesoje të dhëna të sistemit "eDPSHTRR", duhet të disponojë të paktën edhe një rol.
Këto informacione i janë bërë me dije edhe anëtareve të grupit të hetimit në komunikime në kuadër të këtij hetimi. Konstatimet nga grupi i hetimit, në këtë seksion, duke iu referuar informacioneve të bëra me dije gjatë vizitave në DPSHTRR si dhe fakteve të cituara më lart janë të pabazuara dhe nuk qëndrojnë.

6. *Përsa i përket konstatimit që, "... DPSHTRR ka të regjistruar bazën e të dhënave .... por nuk ka vijuar me përditësimin e bazave të të dhënave të regjistruara në kundërshtim me VKM nr.945 ...", sqarojmë se, praktika zyrtare mbi ndryshimet e realizuara sipas kontratave respektive mbi sistemet eDPSHTRR dhe eDM janë dorëzuar nga palët kontraktore pranë AKSHI-t nga ku DPSHTRR ka rolin e përfituesit të ndryshimeve të sistemeve.*

7. *Lidhur me konstatimin se, "Kontrolluesi nuk ka marrë masa organizative dhe teknike të përshtatshme për të mbrojtur të dhënat personale ... në kundërshtim me parashikimet e nenit 27 të ligjit dhe Udhëzimit nr.47 të Komisionerit", bëjmë me dije që, "DPSHTRR, do të marrë të gjitha masat e nevojshme duke kryer procedura administrative dhe marrë konsulenca për realizimin e tyre konform legjislacionit në fuqi."*

8. *Lidhur me konstatimin mbi "... përgjegjësitë për krijimin, administrimin dhe mirëmbajtjen e SMSI për mbrojtjen e të dhënave personale ... në përputhje me dispozitat e nenit 20 të ligjit dhe Udhëzimit nr.19 të Komisionerit...", bëjmë me dije që "DPSHTRR" do marrë të gjitha masat e nevojshme për të parashikuar në programin ekonomik krijimin e SMSI-ve konform parashikimeve ligjore ne fuqi.*

9. Lidhur me konstatimin në lidhje me përcaktimin e detyrimeve në akt-marrëveshjet e DPSHTRR-se *"... në lidhje me aksesin e 28 specialistëve të strukturës së OFL-së të Policisë së Shtetit, të cilët kanë nënshkruar deklaratat e konfidencialitelit për shkak të qasjes në të dhënat personale të administruara nga DPSHTRR ... ku rezulton se nuk janë respektuar parashikimet sa i përket mënyrës së komunikimit/aksesit duke mundësuar gjithashtu edhe komunikim elektronik nëpërmjet ëebservisit", sqarojmë se ...bazuar në përmbajtjen e kësaj marrëveshje, ... të dyja palët respektive janë përmbajtur marrëveshjes, pasi midis 2 institucioneve nuk është bërë komunikim me webserviceve, por vetëm komunikim shkresor dhe elektronik.*

10. *Lidhur me konstatimet mbi marrëveshjet e bashkëpunimit dhe të ngjashme bëjmë me dije se:*

- *Në lidhje me "Aneksin 1" të Memorandumit të Mirëkuptimit midis INSTAT dhe DPSHTRR, në tabelë rezulton e dhëna "numri i shasisë së automjetit" e cila është një e dhëne unike dhe mund të indentifikojë pronarin e makinës në kundërshtim me parimin e mjaftueshmërisë...", sqarojmë se bazuar në marrëveshjen përkatëse pika 5/7 parashikon se të dhënat e transmetuara nga DPSHTRR tek INSTAT trajtohen si te dhëna konfidenciale dhe administrohen duke respektuar në mënyre rigoroze dispozitat e parashikuara në nenin 15 "Konfidencialiteti" i ligjit të statistikave dhe nënshkrimet e deklaratës se konfidencialitetit ndërmjet palëve. Numri i shasise së automjetit është një e dhëne që identifikon në mënyre unike mjetin dhe prej tij në setin e të dhënave që shkëmbehen në kuadër të këtij memorandumi nuk mund te identifikohet pronësia e mjetit.*

- *Lidhur me konstatimin mbi referencën ligjore të përdorur në marrëveshjen e përbashkët, pika 14 e nenit 14, të ligjit nr.9572/2006 "Për Autoritetin e Mbikëqyrjes Financiare" i ndryshuar, nuk mund të përdoret për të legjitimuar procesin e shkëmbimit të informacionit që përmban të dhëna personale, pasi nuk identifikon saktë kuadri ligjor rregullator në të cilin mund të bazohet shkëmbimi i informacionit midis palëve .... , sqarojmë se DPSHTRR dhe AMF janë duke punuar ne lidhje me rishikimin e marrëveshjes aktuale si detyrim ligjor i lindur nga udhëzimi nr. 4, datë 28.6.2019 "Për dokumentet për qarkullim dhe regjistrim te mjeteve rrugore" i ndryshuar. DPSHTRR do te vlerësonte rekomandimet tuaja për kriteret/kushtet qe duhet te plotësojnë palët që ndërveprimi i të dhënave personale te kryhet konform legjislacionit për mbrojtjen e te dhënave personale.*

- *Lidhur me konstatimin mbi marrëveshjen e bashkëpunimi midis DPSHTRR dhe RBS, nuk është evidentuar qartë baza ligjore për të legjitimuar procesin e shkëmbimit të informacionit, pasi konstatohet se referenca ligjore e përdorur në marrëveshjen e përbashkët, nenet 659 e vijues të Kodit Civil, nuk identifikon saktë kuadrin ligjor rregullator në të cilin mund të bazohet shkëmbimi i informacionit midis palëve, sqarojmë se me anë të kësaj marrëveshje nuk është dakortësuar shkëmbimi i të dhënave personale, por komunikimi kryhet vetëm me email, për statusin juridik te numrit te identifikimit të mjeteve (shasisë).*

11. *Lidhur me konstatimin në lidhje me "Njoftimin" mbi përpunimin e të dhënave personale për të cilat DPSHTRR është përgjegjës, konstatohen mangësi në deklarim, sa i përket rubrikave 2, 3, 4, 5, 6, dhe 7 të tij, DPSHTRR kërkojn të njihet me praktikën e informacionit apo dokumentacionit të sipërcituar.*

12. *Lidhur me konstatimin sa i përket kontratës së lidhur me palë të treta midis AKSHI, Infosoft System dhe IKUB Info, në lidhje me mosverifikimin e kushteve të nevojshme për plotësimin e detyrimeve nga ana e përpunuesve, në kundërshtim me Udhëzimin nr.47, udhëzimin nr.19 dhe nenin 20 të ligjit ..., sqarojmë se DPSHTRR do të ketë në vëmendje rekomandimin e mësipërm dhe do të kërkojë nga palët kontraktore në kontratë, plotësimin e detyrimeve ligjore të sipërcituara.*

13. *Lidhur me konstatimin mbi mosdokumentimin e të gjitha log-ve sipas mareveshjeve që DPSHTRR ka me palët e treta, mendojmë se duke e konsideruar shqyrtimin e eventeve te logeve nje proces teknik specifik jashtë kapaciteteve të DPSHTRR, të kërkohet asistence pranë AKSHI-t.*

14. *Lidhur me konstatimin sa i përket formave të ndryshme të kontaktit te tilla si por pa u kufizuar, "denonco akte korruptime apo abuzive nga punonjësit ..." sqarojmë që mbështetur në ligjin nr. 107 /2021 "Për bashkëqeverisjen", kanali i vetëm online për dërgimin e denoncimeve të akteve korruptime është platforma "Me ty për Shqipërinë që duam", seksioni "Denonco korrupsionin", i cili do te zbatohet edhe nga DPSHTRR.*

15. *Lidhur me konstatimin në lidhje me formularët nuk qartësohen se cilat të dhëna janë të detyrueshme për t 'u paraqitur, për të përfituar shërbimin e kërkuar nga ana e subjektit të të dhënave dhe cilat te dhena nuk jane të detyrueshme perpunimi i te cilave do te kërkonte "pëlqimin" e subjektit të të dhënave në përputhje me qëllimin e përpunimit specifik), ju informojmë se formularët tip janë përgatitur dhe përcjellë pranë DPSHTRR nga ADlSA, miratuar me shkresën nr.961 prot., datë 15.10.2018 "Dërgohen formular të standardizuar për DPSHTRR-në".*

16. *Lidhur me konstatimin mbi marrjen e masave konkrete në kuadër të trajnimit të punonjësve që kanë akses dhe përpunojnë të dhëna personale dhe mosplotësim i detyrimeve në lidhje me ngritjen, administrimin dhe mirëmbajtjen e SMSI për sa i takon mbrojtjes së të dhënave personale, të parashikuar në Udhëzimin nr.47, sqarojmë se zëri i trajnimeve është parashikuar në Programin Ekonomiko-Financiar të vitit 2022, miratuar nga Ministri i Infrastrukturës dhe Energjisë me shkresën nr.1097/1 prot, date 04.02.2022, protokolluar me tonën nr.2473/1 prot., datë 08.02.2022.*

    Përsa me sipër kërkojmë marrjen në konsideratë të sqarimeve të bëra nga DPSHTRR. Gjithashtu Nisur nga tendenca ne rritje te institucioneve që detyrohen te nderveprojnë me DPSHTRR (Ligji 107 /2021 dhe VKM 252/2022) kërkojmë asistencen tuaj (neni 29 i ligjit 9887 /2008 i ndryshuar) mbi monitorimin e politikave te menaxhimit për

mbrojtjen e te dhënave personale që do të ndërmarra DPSHTRR konform rekomandime të lëna nga ana juaj.

Në lidhje me argumentet e Kontrolluesit, Zyra e Komisionerit vlerëson se DPSHTRR 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. Në cilësinë e Kontrolluesit, DPSHTRR përgjigjet 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 *"eDPSHTRR"* nga vetë punonjës të Kontrolluesit, Zyra e Komisionerit vlerëson se DPSHTRR 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 DPSHTRR. Dispozitat e legjislacionit për mbrojtjen e të dhënave personale në lidhje me aspektet e sigurisë së të dhënave, nuk përjashtojnë nga përgjegjësia ligjore institucionet në fjalë, të cilat kanë detyrimin të demonstrojnë përgjegjshmëri, si dhe mbajnë përgjegjësi, për realizimin e proceseve përpunuese në përputhje me dispozitat e nenit 5 të Ligjit.

Kontrolluesi nuk mund të justifikojnë 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.

Në lidhje me pretendimet mbi menaxhimin përdoruesve, Zyra e Komisionerit vlerëson se në këtë aspekt Kontrolluesi duhet të jetë koherent dhe proaktiv për çdo ndryshim juridik të funksionaliteteve të punës për çdo punonjës si dhe pasqyrimin e këtyre atributeve në sistemin elektronik *"eDPSHTRR"*, kjo me qëllim garantimin e aksesit sipas detyrave respektive.

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* dhe *dh,* të pikës 1, të nenit 39 të Ligjit, përbëjnë kundërvajtje administrative dhe sanksionohen me gjobë si më poshtë:

a) kontrolluesit, që përdorin të dhëna personale në kundërshtim me kreun II "Përpunimi i të dhënave personale", dënohen me 10 000 deri në 500 000 lekë;

b) kontrolluesit, që nuk përmbushin detyrimin për të informuar, të përcaktuar në nenin 18 të këtij ligji, dënohen me 10 000 deri në 300 000 lekë;

ç) kontrolluesit ose përpunuesit, që nuk zbatojnë detyrimet e përcaktuara në nenin 20 të këtij ligji, dënohen me 10 000 deri në 300 000 lekë;

d) kontrolluesit, që nuk përmbushin detyrimin për të njoftuar, sipas përcaktimit në nenin 21 të këtij ligji, dënohen me 10 000 deri në 500 000 lekë;

dh) kontrolluesit ose përpunuesit, që nuk marrin masat e sigurisë së të dhënave dhe nuk zbatojnë detyrimin për ruajtjen e konfidencialitetit, të përcaktuara përkatësisht në nenet 27 dhe 28 të këtij ligji, dënohen me nga 10 000 deri në 150 000 lekë;

Në bazë të pikës 2 të nenit 39 të Ligjit, personat juridikë, për kundërvajtjet e mësipërme administrative, dënohen me dyfishin e gjobës së përcaktuar në pikën 1 të këtij neni.

Për zgjedhjen e masës së gjobës, Zyra e Komisionerit ka parasysh faktin 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.

PËR KËTO ARSYE:

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

V E N D O S A:

1. Dënimin e Kontrolluesit me gjobë në vlerën 250 000 (dyqind e pesëdhjetë 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 150 000 (njëqind e pesëdhjetë 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. Kontrolluesi, të marrë masa për përpunimin e të dhënave personale në përputhje me dispozitat e parashikuara në nenet 5 dhe 6 të Ligjit;

7. Kontrolluesi, të përcaktojë në mënyrë të qartë databazat në të cilat legjitimohet të ketë akses dhe kategoritë e të dhënave që duhet të aksesojë 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;

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

9. Kontrolluesi, të marrë masa për zbatimin e detyrimeve sipas parashikimeve të nenit 20 të Ligjit, në lidhje me delegimin e përpunimit të të dhënave dhe/ose shërbimit ;

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 Udhëzimin 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 6 më sipër;
    (ii) menjëherë, detyrimet e treguara në pikën 7 më sipër;
    (iii) brenda 15 (pesëmbëdhjetë) ditëve, detyrimet e treguara në pikat 8 dhe 10, më sipër;
    (iv) brenda 30 (tridhjetë) ditëve, detyrimet e treguara në pikat 9 dhe 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