RAPORT

I

ZYRËS SË KOMISIONERIT PËR TË DREJTËN E INFORMIMIT DHE MBROJTJEN E TË DHËNAVE PERSONALE

në kuadër të

Rezolutës, datë 21.05.2020, të Kuvendit të Republikës së Shqipërisë "*Për vlerësimin e veprimtarisë së Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale për vitin 2019*"

Tiranë, më 28.12.2020

PASQYRA E LËNDËS

A. FJALOR SHPJEGUES

Baza e të dhënave shtetërore	Grumbullimi i organizuar i informacionit, i ruajtur në formë elektronike, ku përpunimi dhe përditësimi i tij kryhen nëpërmjet një sistemi kompjuterik, si pjesë e plotësimit të detyrimeve ligjore të institucionit administrues.
BE	Bashkimi Evropian.
Kontrollues	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.
Ligji për Mbrojtjen e të Dhënave Personale	Ligji nr. 9887, datë 10.03.2008 "*Për mbrojtjen e të dhënave personale*" i ndryshuar.
Log	Shënim i shkurtuar që duhet të përmbajë informacionin e nevojshëm për të siguruar që ky informacion të mund të përdoret për të garantuar monitorimin, investigimin dhe zgjidhjen e çdo problemi sigurie.
Përpunues	Çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër që përpunon të dhëna personale në emër të Kontrolluesit.
Rezoluta e Kuvendit	Rezoluta, datë 21.05.2020, e Kuvendit të Republikës së Shqipërisë "*Për vlerësimin e veprimtarisë së Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale për vitin 2019*".
SMSI	Sistemi i Menaxhimit të Sigurisë së Informacionit për mbrojtjen e të dhënave personale, i parashikuar në Udhëzimin nr. 47 dhe Udhëzimin nr. 48 të Komisionerit.
Subjekti i të dhënave	Çdo person fizik, të cilit i përpunohen të dhënat personale.
TIK	Teknologji Informacioni dhe Komunikimi.
Udhëzimi nr. 19	Udhëzimi nr. 19, datë 03.08.2012, i Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale "*Mbi rregullimin e marrëdhënieve mes*

	Kontrolluesit dhe përpunuesit në rastet e delegimit të përpunimit të të dhënave dhe përdorimin e një kontrate tip në rastet e këtij delegimi" i ndryshuar.
Udhëzimi nr. 47	Udhëzimi nr. 47, datë 14.09.2018, i Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale "*Për Përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga subjektet përpunuese të mëdha*".
Udhëzimi nr. 48	Udhëzimi nr. 48, datë 14.09.2018, i Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale "*Për Certifikimin e sistemeve të menaxhimit të sigurisë së informacionit, të dhënave personale dhe mbrojtjes së tyre*".
Udhëzimi nr. 49	Udhëzimi nr. 49, datë 02.03.2020, i Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale "*Për mbrojtjen e të dhënave personale shëndetësore*".
Zyra e Komisionerit	Zyra e Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale

B. RAPORTI

Ky Raport është përgatitur në përputhje me pikën 2 të nenit 30 të Ligjit për Mbrojtjen e të Dhënave Personale, si dhe detyrat e lëna për Zyrën e Komisionerit në bazë të Rezolutës së Kuvendit.

Synimi i Raportit është përcjellja, për vëmendje të Kuvendit, e konstatimeve dhe rekomandimeve të Zyrës së Komisionerit në lidhje me fushat e mbikëqyrjes së përcaktuara si detyra të posaçme nga rezoluta.

Konstatimet dhe rekomandimet sipas këtij Raporti janë pjesë e angazhimeve vijuese të Zyrës së Komisionerit në lidhje me monitorimin dhe mbikëqyrjen e respektimit të legjislacionit për mbrojtjen e të dhënave personale nga Kontrolluesit, ndër të tjera, në sektorët e Teknologjisë së Informacionit dhe Komunikimit, si dhe në sektorë ku përpunohen të dhëna sensitive, siç është ai i kujdesit shëndetësor.

Kohëzgjatja e inspektimeve dhe kontrollove të kryera, për qëllime të këtij Raporti, është diktuar, ndër të tjera, nga rrethanat dhe vështirësitë e krijuara për shkak të gjendjes së pandemisë COVID-19.

Për këtë arsye, Zyra e Komisionerit rezervon të drejtën për të raportuar më tej në Kuvend për zhvillime, rrethana dhe/ose situata të tjera që mund të verifikohen në të ardhmen në lidhje me objektin e këtij Raporti, në përputhje me pikën 2 të nenit 30 të Ligjit për Mbrojtjen e të Dhënave Personale.

Raporti është përgatitur në dy pjesë si vijon:

- *Pjesa 1 - Përpunimi i të dhënave në sektorin e Teknologjisë së Informacionit dhe Komunikimit*.

- *Pjesa 2 - Përpunimi i të dhënave në sektorin e kujdesit shëndetësor*.

Në Pjesën 1 pasqyrohen konstatimet dhe rekomandimet e Zyrës së Komisionerit në lidhje me përpunimin e të dhënave në sektorin publik të Teknologjisë së Informacionit dhe Komunikimit.

Në Pjesën 2 pasqyrohen konstatimet dhe rekomandimet në lidhje me sektorin publik dhe privat të kujdesit shëndetësor.

Arsyet e përfshirjes së sektorit privat në këtë pjesë të Raportit lidhen me situatën e shkaktuar nga COVID-19 dhe, rrjedhimisht, me rëndësinë që merr ky sektor në kuadër të detyrimeve të tij për të bashkërenduar, me institucionet publike të kujdesit shëndetësor, përpjekjet dhe angazhimet me qëllim parandalimin dhe përballimin e pasojave të pandemisë.

PJESA 1 - Përpunimi i të dhënave në sektorin e TIK

I. Hyrje

Ofrimi i shërbimeve publike *online,* nëpërmjet platformave TIK është shoqëruar me shtim të proceseve përpunuese të të dhënave personale nga autoritet publike, për shkak të lehtësimit të aksesit të qytetarëve në shërbimet publike falë këtyre platformave.

Rrjedhimisht, Zyra e Komisionerit ka konstatuar në vazhdimësi një përpunim në rritje të të dhënave personale nga Kontrolluesit publikë (institucione dhe/ose shoqëri me kapital shtetëror) përmes sistemeve TIK.

Përhapja e pandemisë COVID-19 dhe pasojat e rënda të saj në shëndetin dhe jetën e qytetarëve kanë bërë që ofrimi i shërbimeve publike nëpërmjet platformave TIK të mos jetë një nga alternativat për akses në shërbimet publik, krahas sporteleve fizike, por thuajse e vetmja alternativë për këtë qëllim.

Një rol kryesor dhe veçanërisht të rëndësishëm, në këtë aspekt, ka luajtur portali unik qeveritar *e-Albania,* i cili administrohet dhe mirëmbahet nga Agjencia Kombëtare e Shoqërisë së informacionit (AKSHI).

Kësisoj, platformat TIK janë aktualisht dhe, sipas të gjitha gjasave, do të vijojnë të jenë edhe në të ardhmen, një domosdoshmëri dhe një zgjidhje e arsyeshme për qytetarët për akses në shërbime.

Nga ana tjetër, qytetarëve, krahas garantimit të së drejtës për akses në shërbimet publike, duhet t'ju garantohet edhe pacënueshmëria e të drejtave të tyre për mbrojtje të të dhënave personale dhe jetës private në kudër të përdorimit të platformave TIK për marrjen e shërbimeve publike.

Kjo nënkupton detyrimin e Kontrolluesve publikë për t'i kushtuar një vëmendje të posaçme marrjes së masave teknike-organizative dhe krijimit të kushteve të nevojshme për të garantuar sigurinë dhe mbrojtjen e të dhënave personale të qytetarëve, si dhe, bashkë me të, ruajtjen e konfidencialitetit, në përputhje me parashikimet e neneve 27 dhe 28 të Ligjit për Mbrojtjen e të Dhënave Personale, si dhe dispozitave të akteve nënligjore të Komisionerit.

Për këtë arsye, monitorimi dhe mbikëqyrja e përpunimit të të dhënave personale në sektorin TIK ka qenë në qendër të prioriteteve të Zyrës së Komisionerit për vitin 2020.

Përgjatë veprimtarisë së Zyrës së Komisionerit, në veçanti gjatë periudhës së gjendjes së fatkeqësisë natyrore të shpallur për shkak të pandemisë së COVID-19, e në vijim, janë vërejtur një seri ankesash të qytetarëve për problematika në lidhje me përpunimin e të dhënave personale nëpërmjet platformave në rrjet.

Nga ana tjetër, Zyra e Komisionerit ka ofruar asistencë të vazhdueshme për një seri aktesh ligjore dhe nënligjore, të paraqitura për mendim pranë saj, nga Këshilli i Ministrave, Ministritë, si dhe/ose agjenci të ndryshme qeveritare.

Vlen të përmenden, në këtë aspekt, projektligji "*Për krijimin e bazës së të dhënave shtetërore "Portali Unik Qeveritar e-albania" dhe për miratimin e rregullave "Mbi mënyrën e funksionimit të Pikës së Vetme të Kontaktit*", projektligji "*Për regjistrin qëndror të llogarive bankare*", projektvendimi për miratimin në parim të traktatit "*Për shkëmbimin e të dhënave për verifikimin e deklaratave të pasurisë*", etj.

Sa më sipër, në zbatim të detyrave të lëna nga Kuvendi në bazë të rezolutave të tij, krahas angazhimit të saj rregullues, sensibilizues dhe orientues, Zyra e Komisionerit ka zhvilluar një fushatë kontrollesh dhe vizitash mbikëqyrëse në Kontrollues publikë në sektorin e Teknologjisë së Informacionit dhe Komunikimit, rezultatet e përmbledhura të të cilit pasqyrohen në këtë pjesë të Raportit.

II. Faktet dhe rrethanat e zhvillimit të mbikëqyrjes

Në zbatim të Rezolutës së Kuvendit, si dhe kompetencave dhe detyrimeve ligjore të parashikuara në Ligjin për Mbrojtjen e të Dhënave Personale, Zyrës së Komisionerit i është lënë detyra e mbikëqyrjes, ndër të tjera, të platformave *online* dhe TIK, si dhe paraqitja e një raporti të detajuar për gjendjen e mbrojtjes së të dhënave personale.

Në këtë kuadër, me shkresën Nr. 669 Prot., datë 10.06.2020, me lëndë "*Kërkesë për informacion në kuadër të evidentimit dhe analizimit të bazave të të dhënave dhe platformave online, në administrim dhe përdorim të institucioneve publike*", Zyra e Komisionerit i është drejtuar 82 Kontrolluesve publikë (institucione të administratës publike dhe shoqëri tregtare me kapital shtetëror), duke kërkuar informacion në lidhje me si vijon:

(i) Numrin e bazave të të dhënave dhe platforma/sisteme *online* në administrim dhe përdorim;

(ii) Bazën ligjore për krijimin dhe funksionimin e bazave të të dhënave, si dhe platformave/sistemeve *online*;

(iii) Specifikimin e niveleve të aksesit në bazat e të dhënave, si dhe platformat/sistemet *online*. Numrin e punonjësve që kanë akses në to, si dhe pozicionin e tyre pranë institucionit sipas emërtesës së detyrës/funksionit;

(iv) Gjurmueshmërinë e veprimeve përpunuese me qëllim dokumentimin e ndërhyrjeve dhe veprimeve të tjera (krijim, modifikim, shkatërrim, ruajtje/*backup*, etj.) në bazat e të dhënave, si dhe platformat/sistemet *online*.

Kërkesës së mësipërme i janë përgjigjur 68 autoritete publike.

Gjithashtu, nëpërmjet Urdhrit nr. 91, datë 09.06.2020, të Komisionerit, është ngritur një grup pune i posaçëm, i përbërë nga juristë dhe ekspertë TIK, për realizimin e disa kontrolleve dhe vizitave mbikëqyrëse në Kontrollues publikë të caktuar.

Përzgjedhja e Kontrolluesve për këtë qëllim është bazuar, kryesisht, në grupin e atyre që nuk i janë përgjigjur shkresës nr. 669 prot., datë 10.06.2020, si dhe, para së gjithash, bazuar në rëndësinë që veprimtaria e Kontrolluesve në fjalë bart në lidhje me ofrimin e shërbimeve publike dhe, rrjedhimisht, në volumin dhe frekuencën e lartë të përpunimit të të dhënave personale.

Metodologjikisht, grupi i punës, në kontrollet dhe vizitat mbikëqyrëse të realizuara, është përqëndruar në verifikimin e respektimit nga Kontrolluesit publikë të parimeve dhe kritereve ligjore të përpunimit të të dhënave personale, respektimit të të drejtave të subjekteve të dhënave, si dhe në lidhje me masat e posaçme të marra nga këta Kontrollues për garantimin e sigurisë dhe konfidencialitetit të të dhënave personale, me fokus të posaçëm Sistemet e Menaxhimit të Sigurisë së Informacionit (SMSI) për mbrojtjen e të dhënave personale, të rregulluar me Udhëzimet nr. 47 dhe 48 të Komisionerit.

Me qëllim evidentimin e situatës faktike, përtej deklarimeve të kryera nga institucionet, Zyra e Komisionerit, duke marrë në konsideratë, ndër të tjera, faktorë si natyra e shërbimit publik që ofron autoriteti përkatës dhe nivelin e riskut në mbrojtjen e të dhënave personale, ndërmori hapat proceduralë për të mbikëqyrur proceset përpunuese të të dhënave personale pranë Kontrolluesve të mëposhtëm:

i. Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI);

ii. Agjencia Shtetërore e Kadastrës (ASHK);

iii. Posta Shqiptare SHA;

iv. Qendra Kombëtare e Biznesit (QKB);

v. Agjencia Shqiptare e Ofrimit të Shërbimeve të Integruara (ADISA);

vi. Drejtoria e Përgjithshme e Policisë së Shtetit (DPPSH);

vii. Drejtoria e Përgjithshme e Parandalimit të Pastrimit të Parave (DPPPP);

viii. Drejtoria e Përgjithshme e Tatimeve (DPT);

ix. Drejtoria e Përgjithshme e Burgjeve (DPB).

Inspektimet dhe verifikimet në lidhje me respektimin e legjislacionit për mbrojtjen e të dhënave personale janë realizuar, gjatë muajve tetor - nëntor 2020, nëpërmjet rishikimit të dokumentacionit të vënë në dispozicion, sipas kërkesës së inspektorëve të Zyrës së Komisionerit, si dhe nëpërmjet kontrollit në terren pranë subjekteve të sipërpërmendura.

III. Baza ligjore

Kontrollet dhe vizitat mbikëqyrëse të realizuara nga Zyra e Komisionerit, në zbatim të kompetencave të përcaktuara në nenet 31 dhe 32 të Ligjit për Mbrojtjen e të Dhënave Personale, kanë patur në fokus të tyre verifikimin e respektimit të parimeve dhe kritereve ligjore për përpunimin e të dhënave personale, si dhe verifikimin e masave teknike dhe organizative për parandalimin e përhapjes së paligjshme të të dhënave të subjekteve të të dhënave, në përputhje me nenet, 5, 6, 12 - 15, 18 - 20, 27 dhe 28 të ligjit në fjalë.

Gjithashtu, përveç dispozitave të sipërpërmendura të ligjit, grupi i punës është bazuar edhe në dispozitat detyruese të akteve nënligjore të nxjerra nga Komisioneri, përfshirë, veçanërisht, Udhëzimet nr. 19, 47 dhe 48 të Komisionerit, të cilat përmbajnë detyrimet e Kontrolluesve lidhur me marrëdhëniet me Përpunuesit përkatës, si dhe për krijimin, mirëmbajtjen dhe administrimin e SMSI për mbrojtjen e të dhënave personale.

Konkretisht, nenet 5 dhe 6 të Ligjit për Mbrojtjen e të Dhënave Personale përcaktojnë parimet dhe kriteret ligjore në të cilat bazohet përpunimi i të dhënave personale, të tilla si parimi i ligjshmërisë së përpunimit të të dhënave, parimi i mjaftueshmërisë, përpunimin bazuar në pëlqimin e subjektit të të dhënave, për përmbushjen e një detyre ligjore të Kontrolluesit, etj.

Më tej, Kontrolluesit janë të detyruar të respektojnë të drejtat e subjekteve të të dhënave të përcaktuara në Kreun IV të Ligjit për Mbrojtjen e të Dhënave Personale, të cilat përfshijnë, por pa u kufizuar, të drejtën e aksesit në të dhëna, të drejtën për të kërkuar bllokim, korrigjim dhe fshirje të dhënave personale, si dhe detyrimet për informimin përpara fillimit dhe/ose pas ndryshimit të gjendjes së përpunimit të të dhënave të sanksionuar në nenin 18 të ligjit.

Gjithashtu, në varësi të natyrës së veprimtarisë së tyre, një pjesë ose i gjithë procesi i përpunimit të të dhënave mund të delegohet tek palë të treta. Shembull për këtë është ndërveprimi i institucioneve publike me *e-albania* nëpërmjet së cilës ato ofrojnë shërbimet e tyre për qytetarët.

Në themel të këtij ndërveprimi është përpunimi i të dhënave që Kontrolluesit në fjalë e realizojnë nëpërmjet portalit unik qeveritar *e-albania*, i cili passjell detyrimin e palëve për të normuar marrëdhënien e tyre Kontrollues - Përpunues nëpërmjet marrëveshjeve të posaçme të parashikuara në nenin 20 të Ligjit për Mbrojtjen e të Dhënave Personale dhe Udhëzimin nr. 19 të Komisionerit.

Përveç sa më sipër, Kontrolluesit janë të detyruar të marrin masa teknike dhe organizative për garantimin e sigurisë së të dhënave personale dhe ruajtjen e konfidencialitetit të tyre, në përputhje me nenet 27 dhe 28 të Ligjit për Mbrojtjen e të Dhënave Personale.

Këto nene parashikojnë detyrimin e çdo Kontrolluesi për të mbrojtur të dhënat personale nga shkatërrime të paligjshme, aksidentale, humbje aksidentale, për të mbrojtur aksesin ose përhapjen nga persona të paautorizuar, veçanërisht kur përpunimi i të dhënave bëhet në rrjet (kupto: nëpërmjet platformave TIK), si dhe nga çdo formë tjetër e paligjshme përpunimi.

Në zbatim të këtij detyrimi, me qëllim shpjegimin dhe shtjellimin e dispozitave të nenit 27 të Ligjit për Mbrojtjen e të Dhënave Personale, Komisioneri ka hartuar dhe miratuar Udhëzimin nr. 47

Ky udhëzim parashikon detyrimin e të gjithë Kontrolluesve – të cilët angazhojnë më shumë se 6 persona për përpunimin e të dhënave personale – për të krijuar, administruar dhe mirëmbajtur Sistemin e Menaxhimit të Sigurisë së Informacionit (SMSI) për mbrojtjen e të dhënave personale.

SMSI bazohet në identifikimin, analizimin dhe në zbutjen e rreziqeve ndaj sigurisë së të dhënave personale duke marrë parasysh sistemet TIK për përpunimin e të dhënave, format manuale të përpunimit, sigurinë fizike të mjediseve, personelit dhe pajisjeve, si dhe përcaktohet në standardet TIK si vijon:

(i) "*Konfidencialitetin*", duke siguruar që të dhënat personale të jenë të aksesueshme vetëm për personat e autorizuar;

(ii) "*Integritetin*", duke siguruar që të dhënat të jenë të sakta, të plota dhe duke ruajtur metodat e përpunimit të tyre;

(iii) "*Disponueshmërinë*", duke siguruar aksesin e përdoruesit të autorizuar në të dhënat dhe në sistemet e përpunimit;

(iv) "*Konfidencialitetin*", duke garantuar që çdo aktivitet/veprim mbi të dhënat, i sistemeve TIK dhe personelit të përdorur për përpunimin e tyre, është i gjurmueshëm dhe i kontrollueshëm.

Gjithashtu, është e nevojshme që SMSI të përfshijë një set rregullash dhe dokumentesh detyruese për Kontrolluesit, të tilla si Analizën e Ndikimit në të Dhënat Personale, Politikën e Sigurisë së Informacionit, Kontrollin e sistemit të arkivimit të të dhënave, etj., si dhe sigurinë fizike të ambienteve, të personelit dhe pajisjeve (platformave) TIK.

Në vijim, Kontrolluesit duhet të marrin masa 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.

Kontrolluesit kanë detyrimin që, për krijimin, administrimin dhe mirëmbajtjen e SMSI për mbrojtjen e të dhënave personale, të bazohen në kërkesat e standardit ISO/IEC 27001, të parashikuar në nenin 5 të Udhëzimit nr. 48.

Gjithashtu, Udhëzimi nr. 48 parashikon mundësinë e Kontrolluesve për certifikimin e SMSI, për qëllime përputhshmërie me standardin e sipërpërmendur, nga organizma të akredituar dhe autorizuar sipas dispozitave të këtij udhëzimi.

Vlen të theksohet se mekanizmi i çertifikimit përbën një risi të prezantuar në kuadër të Rregullores së Përgjithshme të Mbrojtjes së të Dhënave (GDPR) të BE, të cilën Zyra e Komisionerit e ka "transpozuar" (në mënyre jodetyruese), me asistencën e autoriteteve homologe të BE, në dispozitat e Udhëzimit nr. 48.

Krahas garancive teknike dhe organizative që parakushtëzon për Kontrolluesit, si dhe efekteve pozitive reputacionale që bart për këta të fundit, mekanizmi i certifikimit synon gjithashtu nxitjen e Kontrolluesve për marrjen e masave vetërregulluese në lidhje me garantimin e sigurisë dhe ruajtjes së konfidencialitetit të të dhënave personale.

IV. Problematikat e konstatuara

Problematikat e konstatuara në kuadër të kontrolleve dhe vizitave mbikëqyrëse të realizuara nga grupi i punës së Zyrës së Komisionerit, pranë autoriteteve publike të listuara në Kreun II më sipër, janë paraqitur, për qëllime të këtij Raporti, në dy plane kryesore:

(i) Në planin e respektimit të detyrimeve që burojnë nga kuadrin ligjor për mbrojtjen e të dhënave personale, i cili përfshin verifikimin e respektimit të parimeve dhe kritereve ligjore të përpunimit, respektimin e të drejtave të subjekteve të të dhënave, marrëdhëniet Kontrollues - Përpunues, etj.; dhe

(ii) Në planin e masave teknike dhe organizative, veçanërisht, bazuar në ekzistencën e SMSI pranë çdo Kontrolluesi objekt kontrolli.

IV.1 Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI)

AKSHI është institucioni qendror përgjegjës, ndër të tjera, për zbatimin e politikave dhe të strategjive, për zhvillimin e sektorit të shoqërisë së informacionit, është autoritet rregullator koordinues, përgjegjës i bazave të të dhënave shtetërore, si dhe ofron shërbime të përqendruara nëpërmjet TIK për qeverisjen elektronike, për administratën shtetërore, qytetarët, bizneset.

AKSHI administron çdo sistem dhe infrastrukturë TIK, për institucionet dhe organet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave, sipas Vendimit nr. 673, datë 22.11.2017 "*Për Riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit*", i ndryshuar.

Nga verifikimet e realizuara, u konstatua se AKSHI ka miratuar një rregullore specifike për politikat e privatësisë, e cila është publikuar edhe në faqen zyrtare të institucionit.

Nga shqyrtimi i rregullores rezulton se janë parashikuar parimet e përpunimit të të dhënave, si dhe të drejtat e subjektit të të dhënave, masat organizative të sigurisë, e drejta për tu ankuar, etj.

Megjithatë, vërehet se në këtë rregullore nuk janë përfshirë të gjitha proceset përpunuese të të dhënave personale që kryen AKSHI, duke kufizuar, në këtë mënyrë, të drejtën për t'u informuar të subjekteve të të dhënave në lidhje me kategoritë e të dhënave personale, që përpunohen dhe qëllimin e përpunimit.

AKSHI rezulton të ketë deleguar shërbimin e ruajtjes fizike të ambienteve tek një subjekt privat (Përpunues). Nga analizimi i kësaj kontrate, konstatohet një mungesë e rregullave për mbrojtjen e të dhënave për këtë proces përpunues, si dhe vërehen mangësi në lidhje me elementet, detyrimet dhe garancitë ligjore të kërkuara nga dispozitat e nenit 20 të Ligjit për Mbrojtjen e të Dhënave Personale.

AKSHI ka miratuar sistemin SMSI sipas standardit të sigurisë së informacionit ISO/IEC 27001.

Nga shqyrtimi i dokumenteve, pjesë e këtij sistemi, rezulton se janë përcaktuar procedurat dhe politikat për sigurinë e informacionit në lidhje me menaxhimin e aksesit, përdorimin e aseteve, menaxhimin e burimeve njerëzore, menaxhimin e kapaciteteve të sistemeve, menaxhimin e incidenteve, vazhdimësinë e sigurisë së informacionit, etj.

Megjithatë, vërehet se në këtë institucion mungon, në strukturën organizative, një funksion i pavarur për të monitoruar dhe përmirësuar në mënyrë të vazhdueshme sistemin e implementuar.

Misioni i kësaj strukture organizative, për sigurinë e informacionit, duhet të jetë hartimi, zbatimi dhe mirëmbajtja një programi për sigurinë e informacionit që mbron sistemet, shërbimet dhe të dhënat e AKSHI-it kundër përdorimit të paautorizuar, zbulimit, modifikimit, dëmtimit dhe humbjes.

Rëndësia e një ekipi proaktiv dhe të paanshëm është faktor kyç, për kryerjen e proceseve për garantimin e sigurisë së informacionit në lidhje me menaxhimin, udhëzimet, koordinimin dhe funksionet operacionale, si dhe për përcaktimin e politikave/rregulloreve për monitorimin dhe menaxhimit të sigurisë së informacionit.

Ky rol është i rëndësishëm për të monitoruar në mënyrë periodike efikasitetin e SMSI-së duke analizuar progresin e arritur dhe duke propozuar përmirësime të mëtejshme.

Përmirësimi i vazhdueshëm është një aspekt kyç i SMSI-së në përpjekjen për të realizuar dhe ruajtur konfidencialitetin, integritetin, disponueshmërinë dhe besueshmërinë e sigurisë së informacionit dhe duhet të jetë pjesë e integruar e objektivave të Kontrolluesve publikë.

Duke analizuar rëndësinë e AKSHI-it si institucioni qendror përgjegjës për infrastrukturën e shërbimeve elektronike qeveritare, ngritja e një strukture të pavarur dhe të kualifikuar sipas standardeve të sigurisë së informacionit luan një rol të rëndësishëm në sigurinë e të dhënave personale dhe efikasitetin e SMSI.

Me ritmin e inovacionit dhe përparimit të teknologjisë është thelbësor zhvillimi i kompetencave, veçanërisht për specialistët TIK, sipas standardeve të sigurisë ISO/IEC 27001, për të pasur njohuritë profesionale për administrimin e sistemeve në përdorim.

Duke marrë në konsideratë infrastrukturat kritike në menaxhim, Zyra e Komisionerit vlerëson se nga ky institucion duhet t'i kushtohet me shumë rëndësi monitorimit të vazhdueshëm të sistemeve, infrastrukturave dhe shërbimeve që ofrohen nëpërmjet platformes qeveritare GG (Government Gateway), shërbimet Cloud dhe infrastrukturës së çelësit publik (PKI).

Gjithashtu, strategjia e rimëkëmbjes nga katastrofat, si dhe planet që përcaktojnë vazhdimësinë e proceseve në rastet e dështimit, duhet të jenë në përputhje me normat e lejuara të distancave të sigurisë dhe të testohen periodikisht për të gjithë komponentët e tyre.

IV.2 Agjencia Shtetërore e Kadastrës (ASHK)

ASHK është person juridik publik në varësi të Kryeministrit, përgjegjës për ofrimin e shërbimeve kadastrale, bazuar në dispozitat e ligjit 111/2018 "*Për kadastrën*".

ASHK ka miratuar një seri aktesh rregullatorë, në të cilat parashikohen detyrime përgjithësuese dhe deklarative të ruajtjes së konfidencialitetit, si kodi etik i institucionit, rregullorja e brendshme, si dhe rregullorja për garantimin e sigurisë të regjistrit elektronik të pasurive të paluajtshme.

Megjithatë, në aktet e mësipërme nuk konstatohen norma specifike që rregullojnë ruajtjen, mbrojtjen dhe sigurinë e të dhënave personale të subjekteve të të dhënave, gjatë proceseve përpunuese që zhvillon ky Kontrollues në përmbushjen e detyrave të tij ligjore.

Konkretisht, ASHK ka hartuar një rregullore "*Për garantimin e sigurisë të regjistrit elektronik të pasurive të paluajtshme (ALBSReP)*", në të cilën specifikohen rregulla dhe

procedura të përgjithshme, për të siguruar mbrojtjen e konfidencialitetit, integritetit dhe disponueshmërisë së informacionit në ALBSReP.

Nga ana tjetër, nga kontrolli i ushtruar rezulton se ka një mungesë të theksuar monitorimi të proceseve të sigurisë së informacionit nga departamenti i TIK.

U konstatua, gjithashtu, mungesa e një strategjie për SMSI në përputhje me dipozitat e Udhëzimit nr. 47, e cila konsiston në zbatimin, monitorimin dhe përmirësimin e vazhdueshëm të SMSI, duke garantuar mbrojtjen e informacionit përmes një sistemi menaxhimi të qendërzuar dhe të standardizuar.

Krijimi dhe mbyllja e përdoruesve bëhet sipas formave të regjistrimit me aprovim, por cikli i jetës së një përdoruesi, përditësimet dhe pajisjet (asetet) nuk janë në monitorim të vazhdueshëm nga departamenti i TIK.

U konstatua që përdoruesit nuk janë të kategorizuar për akses në varësi të funksioneve që kryejnë. Në disa raste përdoruesit (*user*) dhe pajisjet (asetet) nuk menaxhohen në mënyrë të centralizuar në *Active Directory* (AD). Kjo cenon integritetin e të dhënave që përpunohen dhe memorizohen në përmbushjen e detyrave funksionale të këtij institucioni.

IV.3 Posta Shqiptare SHA

Posta Shqiptare SHA është përgjegjëse për ofrimin e shërbimit shtetëror postar në Republikën e Shqipërisë.

Ky Kontrollues ka hartuar dhe miratuar një rregullore specifike për ruajtjen, përpunimin, mbrojtjen dhe sigurinë e të dhënave personale, e cila është publikuar edhe në faqen e internetit të shoqërisë, e aksesueshme për vizitorët e faqes së internetit.

Rregullorja përfshin, në një kuadër të përgjithshëm, proceset përpunuese që realizon Posta Shqiptare SHA, parimet dhe kriteret e përpunimit, të drejtat e subjekteve të të dhënave, si të drejtën për akses, të drejtën për korrigjim ose fshirje, masat e sigurisë, si dhe funksionet organizative ndërmjet strukturave të brendshme.

Gjithashtu, Posta Shqiptare SHA ka hartuar dhe miratuar një rregullore për përdorimin e postës elektronike dhe disa procedura në lidhje me funksionimin e proceseve të sigurisë së informacionit.

Ky subjekt menaxhon dhe monitoron përdoruesit me sisteme të centralizuar, duke siguruar integritetin e të dhënave që përpunohen.

Ka hartuar dhe zbaton procedura për vazhdimësinë e aktivitetit dhe i teston rregullisht nëpërmjet kontratave me furnitorët.

Megjithatë, nuk janë evidentuar procese të standardizuara në lidhje me menaxhimin e aseteve, incidente të sigurisë së informacionit, si dhe një plan monitorimi dhe përmirësimi i vazhdueshëm i SMSI në këtë institucion, në përputhje me standardin ISO/IEC 27001.

Zbatimi i një SMSI në përputhje me standardin e sipërpërmendur do të sigurojë mbrojtjen nga rreziqet që mund ndikojnë në konfidencialitetin, integritetin ose disponueshmërinë e të dhënave personale.

Me ritmin e inovacionit dhe përparimit të teknologjisë, është thelbësore zhvillimi i kompetencave, veçanërisht për specialistët TIK, sipas standardit të sigurisë ISO/IEC 27001 për të pasur njohuritë profesionale për administrimin e sistemeve.

Përveç programeve specifike për stafin e TIK, duhet të hartohen edhe programe ndërgjegjësimi të vazhdueshme për këtë të fundit, duke marrë në konsideratë avancimin e teknologjisë, sulmeve kibernetike dhe përditësimet legjislative në fuqi.

IV.4 Qendra Kombëtare e Biznesit (QKB)

QKB është institucioni përgjegjës për mbajtjen dhe administrimin e regjistrit tregtar dhe atij të licencave në Republikën e Shqipërisë.

QKB ka hartuar dhe miratuar një rregullore specifike për ruajtjen përpunimin, mbrojtjen dhe sigurinë e të dhënave personale në vitin 2018.

Rregullorja përfshin, në një kuadër të përgjithshëm, proceset përpunuese që realizon ky Kontrollues, parimet dhe kriteret e përpunimit, të drejtat e subjekteve, ndarjen e proceseve përpunuese në njësitë organizative përkatëse, sigurinë fizike të mjediseve ku zhvillohen procese përpunuese dhe një dispozitë për sigurinë informatike.

Gjithashtu, QKB ka hartuar dhe miratuar rregulloren e TIK, datë 11.11.2020, në të cilën janë specifikuar parimet dhe rregullat e sigurisë së informacionit.

Në këtë rregullore janë përcaktuar përgjegjësitë për veprimet që lidhen me sigurinë me qëllim ruajtjen e integritetit, disponueshmërisë dhe konfidencialitetit të aseteve të informacionit të QKB.

Megjithatë, mungon strategjia e monitorimit në mënyre periodike të efikasitetit të SMSI sipas standardit ISO/IEC 27001, për analizimin e progresit të arritur dhe për propozimin e përmirësimeve të mëtejshme.

Ky faktor është i rëndësishëm për përmbushjen e kërkesave të sigurisë së informacionit dhe mbrojtjen e të dhënave personale.

Përveç programeve specifike për stafin e TIK, duhet të hartohen edhe programe ndërgjegjësimi të vazhdueshme për këtë të fundit, duke marrë në konsideratë avancimin e teknologjisë, sulmeve kibernetike dhe përditësimet legjislative në fuqi.

IV.5 Agjencia Shqiptare e Ofrimit të Shërbimeve të Integruara (ADISA)

ADISA është institucioni përgjegjës për ofrimin e shërbimeve publike për personat fizikë dhe juridikë, nëpërmjet sporteleve fizike të shërbimit, sporteleve fizike të pikave të shërbimit me një ndalesë dhe sporteleve fizike të ofrimit të shërbimeve publike të integruara.

Me Vendimin nr. 7, datë 09.05.2019, të Këshillit Drejtues, ADISA ka miratuar rregulloren për mbrojtjen e të dhënave personale, e cila parashikon respektimin, në proceset përpunuese që realizon ADISA, e parimeve dhe kritereve të përpunimit, të drejtave të subjekteve, ndarjen e proceseve përpunuese në njësitë organizative përkatëse, etj.

Megjithatë, gjatë kontrollit pranë ADISA, u konstatua se numri i shërbimeve të ofruara për qytetarët në sportele është reduktuar ndjeshëm, për shkak se shërbimet ofrohen nëpërmjet portalit unik qeveritar të shërbimeve *e-albania*.

Sportelet pranë njësive të qeverisjes vendore shërbejnë kryesisht për ofrimin e asistencës së qytetarëve në aksesimin e portalit unik qeveritar të shërbimeve *e-albania*.

Nga ana tjetër, rezultoi se ADISA nuk dispononte rregullore dhe procedura për qeverisjen e platformave TIK, menaxhimin e operacioneve të TIK, si dhe sigurinë e sistemeve dhe informacionit.

U konstatua, mungesa e një strategjie ose plani për sigurinë e informacionit në përputhje me dispozitat e Udhëzimit nr. 47.

Ky proces bëhet nga struktura TIK në varësi të AKSHI-it, e cila operon sipas proceseve të përcaktuara në rregulloret e punës së këtij institucioni.

Menaxhimi i përdoruesve dhe i pajisjeve në përdorim bëhet në mënyrë jo të centralizuar, duke paraqitur, kështu, një rrezik të madh për mbrojtjen e të dhënave personale.

Duhet të hartohen programe ndërgjegjësimi të vazhdueshme për stafin, duke marrë në konsideratë avancimin e teknologjisë, sulmet kibernetike dhe përditësimet legjislative në fuqi.

IV.6 Drejtoria e Përgjithshme e Policisë së Shtetit (DPPSH)

Vërehet një vëmendje e shtuar e DPPSH në kuadër të implementimit të detyrimeve ligjore në fushën e mbrojtjes së të dhënave personale, kjo si pasojë e angazhimeve që ky institucion ka me institucionet homologe të vendeve të BE-së dhe më gjerë, të cilat imponojnë një respektim sa më rigoroz të rregullave lidhur me mbrojtjen e të dhënave personale, të cilat qëndrojnë në themel të çdo bashkëpunimi në fushën policore.

Procedurat organizative dhe teknike, si dhe masat për mbrojtjen e të dhënave personale janë përcaktuar në Rregulloren "*Për mbrojtjen e të dhënave personale dhe sigurinë e tyre në Policinë e Shtetit*", miratuar me Urdhër nr. 330, datë 04.07.2011, të Ministrit të Brendshëm.

Aksesi në sistemet e DPPSH është i organizuar në dy nivele. Konkretisht, në nivel administratori të bazave të të dhënave dhe në nivel përdoruesish, sipas roleve dhe përgjegjësive respektive.

Një nga sistemet më të rëndësishme në administrim të këtij Kontrolluesi është Sistemi i Menaxhimit Total të Informacionit (TIMS), i cili menaxhon të dhënat e hyrje-daljeve të subjekteve të të dhënave, nga Republika e Shqipërisë. Ky sistem informatik është ndërtuar dhe mirëmbahet teknikisht nga Drejtoria e Teknologjisë së Informacionit në varësi të Kontrolluesit.

Zyra e Komisionerit gjatë kontrollit të ushtruar konstatoi se DPPSH, gjatë përpunimit të të dhënave në sistemin TIMS, zbaton, ndër të tjera, dispozitat e rregullores "*Për mbrojtjen e të dhënave personale dhe sigurinë e tyre në policinë e shtetit*".

Rregullorja e sipërpërmendur parashikon masat teknike dhe organizative për përpunimin dhe sigurinë e të dhënave personale të administruara nga Policia e Shtetit, në përputhje me nenin 27 të Ligjit për Mbrojtjen e të Dhënave Personale. Masat e teknike dhe organizative të parashikuara janë të një niveli të kënaqshëm.

Megjithatë, me qëllim që këto masa të jenë sa më efektive, është e nevojshme përafrimi i tyre me elementet e SMSI në zbatim të Udhëzimit nr. 47 të Komisionerit.

Gjatë kontrollit është konstatuar ekzistenca e disa marrëveshjeve bashkëpunimi "*Për dhënien e të drejtës së përdorimit të sistemit të menaxhimit total të informacionit (TIMS) të policisë së shtetit*", të nënshkruara midis Drejtorisë së Policisë së Shtetit dhe disa institucione si Prokuroria e Përgjithshme, Drejtoria e Përgjithshme e Doganave, Drejtoria e Përgjithshme e Tatimeve, Shërbimi Informativ Shtetëror dhe Drejtoria e Përgjithshme e Parandalimit e Pastrimit të Parave.

Nëpërmjet këtyre marrëveshjeve, institucionet në fjalë lejohen që të aksesojnë të dhëna personale të shtetasve shqiptarë nëpërmjet sistemit TIMS. Në këto marrëveshje janë përfshirë kushtet, detyrimet dhe përgjegjësia administrative dhe penale e personave që autorizohen të kenë akses në sistem, për ruajtjen e konfidencialitetit dhe mospërhapjen e informacionit.

Në këtë kuadër, Zyra e Komisionerit vlerëson se është e nevojshme që DPPSH në çdo rast të kryejë Analizën e Ndikimit në të Dhënat Personale (si element i rëndësishëm i SMSI), duke vlerësuar paraprakisht riskun e aksesit të ofruar dhe proceseve përpunuese.

Gjithashtu është e nevojshme që marrëveshjet të reflektojnë elementet e nevojshëm që parashikon neni 20 i Ligjit për Mbrojtjen e të Dhënave Personale dhe Udhëzimi nr. 19, për sa kohë që institucionet që kanë akses në TIMS konsiderohen përpunues.

Zyra e Komisionerit me Rekomandimin nr. 32, datë 23.12.2016, ka lënë një sërë detyrash ndaj DPPSH lidhur me sigurinë e mbrojtjes së të dhënave në sistemin TIMS.

Në këtë kuadër u konstatua se janë marrë masa teknike lidhur me gjurmueshmërinë e veprimeve në TIMS duke e rritur afatin nga 6 muaj në 2 vite. Por është e nevojshme që kjo të reflektohet edhe në aktet rregullatore të brendshme të detyrueshme për çdo përdorues.

Afatet për ruajten e të dhënave të subjekteve në sistemin TIMS janë parashikuar me Urdhrin e Drejtorit të Përgjithshëm të Policisë së Shtetit nr. 245, datë 16.03.2016 "*Për afatet e ruajtjes së të dhënave personale në sistemet elektronike të policisë së shtetit, për qëllime parandalimi, hetimi, zbulimi dhe ndjekje të veprave penale*".

Në këtë kuadër konstatohet moszbatim i afateve të parashikuara në Udhëzimin nr. 17, datë 11.05.2012 "*Për përcaktimin e kohës së mbajtjes së të dhënave personale që përpunohen në sistemet elektronike, nga organet e Policisë së Shtetit për qëllime parandalimi, hetimi, zbulimi dhe ndjekje të veprave penale*", miratuar nga Zyra e Komisionerit, i cili gjithashtu i shtrin efektet në të gjitha sistemet elektronike të administruara nga organet e Policisë së Shtetit.

DPPSH ka hartuar dhe miratuar procedura dhe rregullore me qëllim garantimin e sigurisë së të dhënave dhe informacionit. Në procedurat e punës janë përcaktuar përgjegjësitë dhe është strukturuar procesi për krijimin, përditësimin dhe mbylljen e përdoruesve në sistemet kritike.

DPPSH ka ngritur procese monitorimi për përdoruesit dhe akseset e tyre dhe ka filluar auditimin e tyre. Në DPPSH janë ngritur infrastruktura të sigurta që ndërveprojnë me kanale të sigurta komunikimi midis bashkëpunëtoreve të saj dhe infrastrukturës së brendshme.

Megjithatë, implementimi i pjesshëm i SMSI nuk ofron siguri të mjaftueshme për mbrojtjen e të dhënave personale.
Përpjekja për të arritur dhe ruajtur konfidencialitetin, integritetin, disponueshmërinë dhe besueshmërinë e sigurisë së informacionit, duhet të jetë pjesë e integruar e objektivave të DPPSH.

Ndaj, duhet të përmirësohet monitorimi i procesit të gjenerimit të Log-eve (Log-e auditi dhe Log-e të sistemit të operimit).

Sistemet dhe infrastrukturat mbështetëse për gjenerimin e Log-ve duhet të ndërtohen sipas kontrolleve të sigurisë detektuese dhe evidentuese. Gjurmueshmëria në sistemet kritike është një faktor kryesor për të detektuar dhe evidentuar aksesin e paautorizuar apo modifikimin e të dhënave në një bazë të dhënash. Log-et e sistemit të operimit duhet të përmbajnë informacionin e nevojshëm në mënyrë që të sigurojnë që ky informacion të mund të përdoret për të garantuar monitorimin dhe detektimin, si dhe, si rrjedhojë, zgjidhjen e çdo problemi sigurie.

Duhet të kryen analiza periodike mbi Log-et e sigurisë, bazuar mbi ndikimin që kanë sistemet dhe infrastrukturat kritike në të dhënat personale.

IV.7 Drejtoria e Përgjithshme e Parandalimit të Pastrimit të Parave (DPPPP)

DPPPP është një institucion në varësi të Ministrit të Financave dhe shërben si njësi e specializuar financiare për parandalimin dhe luftën kundër pastrimit të parave dhe financimit të terrorizmit.

Zyra e Komisionerit në kuadër të evidentimit të proceseve përpunuese, kategorive të subjekteve të të dhënave personale, kategorive të të dhënave personale dhe masave teknike organizative dhe ligjore për garantimin e sigurisë dhe konfidencialitetit të këtyre të dhënave ka analizuar bazën ligjore specifike, e cila rregullon veprimtarinë e këtij Kontrolluesi dhe parashikohen rregullat për të administruar dhe krijuar bazën e të dhënave që administrohet nga ana e këtij institucioni.

Në nenin 16 të ligjit nr. 9917, datë 19.05.2008 "*Për parandalimin e pastrimit të parave dhe financimit të terrorizmit*" i ndryshuar, parashikohen masa konkrete për ruajtjen e të dhënave lidhur me afatet e ruajtjes, të cilat ju referohen vetëm subjekteve raportuese.

Zyra e Komisionerit vlerëson se, pavarësisht se elementet e përgjithshëm lidhur me sigurinë e të dhënave personale, nivelet e aksesit dhe gjurmueshmërisë së veprimeve, janë të rëndësishëm dhe reflektohen edhe në detyrimet që institucioni ka si Kontrollues publik, është e nevojshme që të merren masa edhe në kuadër të implementimit të elementeve të tjera specifike që burojnë nga Ligji për Mbrojtjen e të Dhënave Personale, si dhe aktet nënligjore të miratuara në zbatim të tij.

Këto masa duhet të reflektojnë të drejtat e subjekteve të të dhënave personale, detyrimet e Kontrolluesit, parimet e mbrojtjes së të dhënave (në veçanti afati i ruajtjes së të dhënave), ofrimin e garancive mbi sigurinë e sistemit të të dhënave, në zbatim të Udhëzimit nr. 47, si dhe duhet të jenë të zbatueshme për çdo proces përpunimi që kryhen DPPPP.

DPPPP ka hartuar dhe miratuar procedura dhe rregullore me qëllim garantimin e sigurisë së të dhënave dhe informacionit, në të cilat janë përcaktuar përgjegjësitë dhe janë strukturuar proceset për menaxhimin dhe monitorim e akseseve, menaxhimin e aseteve,

menaxhimin e incidenteve, menaxhimin e burimeve njerëzore, menaxhimin e kapaciteteve të sistemeve, menaxhimin e incidenteve, sigurinë në transmetimin e informacionit, vazhdimësinë e aktivitetit.

Sistemet operative dhe infrastrukturat e këtij institucioni menaxhohen të centralizuara, si për përdoruesit edhe për asetet, gjë që siguron integritetin e të dhënave që përpunohen.

Më tej, megjithëse janë hartuar politika dhe procedura të përgjithshme që mbulojnë pjesërisht sigurinë e informacionit, u konstatua mungesa e një strategjie për zbatimin e SMSI-së, në të gjithë e elementet e sigurisë, në zbatim të Udhëzimit nr. 47 të Komisionerit.

IV.8 Drejtoria e Përgjithshme e Tatimeve (DPT)

DPT është institucioni në varësi të Ministrit përgjegjës për Financat dhe ka si mision kryesor mbledhjen e të ardhurave tatimore duke zbatuar njëtrajtësisht legjislacionin tatimor, për financimin e buxhetit të shtetit.

DPT ka hartuar një seri aktesh rregullatore, ku përfshihen parashikime mbi ruajtjen e konfidencialitetit.

Megjithatë, nuk janë konstatuar norma specifike që rregullojnë ruajtjen, mbrojtjen dhe sigurinë e të dhënave personale gjatë proceseve përpunuese që zhvillon institucioni në përmbushjen e detyrave funksionale.

DPT ka miratuar një rregullore për sigurinë e informacionit në DPT, në të cilën janë specifikuar rregullat e përgjithshme për sigurinë e informacionit dhe përgjegjësitë për veprimet që lidhen me sigurinë e informacionit në DPT.

Në bazë të kësaj rregulloreje janë hartuar dhe disa politika dhe procedura në funksion të sigurisë së informacionit.

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

Ndaj, auditimi i vazhdueshëm i rrjetit dhe i sistemeve në përdorim duhet të jetë një proces i dokumentuar dhe vijues, për përmbushjen e objektivit të sigurisë së informacionit dhe mbrojtjen e të dhënave personale.

Rishikimi dhe përditësimi në vazhdimësi i rregullave dhe politikave të zbatueshme për sigurinë dhe privatësisë duhet t'i përgjigjet ritmit të inovacionit të teknologjive dhe legjislacionet në fuqi.

IV.9 Drejtoria e Përgjithshme e Burgjeve (DPB)

DPB ka në administrim dhe përdorim, ndër të tjera, "*Bazën e të Dhënave të Menaxhimit të Informacionit të Sistemit Penitenciar*" (MISP) dhe "*Bazën e të Dhënave të Programit të Dëshmisë së Penalitetit*" (ZGJGJ).

Organizimi, administrimi dhe funksionimi i tyre rregullohet me rregullore specifike të miratuara nga Drejtori i Përgjithshëm i Burgjeve.

Nga analizimi i këtyre rregulloreve, Zyra e Komisionerit vlerëson se, pavarësisht përpjekjeve serioze në kuadër të plotësimit të standardeve të sigurisë, masat e parashikuara nuk implementojnë në tërësi elementet e sigurisë së të dhënave personale në zbatim të Udhëzimit nr. 47.

Nga analizimi i kontratës së delegimit të krijimit dhe mirëmbajtjes së aplikacionit për kartelat e të dënuarve dhe personelit, që Kontrolluesi ka nënshkruar më një bashkim operatorësh ekonomikë (në cilësinë e Përpunuesit), vërehen mangësi në adresimin e elementeve, detyrimeve dhe garancive ligjore në zbatim të nenit 20 të Ligjit Për Mbrojtjen e të Dhënave Personale dhe Udhëzimit nr. 19 të Komisionerit.

DPB ka hartuar dhe zbaton rregulla në lidhje me sigurinë e informacionit, për infrastrukturën dhe sistemet që ka në përdorim. Këto rregulla reflektohen dhe në kontratat e mirëmbajtjes që institucioni ka me furnitorët kryesore për sistemet dhe mirëmbajtjen fizike të ambienteve.

U konstatua se në proceset e punës është mirëpërcaktuar dhe strukturuar procesi i akseseve dhe përgjegjësive sipas funksioneve të strukturës administrative.

Gjithashtu, ndërveprimi me sisteme të jashtëm zhvillohet nën kanale të sigurta komunikimi dhe i monitoruar.

Megjithatë, duke marr në konsiderate faktin se DPB përpunon dhe transferon të dhëna sensitive, duhet të përmirësohet monitorimi në vazhdimësi i të gjitha infrastrukturave kritike, me procedura periodike auditimi për analizën e Log-ve të sistemit të operimit.

Drejtuesit kanë një rol kritik në sigurimin e ndërgjegjësimin në lidhje me sigurinë dhe konfidencialitetin e informacionit në të gjithë institucionin dhe në zhvillimin e një "kulture sigurie", duke hartuar programe ndërgjegjësimi të vazhdueshme për stafin, bazuar tek rëndësia e të dhënave personale që përpunohen dhe tek klasifikimi i tyre.

V. Konkluzione dhe rekomandime

Nga i gjithë procesi i mbikëqyrjes rezulton se, në pjesën më të madhe të Kontrolluesve publikë, aspekti rregullator i mbrojtjes së të dhënave personale në proceset përpunuese

përmes teknologjisë së informacionit është i veçuar nga rregullat për proceset e tjera përpunuese të të dhënave.

Në këtë kuadër, institucionet e administratës shtetërore që përpunojnë të dhëna personale duhet të parashikojnë në mënyrë konkrete, të gjitha proceset përpunuese, në akte të mirëfillta rregullatorë që garantojnë ruajtjen, sigurinë, dhe mbrojtjen e të dhënave personale të subjekteve të të dhënave, sipas detyrimit të përcaktuar në nenin 27 të Ligjit për Mbrojtjen e të Dhënave Personale.

Zyra e Komisionerit vlerëson se problematikat e evidentuara në këto institucione publike, lidhen me mungesën e njohurive ligjore dhe teknike dhe sensibilizimin mbi detyrimet që parashikon në tërësi legjislacioni për mbrojtjen e të dhënave personale.

Sa i përket marrëdhënieve kontraktore që institucionet publike (në cilësinë e Kontrolluesit) lidhin me palë të treta (në cilësinë e përpunuesit) për delegimin e shërbimeve të ndryshme, ku në thelb të tyre ka edhe përpunim të të dhënave personale, vërehen mangësi në adresimin e elementeve, detyrimeve dhe garancive ligjore të sanksionuara në nenin 20 të Ligjit për Mbrojtjen e të Dhënave Personale dhe Udhëzimit nr. 19 të Komisionerit.

Zyra e Komisionerit rekomandon që, në vijimësi, institucionet publike, në fazën e hartimit të kontratave me palët e treta, të parashikojnë në përmbajtje të tyre edhe elementet e nenit 20 të Ligjit për Mbrojtjen e të Dhënave Personale dhe Udhëzimit nr. 19.

Zyra e Komisionerit ka konstatuar se Kontrolluesit kanë hartuar dhe miratuar akte të brendshme rregullatore lidhur me mbrojtjen e të dhënave personale, por këto akte disponojnë rregullime të përgjithshme, lidhur me menaxhimin e të dhënave personale dhe ruajtjen e konfidencialitetit të subjekteve të të dhënave, të padetajuara rregullisht në lidhje me masat tekniko-organizative të përshtatshme dhe të zbatueshme për garantimin e mbrojtjes së të dhënave personale dhe sensitive, kriteret e ligjshmërisë së përpunimit të të dhënave, masat për garantimin e gjurmueshmërisë dhe kontrollit të veprimeve të personave/personelit që ka pasur dhe/ose ka akses në këto të dhëna, si dhe për mënyrën e shkatërrimit të tyre, kur të jetë përmbushur qëllimi i përpunimit të tyre.

Veçanërisht në lidhje me dhënien e aksesit në të dhënat personale, gjejmë rastin të ritheksojmë qëndrimin tonë të vazhdueshëm si autoritet mbikëqyrës, se ky veprim/përpunim, edhe kur është i autorizuar sipas ligjit, nuk nënkupton domosdoshmërisht dhe gjithnjë një akses të drejtpërdrejtë dhe të pakufizuar në të dhënat e kërkuara.

Dhënia e një aksesi të drejtpërdrejtë dhe të pakufizuar në të dhënat personale, pavarësisht se mund të jetë parimisht e autorizuar me ligj, mund të shpie në përpunim të dhënash në tejkalim të qëllimit të veprimtarisë dhe/ose detyrës për të cilën ligji e autorizon një Kontrollues (autoritet/institucion) të caktuar për të patur akses në të dhënat personale të administruara nga një Kontrollues (autoritet/institucion) tjetër dhe anasjelltas.

Për këtë arsye, në mënyrë që të sigurohet përputhshmëria me parimin e ligjshmërisë së përpunimit, të përcaktuar në germën "a" të pikës 1 të nenit 5 të Ligjit për Mbrojtjen e të Dhënave Personale dhe, rrjedhimisht, të parandalohen cenime eventuale të sigurisë dhe konfidencialitetit të të dhënave si rezultat i përpunimeve të mundshme eksesive (në tejkalim të qëllimit), sikundër kërkohet nga dispozitat e neneve 27 dhe 28 të këtij ligji, si dhe Udhëzimi nr. 47 i Komisionerit, është e domosdoshme që Kontrolluesit të marrin masa konkrete (i) për sigurimin e gjurmueshmërisë së aksesit në të dhëna, si dhe (ii) përcaktimin e niveleve të aksesit në përputhje me dispozitat ligjore që e autorizojnë atë – në harmoni të plotë me objektin dhe qëllimin e veprimtarisë së Kontrolluesit (autoritetit/institucionit) që i është akorduar ky akses.

Sa më sipër, Zyra e Komisionerit këshillon që nga ana e Kontrolluesve të ndërmerren në mënyrë imediate iniciativa për të evidentuar fillimisht të gjitha proceset përpunuese dhe më pas të përshtatin rregulloret ekzistuese ose hartojnë rregullore të brendshme që të parashikojnë masa konkrete teknike organizative në referim dhe zbatim të nenit 27 dhe 28 të Ligjit dhe për Mbrojtjen e të dhënave Personale, akteve nënligjore të miratuara nga Zyra e Komisionerit në sektorë të ndryshëm.

Në këtë kuadër, është i nevojshëm një angazhim më serioz i këtyre institucioneve, në drejtim të trajnimit të punonjësve që kanë akses në të dhënat personale dhe mbikëqyrin proceset përpunuese dhe në drejtim të konsolidimit të praktikave dhe legjislacionit specifik që rregullon veprimtarinë e tyre.

Më tej, mbetet detyrë e Kontrolluesve, në përputhje me parashikimet e germës "a" të nenit të pikës 1 të nenit 31 të Ligjit për Mbrojtjen e të Dhënave Personale, për të konsideruar dhe respektuar përgjegjësinë taksative të Zyrës së Komisionerit për dhënien e mendimeve lidhur me projekt-aktet, ligjore dhe nënligjore, që kanë të bëjnë me të dhënat personale, si dhe, sidomos dhe veçanërisht, në lidhje me projekte që planifikohen, ndërmerren dhe/ose kërkohen të zbatohen nga Kontrolluesit (qoftë vetëm, qoftë në bashkëpunim me të tjerët). Theksojmë se, në të shkuarën e afërt, janë konstatuar raste projektesh të vëna në zbatim nga institucione qendrore, të cilat ushtrojnë edhe detyra jetike për shtetin (si menaxhimi buxhetor dhe menaxhimi i financave publike), të cilët rezultojnë në kundërshtim me dispozitat e legjislacionit në fuqi për mbrojtjen e të dhënave personale.

Gjithashtu mbetet e një rëndësie themelore nevoja për të modernizuar infrastrukturën dhe aktet rregullatore që lidhen me sistemet dhe Bazat e të Dhënave.

Në këtë kuadër Zyra e Komisionerit vlerëson se nevojiten përpjekje të vazhdueshme në aspektin e garantimit të sigurisë teknike dhe organizative të të dhënave, si dhe krijimit, mirëmbajtjes dhe administrimit të SMSI, në përputhje me parashikimet detyruese të Udhëzimit nr. 47 të Komisionerit.

Pjesa më e madhe e Kontrolluesve nuk kanë venë në zbatim mekanizmat e nevojshëm për kontrollet dhe monitorimin e aktiviteteve të TIK, me qëllim zhvillimin, operimin, menaxhimin dhe mirëmbajtjen e tyre.

Rezultatet e kontrollit kanë treguar se ka vështirësi në menaxhimin e burimeve të teknologjisë së informacionit. Menaxhimi i aktiviteteve të TIK nuk është bazuar mjaftueshëm në politika, procedura dhe procese operimi të përshtatshme për sigurinë e informacionit.

U konstatua mungesa e një strategjie ose plani për zbatimin e SMSI-së që përfshin të gjithë komponentët e një sistemi të kompletuar për menaxhimin e sigurinë së informacionit, në përputhje me dispozitat e udhëzimeve të sipërpërmendura.

Përveç mungesës së një strategjie për SMSI-në, e cila konsiston në zbatimin, monitorimin dhe përmirësimin e vazhdueshëm të saj, vihet re mungesa e një strukture të pavarur për të kryer këtë funksion. Ky rol është i rëndësishëm për të monitoruar në mënyrë periodike efikasitetin e SMSI-së, duke analizuar progresin e arritur dhe duke propozuar përmirësime të mëtejshme.

Përmirësimi i vazhdueshëm është një aspekt kyç i SMSI-së në përpjekjen për të realizuar dhe ruajtur konfidencialitetin, integritetin, disponueshmërinë dhe besueshmërinë e sigurisë së informacionit dhe duhet të jetë pjesë e integruar e objektivave të Kontrolluesve publikë.

Veçanërisht, në lidhje me SMSI, Zyra e Komisionerit rekomandon si vijon:

(i) Hartimin e strategjisë për SMSI, bazuar në parimet e sigurisë TIK (konfidencialiteti, integriteti, disponueshmëria, besueshmëria), sipas standardit ISO/IEC 27001;

(ii) Ngritjen e strukturave monitoruese për SMSI-të dhe përmirësimi i vazhdueshëm i objektivave të sigurisë;

(iii) Trajnimin e vazhdueshëm i stafit në lidhje me standardet ndërkombëtare (veçanërisht, atë ISO/IEC 27001) të sigurisë së informacionit dhe privatësisë;

(iv) Projektimin dhe monitorimin e vazhdueshëm të sigurisë së rrjetit dhe enkriptimi i të dhënave gjatë transferimit të tyre në të gjitha kanalet (*HTTPS, IPSec, TLS, PPTP, SSH*);

(v) Krijimin e një regjistri të plotë të pajisjeve (aseteve) TIK në përdorim, duke analizuar rëndësinë e të dhënave personale që këto asete ruajnë dhe përpunojnë.

Centralizimin e të gjitha aseteve me anë të të cilave kryhet përpunim i të dhënave personale dhe monitorimi periodik i tyre, si dhe zbatimin dhe monitorimin

politikave për instalimin, aksesin dhe përditësimin e pajisjeve (aseteve) me anë të të cilave kryhet përpunim i të dhënave personale;

(vi) Zbatimin e politikave për kontrollet (fizike dhe teknike) dhe kufizimi i përdoruesve sipas nevojave për punë, si dhe auditimin periodik i sistemeve dhe rrjetit bazuar mbi matricën e akseseve. Përdorimin e *Multifactor Authentication* (MFA) në strukturat kritike dhe ato që përmbajnë të dhëna sensitive;

(vii) Kontrollin nëpërmjet skanimeve, në mënyrë sistematike, të infrastrukturës kritike;

(viii) Zbatimi i një plani për vazhdimësinë e sigurisë së informacionit (*disaster recovery plan*) dhe testimi në mënyrë periodike i të gjithë komponentëve të tij;

(ix) Vlerësimin përputhshmërisë së SMSI me standardin ISO/IEC 27001 në përputhje me Udhëzimin nr. 48 të Komisionerit, nëpërmjet auditimit periodik dhe mekanizmit të certifikimit për këtë qëllim.

PJESA 2 - Përpunimi i të dhënave në sektorin e kujdesit shëndetësor

I. Hyrje

Përpunimi i të dhënave personale në sektorin e shëndetësisë ka zënë një vend të posaçëm në të gjithë veprimtarinë e Zyrës së Komisionerit për vitin 2020.

Në këtë kontekst, Zyra e Komisionerit i ka kushtuar një vëmendje të shtuar këtij sektori, qoftë në rrafshin rregullator, qoftë në kuadër të veprimtarisë së saj monitoruese dhe mbikëqyrëse në terren.

Nga pikëpamja rregullatore, Zyra e Komisionerit, ka hartuar dhe publikuar disa akte me karakter detyrues, si dhe orientues, që lidhen me përpunimin e të dhënave shëndetësore.

Më kryesori, në këtë aspekt, është Udhëzimi nr. 49, datë 02.03.2020 "*Për mbrojtjen e të dhënave personale shëndetësore*" (në vijim, "*Udhëzimi nr. 49*)", i cili përfaqëson edhe një ndërhyrje përmirësuese të Zyrës së Komisionerit në sektorin e shëndetësisë, pasi shfuqizon dy udhëzimet e mëhershme në fuqi, konkretisht, Udhëzimin nr. 5, datë 26.05.2010 "*Për rregullat themelore në lidhje me mbrojtjen e të dhënave personale në sistemin e kujdesit shëndetësor*" dhe Udhëzimin nr. 23, datë 20.11.2012 "*Për përpunimin e të dhënave personale në sektorin e shëndetësisë*".

Qëllimi i këtij udhëzimi, i cili ka hyrë në fuqi më datë 05.03.2020, pas publikimit në Fletoren Zyrtare, është rregullimi i përpunimit të të dhënave personale që lidhen me shëndetin, duke synuar respektimin e të drejtave dhe lirive themelore të çdo individi, veçanërisht, të drejtën për privatësi dhe mbrojtje të të dhënave personale.

Udhëzimi nr. 49 është detyrues dhe i zbatueshëm për të gjithë Kontrolluesit (publikë dhe privatë) që veprojnë në sistemin e kujdesit shëndetësor.

Siç vërehet edhe nga data e publikimit të tij në Fletoren Zyrtare, Udhëzimi nr. 49 ka hyrë në fuqi përpara shpalljes, nga Këshilli i Ministrave, së gjendjes së emergjencës në rang vendi, si rezultat i përhapjes së pandemisë COVID-19, çfarë ka mundësuar, fatmirësisht, adresimin paraprakisht të situatës së përpunimit të të dhënave personale gjatë periudhës së pandemisë, e cila vijon ende.

Më tej, duke ndjekur me kujdes të posaçëm veprimtaritë e përpunimit të të dhënave personale në sektorin shëndetësor, ndër të tjera, në kuadër të masave për përballimin dhe parandalimin e përhapjes së mëtejshme të COVID-19, Zyra e Komisionerit ka përgatitur e publikuar 3 udhëzues, me karakter të përgjithshëm, si dhe sipas disa sektorëve specifikë (përshirë këtu atë të shëndetësisë), bazuar kjo në dispozitat e legjislacionit në fuqi për mbrojtjen e të dhënave personale, si dhe në sintoni të plotë edhe me praktikën e ndjekur në vendet e BE dhe më gjerë.

Publikimi i udhëzuesve të sipërpërmendur ka synuar të orientojë dhe udhëzojë Kontrolluesit e sektorit të shëndetësisë në adresimin sa më korrekt të detyrimeve që burojnë nga legjislacioni për mbrojtjen e të dhënave personale, si dhe, njëkohësisht, për të eliminuar sa më shumë të jetë e mundur pasiguritë që sjell me vete, në kontekstin e respektimit të të drejtave të njeriut në përgjithësi, ballafaqimi me një situatë të paparashikueshme si pandemia COVID-19.

Zyra e Komisionerit e ka konsideruar prioritare një ndërhyrje të tillë, ndër të tjera, me qëllim orientimin e autoriteteve ligjzbatuese, nëpërmjet të udhëzuesve në fjalë, në lidhje me masat e survejancës dhe hetimit epidemiologjik të COVID-19 që këto të fundit kanë marrë (në bazë të legjislacionit për parandalimin e infeksioneve dhe sëmundjeve infektive), të cilat, në mënyrë të vetëkuptueshme, pasjellin përpunim të të dhënave personale dhe sensitive (shëndetësore) të personave të infektuar me dhe/ose të ekspozuar ndaj COVID-19.

Sa më sipër, të diktuar edhe nga situata të cilën po kalojmë, si dhe, veçanërisht, nga detyrat e lëna në bazë të Rezolutës së Kuvendit, krahas angazhimit të saj rregullues, sensibilizues dhe orientues, Zyra e Komisionerit ka zhvilluar një fushatë inspektimesh në Kontrollues, publikë dhe privatë, në sektorin e kujdesit shëndetësor, rezultatet e përmbledhura të të cilit pasqyrohen në këtë pjesë të Raportit.

II. Faktet dhe rrethanat e zhvillimit të mbikëqyrjes

Çdo Kontrollues publik dhe privat në Republikën e Shqipërisë, gjatë ushtrimit të veprimtarisë së tij, është i detyruar të veprojë në përputhje me dispozitat e Ligjit për Mbrojtjen e të Dhënave Personale, si dhe aktet nënligjore të nxjerra nga Komisioneri në zbatim të tij.

Situata e shkaktuar nga pandemia COVID-19 nuk përbën shkak të ligjshëm për kufizimin dhe mosrespektimin e të drejtës së çdo qytetari për mbrojtjen e të dhënave të tij personale dhe, rrjedhimisht, për mosrespektimin e jetës së tij private, të cilat së bashku përbëjnë një kategori të drejtash vetjake të mbrojtura nga Kushtetuta (neni 35).

Veçanërisht i rëndësishëm, në këtë kontekst, është përpunimi i të dhënave që lidhen me shëndetin e qytetarëve, sidomos të dhënat lidhur me infektimin nga COVID-19, si dhe sëmundjet e tjera të cilat, në kombinim me të, mund të kërcënojnë seriozisht shëndetin dhe/ose jetën e qytetarëve.

Këto informacione përbëjnë të dhëna sensitive në referim të pikës 4 të nenit 3 të Ligjit për Mbrojtjen e të Dhënave Personale dhe përpunimi i tyre rregullohet specifikisht nga neni 7 i këtij ligji, në harmoni me nenet 5 dhe 6 të tij.

Ngjarjet si përhapja e COVID-19, të cilat përbëjnë kërcënime serioze për shëndetin dhe jetën e qytetarëve, kërkojnë masa kontrolli të veçanta apo të lidhura me gjurmimin e

kontakteve në mënyrë të koordinuar, për të identifikuar persona që mund të jenë të infektuar apo të ekspozuar ndaj rrezikut të infektimit.

Gjithashtu, në kuadër të masave kundër pandemisë, organet e angazhuara në luftën kundër saj mund ta kenë të detyrueshme apo nevojshme transferimin ndërkombëtar të të dhënave në vende dhe/ose organizata ndërkombëtare të ndryshme (si OBSH), për qëllime statistikore, shkencore dhe/ose për qëllime analizimi më të specializuar të tyre.

Zyra e Komisionerit vlerëson se përpunimi i të dhënave personale dhe, veçanërisht, atyre të lidhura me shëndetin e subjekteve të të dhënave është jashtëzakonisht i rëndësishëm për mbrojtjen e shëndetit dhe interesit publik, në situatën në të cilën ndodhet vendi aktualisht.

Në këto kushte, përveç mbledhjes dhe ruajtjes së të dhënave personale, gjendet parimisht e arsyetuar edhe nevoja për transmetim dhe shkëmbim të shtuar të këtyre të dhënave, midis çdo Kontrolluesi dhe institucioneve ligjzbatuese në kuadër të masave kundra virusit COVID-19, procese përpunuese këto që, në çdo rast, duhet të paraprihen nga masa të përshtatshme tekniko-organizative për garantimin e sigurisë së të dhënave dhe ruajtjen e konfidencialitetit, në përputhje me nenet 27 dhe 28 të Ligjit, si dhe Udhëzimin nr. 47 të Komisionerit, i cili, siç shpjegohet në Pjesën I të këtij Raporti, është veçanërisht i rëndësishëm në këtë aspekt.

Zyra e Komisionerit ka konstatuar gjatë gjithë kësaj periudhe një shqetësim në rritje të subjekteve të të dhënave lidhur me ligjshmërinë e përpunimit të të dhënave të tyre personale, si dhe për sigurinë dhe ruajtjen e konfidencialitetit të tyre, nga operatorët e sektorit të kujdesit shëndetësor.

Ky shqetësim është konstatuar qoftë në kuadër të ankesave të paraqitura nga subjektet e të dhënave pranë Zyrës së Komisionerit, qoftë në indicie të publikuara në media të ndryshme, lidhur me pretendime për përhapje të paligjshme të të dhënave personale, veçanërisht atyre shëndetësore, të pacientëve të infektuar me COVID-19.

Në të gjitha rastet, Zyra e Komisionerit ka proceduar në rrugë ligjore, si dhe, njëkohësisht, ka reaguar publikisht, nëpërmjet përgatitjes dhe publikimit të 3 udhëzuesve të dedikuar për situatën e pandemisë, si dhe nëpërmjet njoftimesh për shtyp, ku ka tërhequr vëmendjen e Kontrolluesve në fjalë për të vepruar në përputhje me legjislacionin në fuqi për mbrojtjen e të dhënave personale.

Më konkretisht, për arsyet e lartpërmendura, Zyra e Komisionerit brenda muajit nëntor, ka kryer një grup hetimesh administrative pranë Kontrolluesve publikë dhe privatë të sektorit – pavarësisht rrezikut të shtuar të infektimit të mundshëm me COVID-19, gjatë hetimeve administrative.

Për këtë qëllim, objekt hetimi dhe mbikëqyrjeje kanë qenë subjektet në vijim.

(i) ***Në sektorin publik***:

- Instituti i Shëndetit Publik
- Operatori i Shërbimeve të Kujdesit Shëndetësor
- Njësia Vendore e Kujdesit Shëndetësor Tiranë
- Qendra Shëndetësore e Specialiteteve nr. 1.

(ii) ***Në sektorin privat***:

- Spitali Amerikan;
- Klinika "Intermedica Center"
- Klinika "Pegasus Med"
- Spitali "Salus".

III. Baza ligjore

Në zbatim të kompetencave të sanksionuara në nenet 31 dhe 32 të Ligjit, siç përmendet më sipër, Zyra e Komisionerit ka realizuar një numër inspektimesh administrative, me qëllim mbikëqyrjen e veprimtarive përpunuese nga Kontrollues në sektorin shëndetësor, publik dhe privat, me theks verifikimin e respektimit të parimeve dhe kritereve ligjore të parashikuar në nenet 5, 6 dhe 7 të Ligjit, si dhe verifikimin e masave teknike dhe organizative për parandalimin e përhapjes së paligjshme të të dhënave personale dhe sensitive të pacientëve, në përputhje me nenet 27 dhe 28 të Ligjit.

Në këtë kontekst, krahas dispozitave të sipërpërmendura të ligjit, inspektimet janë bazuar edhe në parashikimet detyruese të akteve ligjore të nxjerra nga Zyra e Komisionerit në zbatim të Ligjit, përfshirë, këtu, por pa u kufizuar dispozitat e Udhëzimeve nr. 47, 48 dhe 49 të Komisionerit.

Ndërsa, një përshkrim i përgjithshëm i detyrimeve kryesore që burojnë nga Udhëzimet nr. 47 dhe 48 është paraqitur në Pjesën I të këtij Raporti, në vijim janë përmbledhur detyrimet kryesore që burojnë nga Udhëzimi nr. 49:

- Të dhënat shëndetësore duhet të përpunohen në mënyrë transparente, të ligjshme dhe të drejtë, të mblidhen për qëllime të qarta, specifike e legjitime dhe nuk duhet të përpunohen në kundërshtim me këto qëllime.

- Përpunimi i të dhënave shëndetësore duhet të jetë proporcional dhe i nevojshëm në raport me qëllimin legjitim të synuar dhe duhet të realizohet vetëm bazuar në ligj ose në pëlqimin e subjektit të të dhënave.

- Gjatë përpunimit të të dhënave shëndetësore, Kontrolluesit duhet të marrin masat e përshtatshme të sigurisë, të cilat duhet të parashikojnë zhvillimet më të fundit teknologjike, natyrën sensitive të të dhënave që lidhen me shëndetin dhe vlerësimin e rrezikut të mundshëm, me qëllim parandalimin e rreziqeve të tilla si aksesi i paautorizuar tek të dhënat, shkatërrimi, humbja, përdorimi, mos përdorimi, pamundësia e aksesimit të tyre.

- Profesionistët e shëndetësisë në sektorët të ndryshëm të kujdesit shëndetësor duhet t'i nënshtrohen rregullave mbi ruajtjen e konfidencialitetit.

- Kontrolluesi duhet të informojë subjektet e të dhënave për përpunimin e të dhënave të tyre që lidhen me shëndetin në lidhje me identitetin, qëllimin e përpunimit, kohëzgjatjen, kategoritë e marrësve, mundësinë e kundërshtimit dhe ofrimin e kushteve për të ushtruar të drejtat. Informacioni duhet të jetë i kuptueshëm dhe lehtësisht i aksesueshëm.

- Afati i ruajtjes së të dhënave shëndetësore, caktohet në përputhje me legjislacionin specifik dhe legjislacionin për mbrojtjen e të dhënave personale.

- Të dhënat e përpunuara në mënyrë manuale ose elektronike pas përfundimit të afatit shkatërrohen ose anonimizohen në mënyrë që individët të mos identifikohen ose të bëhen të identifikueshëm.

- Kontrolluesit dhe përpunuesit publik dhe privat të dokumentacionit mjekësor duhet, në përputhje me legjislacionin e mbrojtjes së të dhënave, të hartojnë rregullore të brendshme të përshtatshme që reflekton parimet ne legjislacionin specifik.

IV. Problematikat e konstatuara

IV.1 Sektori publik

Synimi kryesor i inspektimit në sektorin publik ka qenë monitorimi i respektimit të legjislacionit për mbrojtjen e të dhënave personale në kuadër të përpunimit të të dhënave të personave të infektuar me COVID-19 dhe/ose ekspozuar ndaj këtij virusi.

Kontrolluesit, subjekt inspektimi, përpunojnë të dhëna personale sensitive (shëndetësore), në mënyrë manuale dhe elektronike, në përmbushje të detyrave dhe funksioneve të parashikuar në ligjin 15/2016 "*Për parandalimin e Infeksioneve dhe sëmundjeve infektive*", si dhe në përputhje me dispozitat e tjera detyruese të legjislacionit sektorial.

Konkretisht, nga verifikimet e kryera, rezulton se, në kuadër të hetimit epidemiologjik, Kontrolluesit mbledhin, ndër të tjera, të dhëna si "*emri, mbiemri, gjinia, mosha, adresa, numri i telefonit, etj.*", si dhe kryejnë anonimizimin e emrit dhe mbiemrit në mostrën e tamponit të përdorur për testimin për COVID-19, duke vendosur një kod për të mundësuar më vonë identifikimin e pacientit.

Nga verifikimet në terren, rezulton se Kontrolluesit në fjalë, komunikojnë të dhënat personale të pacientëve nëpërmjet e-maileve personale të stafit, si dhe të aplikacionit "*WhatsApp*". Kësisoj, rezulton se këta Kontrollues kanë formuar grupe të ngushta komunikimi në "*WhatsApp*", në të cilin raportohen në mënyrë të vazhdueshme rastet pozitive me COVID-19.

Gjithashtu, kjo formë komunikimi (*WhatsApp*), përdoret edhe për informimin e pacientëve.

Më tej, vërehet se pjesëmarrja dhe frekuenca e komunikimit të të dhënave të pacientëve COVID-19 dhe/ose atyre të ekspozuar ndaj tij, është jashtëzakonisht e lartë. Kjo ka rezultuar edhe në rrjedhje (përhapje të paligjshme) të të dhënave personale të pacientëve COVID-19 dhe/ose personave të ekspozuar ndaj këtyre të fundit.

Përmendim si shembull, këtu, një situatë të denoncuar pranë Zyrës së Komisionerit në lidhje me pretendimin për përhapje të paligjshme të listës së personave me COVID-19 në Njësinë Vendore të Kujdesit Shëndetësor (NJVKSH) Durrës. Pas verifikimeve të Zyrës së Komisionerit, konfirmuar zyrtarisht edhe nga NJVKSH Durrës, ka rezultuar se lista e të infektuarve me COVID-19 qarkullohet nëpërmjet *WhatsApp,* ndër të tjera, në komunikime me 18 (tetëmbëdhjetë) mjekë familjeje, etj.

Sa më sipër, gjatë inspektimeve të kryera në sektorin publik janë konstatuar problematika të mëdha në drejtim të respektimit të legjislacionit për mbrojtjen e të dhënave personale nga Kontrolluesi subjekt inspektimi.

Veçanërisht problematike është gjendja e nivelit të sigurisë së të dhënave, si rezultat i mungesës së masave të nevojshme tekniko-organizative siç parashikohen nga dispozitat e legjislacionit në fuqi.

Në mënyrë të përmbledhur, në vijim janë pasqyruar disa nga problematikat kryesore:

(i) Mungojnë rregullat të qarta për garantimin e mbrojtjes, përpunimin, ruajtjen dhe sigurinë e të dhënave personale, në mënyrë që të përcaktojnë procedurat organizative dhe teknike në lidhje me masat për mbrojtjen e të dhënave personale.

Kontrollues të caktuar rezultojnë të kenë rregullore standarde në lidhje me përpunimin e të dhënave personale, por të pamjaftueshme dhe të papërshtatshme për të adresuar kërkesat e legjislacionit në fuqi në fushën e mbrojtjes së të dhënave personale të pacientëve;

Në bazë të nenit 2 të Udhëzimit nr. 49, Kontrolluesit janë të detyruar të marrin masa të përshtatshme sigurie, të cilat duhet të parashikojnë zhvillimet më të fundit teknologjike, natyrën sensitive të të dhënave që lidhen me shëndetin dhe vlerësimin e rrezikut të mundshëm, me qëllim parandalimin e rreziqeve të tilla si aksesi i paautorizuar tek të dhënat, shkatërrimi, humbja, përdorimi, mos përdorimi, pamundësia e aksesimit të tyre.

Sa më sipër, konstatohet një mungesë e plotë e rregullimeve lidhur me nivelet e aksesit në të dhënat sensitive (sidomos të pacientëve COVID-19).

Kjo mungesë shkakton pamundësi për të gjurmuar dhe hetuar rastet e rrjedhjes së listave të pacientëve, pasi, siç theksohet më sipër, numri i madh i pjesëmarrësve në komunikimet *WhatsApp*, si dhe frekuenca e lartë e tyre e pamundëson këtë (siç ishte rasti i NJVKSH Durrës).

Sqarojmë se përcaktimi i niveleve të aksesit dhe gjurmueshmërisë së personave të angazhuar në përpunimin e të dhënave personale, të cilat mund të jenë shpërndarë në mënyrë të paligjshme, ndihmon në parandalimin e tyre në raste të tjera, në ndëshkimin e shkelësve, si dhe në garantimin e të drejtës së subjekteve të të dhënave personale për të kërkuar dëmshpërblim ndaj këtyre të fundit (në kuptim të neneve 17 dhe 28 të Ligjit për Mbrojtjen e të Dhënave Personale).

(ii) Mungon çdo element i infrastrukturës së nevojshme për ngritjen, mirëmbajtjen dhe administrimin e SMSI për mbrojtjen e të dhënave personale, të parashikuara në Udhëzimin nr. 47;

Gjithashtu, nuk është kryer asnjë trajnim me personelin përkatës lidhur me respektimin e legjislacionit në fuqi në fushën e mbrojtjen së të dhënave personale. Në bazë të Udhëzimit nr. 47, ky trajnim zhvillohet, të paktën, 1 (një) herë në vit;

(iii) Mungon informimi i subjekteve të të dhënave, në lidhje kohëzgjatjen e përpunimit të të dhënave të tyre, të drejtën për të kërkuar, sipas rastit, akses, korrigjim, fshirje, etj., si dhe në lidhje të çdo element tjetër informimi të detyrueshëm për Kontrolluesit në bazë nenit 18 të Ligjit për Mbrojtjen e të Dhënave Personale.

Gjithashtu, subjekteve të të dhënave nuk rezulton t'ju vihet në dispozicion asnjë informacion në lidhje me kohëzgjatjen e përpunimit të të dhënave të tyre, si dhe në lidhje me shkatërrimin/fshirjen e të dhënave në përfundim të afatit përkatës të përpunimit;

(iv) Kontrolluesit nuk disponojnë rregullime konkrete për menaxhimin e të dhënave personale dhe ruajtjen e konfidencialitetit të subjekteve të të dhënave që përdorin faqet zyrtare të internetit, duke mos informuar subjektet e të dhënave, që vizitojnë këtë faqe, për mënyrat e përpunimit të të dhënave, masat e sigurisë, ruajtjen e

konfidencialitetit, të drejtat e subjekteve të të dhënave dhe detyrimet e Kontrolluesit në kuadër të mbrojtjes së privatësisë;

(v) Mosrespektim i detyrimit për të njoftuar dhe përditësuar të dhënat personale sa here që përpunohen kategori apo sasi të ndryshme të tyre, me qëllim mundësimin subjekteve të të dhënave që të informohen në lidhje me çdo përpunim të të dhënave personale të tyre dhe, kësisoj, për të ushtruar të drejtat që ju akordon shprehimisht kreu IV i Ligjit për Mbrojtjen e të Dhënave Personale.

IV.2 Sektori privat

Inspektimet e kryera në sektorin privat kanë patur një fokus më të përgjithshëm sesa në rastin e sektorit publik, duke mos u fokusuar vetëm në lidhje me veprimtaritë përpunuese në kuadër të shërbimeve që ofrojnë për testimin e të dyshuarve me COVID-19.

Kështu, kontrollet e ushtruara kanë patur si objekt verifikimin e respektimit nga këta Kontrollues të detyrimeve që burojnë nga legjislacioni për mbrojtjen e të dhënave personale.

Në këtë sektor konstatohet një angazhim më i madh për adresimin e kërkesave të përgjithshme të legjislacionit për mbrojtjen e të dhënave personale, si dhe në drejtim të garantimit të respektimit të të drejtave të subjekteve të të dhënave personale.

Gjithashtu, vërehet se Kontrolluesit në këtë sektor janë të orientuar drejt marrjes së masave tekniko-organizative për garantimin e sigurisë së të dhënave personale, të cilat ata përpunojnë.

Megjithatë, edhe në këtë sektor masat e marra në rrafshin e sigurisë së të dhënave janë jashtëzakonisht larg nivelit standard që imponojnë Udhëzimet nr. 47, 48 dhe 49 të Komisionerit.

Konstatimet kryesore lidhur me gjendjen e përpunimit të të dhënave personale në sektorin privat janë renditur në vijim:

(i) Nga verifikimet e kryera, rezulton se Kontrolluesit përpunojnë të dhëna si "*emri, mbiemri, gjinia, mosha, adresa, numri i telefonit, të dhëna shëndetësore, etj.*".

Ata informojnë subjektet e të dhënave lidhur me përpunimin e të dhënave personale/sensitive, megjithatë ky informacion ka nevojë të detajohet për të specifikuar, ndër të tjera, në përputhje me nenin 18 të Ligjit për Mbrojtjen e të Dhënave Personale, se cilat të dhëna personale janë të detyrueshme për t'u paraqitur dhe cilat janë vullnetare, qëllimin dhe mënyrat e përpunimit të të dhënave, masat e sigurisë, të drejtat e subjekteve të të dhënave dhe detyrimet e Kontrolluesit.

Gjithashtu, në shumë raste, subjektet e të dhënave nuk informohen në lidhje me marrësit e të dhënave personale në rastet e përhapjes dhe transferimit të të dhënave, si dhe "*Politika e Privatësisë*" në faqet përkatëse të internetit nuk parashikojnë elementet e nevojshëm për informim, në zbatim të nenit 18 të Ligjit për Mbrojtjen e të Dhënave Personale.

(ii) Në shumë raste, Kontrolluesit rezultojnë të mos kenë parashikuar afate për ruajtjen e të dhënave personale/sensitive të pacientëve që përpunohen, në kundërshtim me germën "d" të pikës 1 të nenit 5 të Ligjit për Mbrojtjen e të Dhënave Personale, si dhe nenin 5 të Udhëzimit nr. 49, si dhe konstatohen përpunime (ruajtje) të të dhënave në tejkalim të qëllimit të përpunimit, në kundërshtim me parimet e mbrojtjes së të dhënave personale sanksionuar në gërmën *"c"* të pikës 1, të nenit 5 dhe kriteret ligjore të sanksionuara në nenin 6 të Ligjit;

(iii) Vërehet përpjekje për të rregulluar marrëdhëniet e delegimit të përpunimit të të dhënave personale, nëpërmjet kontratave të delegimit të parashikuara në nenin 20 të Ligjit për Mbrojtjen e të Dhënave Personale dhe Udhëzimit nr. 19, megjithatë, në pjesën dërrmuese të rasteve, këto instrumente kontraktore detyruese rezultojnë të përmbajnë vetëm formalisht detyrimet standarde të ligjit, pa reflektuar konkretisht nivelet e delegimit, llojin e përpunimit, kohëzgjatjen, etj.

Çfarë është më e rëndësishmja, nuk rezulton asnjë masë apo qoftë përpjekje konkrete nga këta Kontrollues lidhur me verifikimin dhe sigurimin që përpunuesit e kontraktuar për përpunimin e të dhënave personale të pacientëve të tyre (veçanërisht atyre sensitive) të kenë marrë masa tekniko-organizative për të mbrojtur të dhënat në fjalë nga çdo përpunim i paautorizuar, duke përfshirë, por pa u kufizuar, shkatërrimin, humbjen, përhapjen e paligjshme apo dëmtimin e tyre;

Gjithsesi, janë konstatuar edhe raste kur delegimi i përpunimit nuk është kryer në bazë të një marrëveshjeje delegimi sipas Udhëzimit nr.19.

(iv) Kontrolluesit disponojnë rregullime të përgjithshme, me shkrim, lidhur me menaxhimin e të dhënave personale dhe ruajtjen e konfidencialitetit të subjekteve të të dhënave, por të padetajuara rregullisht në lidhje me masat tekniko-organizative të përshtatshme dhe të zbatueshme për garantimin e mbrojtjes së të dhënave personale dhe sensitive, kriteret e ligjshmërisë së përpunimit të të dhënave të pacientëve, masat për garantimin e gjurmueshmërisë dhe kontrollit të veprimeve të personave/personelit që ka pasur dhe/ose ka akses në këto të dhëna, si dhe për mënyrën e shkatërrimit të tyre kur të jetë përmbushur qëllimi i përpunimit të tyre;

(v) Asnjë Kontrollues nuk ka realizuar detyrimet në lidhje me ngritjen, administrimin dhe mirëmbajtjen e sistemit të menaxhimit së sigurisë së informacionit (SMSI) lidhur me mbrojtjen e të dhënave personale, të parashikuar nga Udhëzimi nr. 47, në harmoni me standardin e parashikuar në Udhëzimin nr. 48.

Gjithashtu, në pjesën më të madhe të rasteve, Kontrolluesit nuk rezultojnë të kenë marrë masa për trajnimin e detyrueshëm të punonjësve që kanë akses dhe përpunojnë të dhëna personale, lidhur me legjislacionin në fuqi për mbrojtjen e të dhënave personale, sipas përcaktimeve të Udhëzimit nr. 47.

V. Konkluzione dhe rekomandime

Zyra e Komisionerit thekson se nevojitet një angazhim serioz dhe rigoroz i Kontrolluesve në sektorin e kujdesit shëndetësor, me qëllim garantimin e respektimit të të drejtave të subjekteve të të dhënave personale, si dhe, në mënyrë imediate, në lidhje me marrjen e masave teknike dhe organizative për garantimin e sigurisë dhe konfidencialitetit të të dhënave personale, në përputhje me Udhëzimet nr. 47, 48 dhe 49 të Komisionerit.

Në këtë kontekst, për shkak të cilësisë së tyre si Kontrollues/përpunues të mëdhenj, si dhe për shkak të natyrës së veprimtarisë që ata ushtrojnë, e cila kërkon masa të shtuara teknike dhe organizative për garantimin e sigurisë së të dhënave personale, Kontrolluesit e sektorit të kujdesit shëndetësor, jo vetëm duhet të krijojnë, mirëmbajnë dhe administrojnë SMSI në përputhje me parashikimet detyruese të Udhëzimit nr. 47, por duhet ta konsiderojnë prioritare këtë çështje thelbësore për garantimin e sigurisë së të dhënave personale të pacientëve të tyre.

Për këtë qëllim Zyra e Komisionerit rekomandon që Kontrolluesit e këtij sektori të vlerësojnë marrjen përsipër të angazhimeve vetërregulluese, në lidhje e ekzistencën e SMSI, edhe nëpërmjet mekanizmit të certifikimit të SMSI.

Gjithashtu, konstatohet një mungesë e përgjithshme e njohurive të të gjitha niveleve të këtij sektori në lidhje me detyrimet që burojnë nga legjislacioni për mbrojtjen e të dhënave personale.

Për këtë arsye, është jo vetëm detyrim, por, pikë së pari, në dobi të vetë Kontrolluesve realizimi dhe dokumentimi i trajnimeve të vazhdueshme të personelit përkatës (të përfshirë aktivisht në përpunimin e të dhënave personale) në lidhje me parimet, kriteret dhe detyrimet që duhen respektuar dhe përmbushur në kuadër të legjislacionit për mbrojtjen e të dhënave personale.

Bazuar në konstatimet e reflektuara në këtë raport, krahas procedimeve individuale administrative, Zyra e Komisionerit do të dalë me një rekomandim unifikues sektorial, për të vënë në dukje dhe orientuar më konkretisht këta Kontrollues në lidhje me mangësitë dhe detyrimet e tyre për t’i adresuar ato, në përputhje me dispozitat e ligjit dhe akteve nënligjore të Komisionerit, si dhe do të vijojë monitorimin e rreptë të tyre edhe në të ardhmen.