

Strengthening of the Data Protection Commissioner Office in Albania
for Alignment with European Union Standards
Project EuropeAid/129606/C/SER/AL

Udhëzues Praktik Për Kontrolluesit E Të Dhënave



Ky projekt u financua
nga Bashkimi Evropian



Republika e Shqipërisë



100 Vjet Pavarësi



Përfutësi i projektit



FIIAPP

Zbatuesi i projektit

Udhëzues Praktik Për Kontrolluesit E Të Dhënave

JUDr Jiří Maštalka, Dr Stefan Szyszko

Mendimet e shprehura në këtë publikim nuk pasqyrojnë në mënyrë të domosdoshme pikëpamjet e Bashkimit Evropian.

The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Union.

JUDr Jiří Maštalka
Kapituly 2-7

Dr Stefan Szyszko
Kapituly 8-11

Tiraně 2012

PËRMBAJTJA

I.	Hyrje	7
II.	Legjislacioni evropian dhe shqiptar si dhe përkufizimet bazë të mbrojtjes së të dhënave	9
2.1	Legjislacioni evropian dhe ligjet vendase për mbrojtjen e të dhënave	9
2.2	Përkufizime në ligjin për mbrojtjen e të dhënave	12
III.	Legjitimimi i përpunimit të të dhënave personale	20
IV.	Cilësia e të dhënave	23
4.1	Parimi i përdorimit përfundimtar	23
4.2	Parimi i saktësisë së të dhënave	23
4.3	Parimi i proporcionalitetit/parimi i përshtatshmërisë së të dhënave	24
4.4	Parimi i kufizimit të kohës	24
V.	E drejta e subjektit të të dhënave për tu informuar, për të marrë akses në të dhënat dhe të drejta të tjera	27
VI.	Detyrimi për të njoftuar	30
VII.	Transferimi i të dhënave tek shtete të treta	32
VIII.	Siguria e të dhënave personale: koncepte bazë, detyrime ligjore e rekomandime	35
8.1	Detyrime të zakonshme për sigurinë e të dhënave për çdo kontrollues që përpunon të dhëna personale	37
8.2	Detyrimet kryesore që rrjedhin nga “Udhëzimi për detyrimet e kontrolluesve dhe përpunuesve përpara se të përpunojnë të dhëna personale”	40
8.3	Detyrime të ndryshme për sigurinë për kontrolluesit e mëdhenj dhe të vegjël, arsyet për diferencimin, çështjet kryesore	41
8.4	Rregulla shtesë për sigurinë kur delegohet përpunimi i të dhënave	43
IX.	Detyrimet kryesore që rrjedhin nga “Udhëzimi për përcaktimin e rregullave të sigurisë së të dhënave personale të përpunuara nga kontrolluesit e vegjël”	44
X.	Detyrimet kryesore që rrjedhin nga “Udhëzimi për përcaktimin e	

	rregullave të sigurisë së të dhënave personale që përpunohen nga kontrolluesit e mëdhenj”	46
10.1	Roli i personit të kontaktit	49
XI.	Detyrimet kryesore që rrjedhin nga “Udhëzimi për delegimin e të dhënave personale”	55

I . HYRJJE

Ky Udhëzues është hartuar në kuadër të Projektit të financuar nga BE për “Forcimin e Komisionerit për Mbrojtjen e të Dhënave Personale në Shqipëri për përafrimin me standardet e BE-së”.

Nisja e një procesi përpunimi të të dhënave personale është moment i rëndësishëm në punën e një kontrolluesi, jo vetëm për suksesin e sipërmarrjes, por edhe për shkak të rëndësisë së mbrojtjes së të drejtave të individëve dhe subjekteve të të dhënave, të dhënat e të cilëve do të përpunohen. Ky udhëzues ka për qëllim t’ju ofrojë kontrolluesve që veprojnë në Republikën e Shqipërisë, përfaqësive diplomatike shqiptare si dhe kontrolluesve të cilët nuk janë të vendosur në Republikën e Shqipërisë, por që e ushtrojnë veprimtarinë nëpërmjet përdorimit të çdo mjeti që ndodhet në Republikën e Shqipërisë, udhëzime të qarta dhe të kuptueshme që do t’i ndihmojnë ata të respektojnë ligjin dhe të drejtat e subjekteve të të dhënave, si dhe të lehtësojë punën e tyre.

Për të patur një përpunim të suksesshëm dhe të ligjshëm të të dhënave personale, është e nevojshme që kontrolluesit, para së gjithash, të jenë në dijeni mbi shumëllojshmërinë e dispozitave ligjore të cilat kanë një ndikim të rëndësishëm në veprimtarinë e tyre të përditshme. Një sërë aktivitete janë të lidhura me nevojën e përdorimit të të dhënave personale, prandaj çdo subjekt duhet të përmbushë disa detyrime në fushën e mbrojtjes së të dhënave. Këto detyrime janë të zbatueshme për sektorin publik dhe privat.

Ky Udhëzues, duke përshkruar disa çështje të përgjithshme lidhur me mbrojtjen e të dhënave, i drejtohet kontrolluesve që dëshirojnë të fillojnë një proces përpunimi të të dhënave personale. Përveç kësaj, ky dokument ka për qëllim të paraqesë dhe të përshkruajë kuadrin evropian në këtë fushë. Për pasojë, ofron një vështrim të përgjithshëm të legjislacionit shqiptar për përpunimin e të dhënave personale, duke

marrë parasysh gjithashtu edhe legjislacionin evropian. Udhëzuesi synon të ndërgjegjësojë subjektet përpunuese të të dhënave personale, si kontrolluesit edhe përpunuesit për detyrat e tyre, për të siguruar një përpunim të duhur, duke marrë parasysh detyrimet e tyre ligjore dhe kodet e praktikës së mirë. Vëmendje e veçantë i kushtohet çështjeve të delegimit të proceseve të përpunimit (outsourcing) pasi është një marrëveshje e rëndësishme për përpunimin e të dhënave personale si në sektorin publik edhe në atë privat.

Megjithatë, për të marrë informacione të mëtejshme më të detajuara, Ju rekomandojmë të kontaktoni Komisionerin për Mbrojtjen e të Dhënave Personale në Shqipëri dhe të njiheni me materialet e vendosura në faqen e tij në internet (<http://www.kmdp.al>).

Ne kemi bindjen se ky Udhëzues do të rezultojë një mjet i vlefshëm për ju.

Flora ÇABEJ (POGAÇE)

Komisioner për Mbrojtjen e të Dhënave Personale



Dorota SKOLIMOWSKA

Drejtuesja e Ekipit të Projektit



II. LEGJISLACIONI EVROPIAN DHE SHQIPTAR SI DHE PËRKUFIZIMET BAZË TË MBROJTJES SË TË DHËNAVE.

2.1 Legjislacioni evropian dhe ligjet vendase për mbrojtjen e të dhënave.

Në Evropë, mbrojtja e të dhënave personale ka një rëndësi të veçantë. Si një nga të drejtat themelore, ajo garantohet nga një numër aktesh ligjore ndërkombëtare dhe kombëtare. E drejta për respektimin e jetës private dhe familjare është e garantuar në *Nenin 8 të Konventës Evropiane për të Drejtat e Njeriut*. Akti i parë ligjor ndërkombëtar që rregullon këto çështje në mënyrë gjithëpërfshirëse është *Konventa Nr. 108 "Për mbrojtjen e individëve në lidhje me përpunimin automatik të të dhënave personale"*, e miratuar nga Këshilli i Evropës më 28 janar 1981. Në rang Bashkimi Evropian, këto çështje janë të rregulluara në *Direktivën 95/46/EC të Parlamentit Evropian dhe Këshillit, datë 24 tetor 1995, "Për mbrojtjen e individëve në lidhje me përpunimin e të dhënave personale dhe për lëvizjen e lirë të këtyre të dhënave"*. Për më tepër, e drejta për mbrojtjen e të dhënave mbrohet si e drejtë themelore në *Nenin 8 të Kartës së të Drejtave Themelore të Bashkimit Evropian dhe në Nenin 16 të Traktatit për Funksonimin e Bashkimit Evropian*. Për sa i përket legjislacionit të BE-së, përveç Direktivës 95/46/EC, ka edhe akte të tjera ligjore që rregullojnë mbrojtjen e të dhënave personale. Në një masë të madhe, ato plotësojnë dispozitat e Direktivës 95/46/EC, e cila është e një natyre të përgjithshme dhe shërben si një pikë referimi për legjislacionet përkatëse të vendeve të BE-së.

Objekti kryesor i Direktivës 95/46/EC është të sigurojë nivelin më të lartë të mundshëm të mbrojtjes së të dhënave personale dhe të lehtësojë lëvizjen e lirë të të dhënave në kuadër të Bashkimit Evropian dhe praktikisht në kuadër të mbarë Zonës Ekonomike Evropiane. Përpunimi i të dhënave personale në Komunitet duhet të kryhet në përputhje me ligjin e Shtetit Anëtar në të cilin është regjistruar biznesi i kontrolluesit përgjegjës për përpunimin e të dhënave. Nëse një kontrollues është regjistruar në territorin e disa Shteteve Anëtare të ndryshme, në veçanti nëpërmjet degëve të tij, ai duhet të sigurojë që degët të jetë në përputhje

me kërkesat përkatëse të vendosura nga ligji përkatës i secilit Shtet Anëtar.







Shtetet anëtare të BE-së janë të detyruara të zbatojnë dispozitat e Direktivës 95/46/EC në sistemet e tyre ligjore. Shteteve Anëtare iu është lënë një farë hapësire e caktuar për sa i përket zbatimit të saj gjë që ka çuar në dallime të mundshme ndërmjet legjislacioneve kombëtare. Në kontekstin e anëtarësimit të ardhshëm të Shqipërisë në BE, qëllimi i Shqipërisë është të arrijë përafrimin e plotë të kuadrit ligjor me kërkesat e Direktivës 95/46/EC në këtë drejtim.

Kushtetuta e Republikës së Shqipërisë parashikon mbrojtjen e të dhënave personale. Neni 35 i Kushtetutës parashikon se askush nuk është i detyruar të bëjë publike të dhëna e tij personale, përveç nëse kjo është një kërkesë ligjore. Kushtetuta njeh të drejtën e subjektit të të dhënave për t'u informuar, si dhe të drejtën e tij për të kërkuar korrigjimin ose fshirjen e të dhënave të pasakta ose që janë mbledh në mënyrë të paligjshme.

Ligji kryesor që rregullon mbrojtjen e të dhënave personale në Shqipëri është Ligji Nr. 9887, datë 10 mars 2008, "Për mbrojtjen e të dhënave personale", i ndryshuar me Ligjin Nr. 48/2012 (më poshtë referuar "Ligji Nr. 9887"), i cili në këtë kontekst trajton më tej këtë të drejtë.

Ligji Nr. 9887 është një ligj i përgjithshëm që rregullon përpunimin e të dhënave personale në territorin e Shqipërisë, me përjashtim të përpunimit të kryer nga personat fizikë për nevojat thjesht personale apo familjare. Megjithatë, Ligji Nr. 9887 lejon përpunimin e të dhënave personale për qëllime të veçanta, sipas Direktivës 95/46/EC), si edhe, për të përmbushur detyrat e mandatuara nga ligji. Kontrolluesit duhet të shqyrtojnë nëse operacioni i synuar i përpunimit apo tashmë në kryerje e sipër është objekt i një rregulli të veçantë ligjor, veçanërisht në lidhje me të dhënat personale të mbledhura për qëllime të ndjekjes penale. Në këtë rast do të zbatohet legjislacioni përkatës i kësaj fushe.

Ligji Nr. 9887 (dhe legjislacioni për mbrojtjen e të dhënave personale si i tillë) mund të ndahet në tri pjesë kryesore tematike:

-  Dispozita që rregullojnë kushtet e përpunimit të të dhënave personale (të përfshira në Kapitujt II - VII të Ligjit Nr. 9887), përcaktojnë bazat ligjore për përpunimin e të dhënave, (për shembull, pëlqimi i subjektit të të dhënave, përcaktimi i qëllimit, njoftimi, masat për sigurinë e të dhënave personale, etj.)
-  Dispozita që rregullojnë pasojat e shkeljes së parimeve të përpunimit të të dhënave, që kanë të bëjë me çështje si në vijim:
 -  Zgjidhjet, të cilat mund të urdhërojnë shkatërrimin e të dhënave, ndërprerjen e përpunimit të paligjshëm, etj. (shiko nenin 30 të Ligjit Nr. 9887), megjithatë këto mjete nuk janë njësoj me sanksionet;
 -  Sanksionet administrative (shiko Nenin 39 të Ligjit Nr. 9887, mund të vendoset një gjobë deri në 1 000 000 lekë).
 -  Kompensim, për dëmet, ku zbatohen dispozitat e Kodit Civil (shiko nenin 17 të Ligjit Nr. 9887).
-  Dispozita procedurale që përcaktojnë metodat për vënien në vend të të drejtave në rast të shkeljes së rregullave për mbrojtjen e të dhënave. Procedurat për të kërkuar kompensim duhet të bëhen në gjykatë, ndërsa në raste të tjera (masat e ndërmjetme dhe sanksionet administrative) janë kompetencë e Autoritetit për mbrojtjen e të dhënave personale.

Autoriteti për mbrojtjen e të dhënave personale:

Komisioneri për Mbrojtjen e të Dhënave Personale (më poshtë referuar “Komisioneri”) është një organ mbikëqyrës i pavarur i veshur me një sërë kompetencash. Aktivitetet e Komisionerit janë të shumë anshme, duke filluar që nga trajtimi i ankesave dhe kryerja e inspektimeve (duke përfshirë vendosjen e gjobave) tek mbajtja e një regjistri të operacioneve të përpunimit të njoftuara, autorizimi i transfertave ndërkombëtare të të dhënave, apo përgatitjen e opinionëve për çështje specifike. Aktivitetet e Komisionerit rregullohen me Ligjin Nr. 9887, i ndryshuar.

Mbani mend:

Çdo subjekt i të dhënave që konstaton, ose hamendëson se një kontrollues po kryen përpunim të të dhënave personale që është në kundërshtim me ligjin, ka të drejtë të ankohet drejtpërdrejt tek Komisioneri.

2.2 Përkufizime në ligjin për mbrojtjen e të dhënave personale.

Përkufizimet kryesore në nenin 3 të Ligjit Nr. 9887 janë bazuar në nenin 2 të Direktivës 95/46/EC.

Të dhëna personale dhe subjekt i të dhënave:

Të dhëna 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





Subjekt i të dhënave personale është çdo person fizik, të cilit i përpunohen të dhënat personale.

Nocioni i të dhënave personale është i një rëndësie jetike, sepse aktet për mbrojtjen e të dhënave zbatohen vetëm për informacionin që përbën të dhënë personale. Mbrojtja e informacioneve të tjera mund të jenë e garantuar me dispozita të ligjeve të tjera.

Të dhënat personale përbëjnë një grup të dhënash të cilat lejojnë identifikimin e një person në atë masë që mund ta dallojmë këtë subjekt të të dhënave nga subjektet e tjera dhe që mund ta kontaktojmë apo për ta bërë relativisht të lehtë krijimin e një kontakti me të, dhe për të nxjerrë përfundime në lidhje me një subjekt të të dhënave, që mund të nxirren nga këto të dhëna. Gjatë përpunimit të të dhënave, këto të dhëna do të konsiderohen si personale për aq sa mund të arrihet lidhja e tyre me subjektin e të dhënave.

Kontrolluesit shpesh përdorin informacion bazë për personat fizikë, si emrat, mbiemrat, adresat, datat e lindjes, numrat e identifikimit apo të dhëna të tjera që përdoren shpesh, të cilat përhapen në situata të përditshme. Legjislacioni për mbrojtjen e të dhënave personale nuk përfshin një katalog të plotë të kategorive të të dhënave, për shkak të kompleksitetit të nocionit të të dhënave personale, do të ishte e pamundur të krijohet një katalog i tillë.

Shembuj:

-  *Disa lloje të dhënash që përbëjnë të dhëna personale janë për shembull: emri, mbiemri, adresa, arsimi, punësimi dhe përvoja profesionale.*
-  *Informacioni në lidhje me personat juridik apo njësitë organizative pa personalitet juridik nuk konsiderohet si e dhënë personale.*
-  *Informacioni në lidhje me një person të vdekur nuk klasifikohet si e dhënë personale, përveç kur në një situatë të veçantë ky informacion ka të bëjë me persona që janë gjallë.*
-  *Të dhëna për personat fizikë që ushtrojnë veprimtari tregtare kuptohen gjithashtu si të dhëna personale.*

Të dhëna sensitive:




“Të dhëna sensitive” është çdo informacion për personin fizik, që ka të bëjë me origjinën e tij, racore ose etnike, mendimet politike, anëtarësimin në sindikata, besimin, fetar apo filozofik, dënimin penal, si dhe të dhëna për shëndetin dhe jetën seksuale.

Në zbatim të Direktivës 95/46/EC, Ligji Nr. 9887 përfshin një katalog të kategorive të veçanta të të dhënave, të ashtuquajturat të dhëna sensitive. Nga vetë natyra e tyre, të dhëna sensitive janë veçuar nën një regjim të veçantë mbrojtje, sepse ato mund të shkaktojnë shkelje flagrante të të drejtave dhe lirive të individit, p.sh. diskriminim.

Duhet të mbahet parasysh se të dhënat sensitive mund të ndryshojnë nga një vend në tjetrin. Për shembull, në Ligjin çek, të dhënat sensitive përfshijnë edhe të dhënat gjenetike ose të dhënat biometrike që lejojnë identifikimin e drejtpërdrejtë, ose edhe verifikimin e subjektit të të dhënave gjithashtu.

Shembuj:

Gjatë zbatimit të Ligjit Nr. 9887, duhet të merren parasysh sa mëposhtë:

-  *E dhëna mbi përkatësinë etnike duhet të dallohet qartë nga e dhënat mbi shtetësinë. Këto nocione shpesh ngatërrohen në gjuhën e përditshme.*
-  *Informacioni për anëtarësimin në parti politike konsiderohet si e dhënë sensitive që zbulon mendimet apo qëndrimet politike.*
-  *Informacioni mbi dënim për një veprë penale konsiderohet si e dhënë sensitive. Si e tillë, ajo nuk mund të konsiderohet si informacion mbi një sjellje që mund të klasifikohet si kriminale, apo si e dhënë në lidhje me sanksione të tjera, p.sh. gjobat. Megjithatë, informacioni që një person i veçantë nuk ka qenë i dënuar për një veprë penale, për shembull, një dëshmi penaliteti e pastër e nxjerrë nga regjistri penal nuk konsiderohet si e dhënë sensitive. As informacioni në lidhje me një sjellje të caktuar që plotëson karakteristikat e një veprë penale por që nuk është ndëshkuar për shkak të moshës së mitur të autorit të veprës, për shembull, nuk konsiderohet si e dhënë sensitive.*

Përpunim i të dhënave personale:

“Përpunim i të dhënave personale” është çdo veprim ose grup veprimesh, të cilat janë kryer mbi të dhënat personale, me mjete automatike ose jo, të tilla si mbledhja, regjistrimi, organizimi, ruajtja, përshtatja ose ndryshimi, rikthimi, konsultimi, shfrytëzimi, transmetimi, shpërndarja ose ndryshe duke vënë në dispozicion, shtrirja ose kombinimi, fotografimi, pasqyrimi, hedhja, plotësimi, seleksionimi, bllokimi, asgjësimi ose shkatërrimi, edhe në qoftë se nuk janë të regjistruara në një bankë të dhënash.

Ky nocion është shumë i rëndësishëm për kontrolluesit, për shkak se ata kanë nevojë për një bazë të duhur ligjore për çdo operacion përpunimi të të dhënave personale.

Përpunimi mund të kryhet një ose disa herë, mund të jetë i ngjashëm ose i përputhshëm për nga ana teknologjike. Është shumë e rëndësishme të kujtojmë se një operacion i vetëm (i kryer një herë) me të dhënat, p.sh. përhapja e tyre, do të trajtohet si përpunimi i tyre.

Operacionet që konsiderohen si përpunim i të dhënave janë fotografimi, regjistrimi me zë ose figurë si dhe regjistrimi i karakteristikave fizike të përshtatshme për identifikim e personit (të tilla si shenjat e gishtave dhe të duarve, mostrat e ADN-së dhe imazhet e irisit). Ruajtja e të dhënave në formë të shkruar (në letër) konsiderohet gjithashtu si përpunim i të dhënave.

Megjithatë, një lloj i veçantë operacioni që është kryer në mënyrë të përsëritur dhe realizimi i të cilit është i ngjashëm, i përputhshëm për nga ana teknologjike kuptohet si përpunim. Nuk mund të përcaktohet se një grup operacionesh do të ndodhë vetëm një herë. Ose, që do të ndodhë vetëm një herë një operacion i vetëm nga tërësia e tyre. Ajo çfarë përcakton natyrën e tij është qëllimi për të përsëritur ose kryer këto operacione në rrethana të caktuara. Ky qëllim mund të dokumentohet në formën e përshkrimit, rrjedhës së punës, elemente teknike ose softuerë, etj. Termi “përpunimin i të dhënave personale” për shembull mund të jetë sinonim me “mbajtjen një regjistri, dosje apo regjistri të caktuar”.

Sistem arkivimi i të dhënave personale:

“Sistem arkivimi” është çdo grup i strukturuar i të dhënave personale, të cilat janë të aksesueshme në bazë të kriterëve specifike, të centralizuara, të decentralizuara ose të shpërndara në një bazë, funksionale ose gjeografike.

Mundësia për të kërkuar sipas ndonjë kriteri personal (emrit, mbiemrit, datës së lindjes, numrit të identifikimit) ose një kriteri jo personal (data e hyrjes së të dhënave në sistemin e arkivimit) përcakton natyrën e organizuar të një grupi të dhënash dhe kështu lejon klasifikimin e këtij grupi si një sistem arkivimi i të dhënave.

Shembull:

Një sistem tipik i arkivimit të të dhënave, në rastin e sipërmarrësve, janë dosjet personale të punonjësve të mbledhura në lidhje me punësimin e tyre dhe punën e kryer prej tyre, apo dosjet e konsumatorëve. Dosjet mund të mbahen si në sisteme TI ashtu edhe në formë shkresore.

Kontrollues:

“Kontrollues” është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër që, vetëm apo së bashku me të tjerë, përcakton qëllimet dhe mënyrat e përpunimit të të dhënave personale, në përputhje me ligjet dhe aktet nënligjore të fushës, dhe përgjigjet për përmbushjen e detyrimeve të përcaktuara në këtë ligj. (Nr. 9887)

Një kontrollues vendos për qëllimet dhe mënyrat e përpunimit të të dhënave. Ai është përgjegjës për përpunimin e të dhënave personale dhe për kontrollimin e këtij përpunimi. Kontrollues mund të jenë autoritetet publike, autoritetet e qeverisjes vendore, subjektet ekonomike apo personat fizikë që zhvillojnë aktivitet ekonomik, etj, në qoftë se ata vendosin për qëllimet dhe mënyrat e përpunimit të të dhënave.

Përpunues:

“Përpunues” është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër që përpunon të dhëna personale në emër të kontrolluesit.

Kontrolluesi nuk duhet që të kryejë vetë të gjitha aktivitetet që lidhen me përpunimin e të dhënave personale. Ai mund të autorizojë një subjekt tjetër për të kryer përpunimin, tërësisht ose pjesërisht. Përpunuesi nuk bëhet kontrollues i përpunimit të të dhënave që i është ngarkuar. Megjithatë, përpunuesi është i detyruar të ruajë dhe mbrojë të dhënat personale.

Ligji Nr. 9887 (neni 20), ndër të tjera, kërkon që kontrata që ngarkon një subjekt tjetër me përpunimin e të dhënave duhet të hartohet me shkrim dhe duhet të specifikojë qartë objektin dhe qëllimin e përpunimit të të dhënave. Për sa i përket pajtueshmërisë me kërkesat për ruajtjen e të dhënave, përpunuesi do të mbajë të njëjtën përgjegjësi si kontrolluesi.

Shembull:

Shoqëria “XYZ” lidh kontrata me organizata të ndryshme për të kryer fushatën e saj të marketingut me postë dhe për të kryer pagesat e punonjësve të saj. Ajo jep udhëzime të qarta (se çfarë materiali marketingu

do të dërgohet dhe kujt to do t'i dërgohet, kush do të marrë pagesën dhe shumën, në çfarë date, etj.). Pavarësisht se organizatat kanë një farë lirie (përfshirë çfarë softueri të përdorin) detyrat e tyre janë tepër të qarta dhe të mirë përcaktuara edhe nëse agjencia postare mund të ofrojë këshilla (p.sh. këshillon të mos dërgohen letra në gusht), ato janë të detyruara të veprojnë siç udhëzon "XYZ". Për më tepër, vetëm një subjekt, Shoqëria "XYZ", ka të drejtë të përdorë të dhënat e përpunuara, të gjitha subjektet e tjera duhet të mbështeten në bazën ligjore të shoqërisë "XYZ" nëse vihet në dyshim aftësia e tyre ligjore për përpunimin e të dhënave. Në këtë rast është e qartë se shoqëria "XYZ" është kontrolluesi i të dhënave dhe secila prej organizatave të veçanta mund të konsiderohet si përpunues në lidhje me përpunimin specifik të të dhënave të kryer në emër të saj.

Palë e tretë:

"Palë e tretë" është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër, përveç subjektit të të dhënave, kontrolluesit, përpunuesit dhe personave, të cilët, nën autoritetin e drejtpërdrejtë të kontrolluesit apo përpunuesit, janë të autorizuar të përpunojnë të dhëna.

Nocioni palë e tretë është i një rëndësie të madhe për veprimtarinë e kontrolluesve, pasi përhapja e të dhënave personale tek palët e treta kërkon detyrime të shumta, të tilla si ekzistenca e një bazë të vlefshme ligjore ose detyrimi për të mbrojtur të dhënat kundër aksesit nga një palë e tretë për të cilën nuk ekziston një bazë e tillë ligjore. Duhet të theksohet se nuk është vetë kontrolluesi, por personat e autorizuar prej tij për përpunimin e të dhënave ose përpunuesi që do të trajtohet si palë e tretë.

Shembull:

Marrëdhënia e punësimit krijon një lidhje juridike ndërmjet punëdhënësit dhe punëmarrësit. Me përjashtim të punëdhënësit kur vepron si kontrollues i të dhënave dhe personave të tjerë të autorizuar të kontrollojnë të dhënat gjatë punësimit (punonjës, pra subjekte të të dhënave; autoritet publik, etj.), të gjithë pjesëmarrësit e tjerë (për shembull Posta Shqiptare, agjencia e telekomunikacionit, etj.) mund të trajtohen si palë të treta sipas ligjit Nr. 9887.

Marrës:

“Marrës” është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër të cilit i janë dhënë të dhënat e një palë të tretë ose jo. Autoritetet, të cilat mund të marrin të dhëna në kuadrin e një hetimi të veçantë, nuk konsiderohen si marrës.

Për të siguruar që subjektet e të dhënave të kenë mundësi të kontrollojnë të dhënat e tyre personale, kontrolluesi duhet t’i informojë në lidhje me marrësit e të dhënave që ai përpunon.

Marrësi është çdo subjekt të cilit i përhapen të dhënat personale. Marrësi nuk është një subjekt që përpunon të dhënat personale për qëllime inspektimi, mbikëqyrje dhe rregullimi për ushtrimin e autoritetit publik.

Pëlqim i subjekteve të të dhënave:

“Pëlqim i subjekteve të të dhënave” është çdo deklaratë me shkrim, e dhënë shprehimisht me vullnet të plotë e të lirë dhe duke qenë në dijeni të plotë për arsyen pse të dhënat do të përpunohen, çka nënkupton që subjekti i të dhënave pranon që të përpunohen të dhënat e tij.

Kjo do të thotë çdo shprehje specifike e vullnetit të dhënë lirisht dhe në dijeni të plotë nga ana e subjektit të të dhënave mes të së cilës ai shpreh pranimin e tij të padyshimtë për përpunimin e të dhënave personale. Pëlqimi për të përdorur të dhënat sensitive mund të revokohet në çdo kohë.

Ligji Nr. 9887, megjithëse nuk parashikon që pëlqimi të jetë në formë të shkruar, kërkon në mënyrë të nënkuptuar që pëlqimi të jetë i verifikueshëm përgjatë gjithë kohëzgjatjes së përpunimit të të dhënave.

Shembull i pëlqimit të subjektit:

Unë, “AA”, jap këtu pëlqimin tim për përpunimin e të dhënave të mia personale në lidhje me emrin, mbiemrin, adresën, arsimin, punësimin dhe përvojën profesionale. Qëllimi i këtij përpunimi do të jetë ekskluzivisht për kërkime shkencore. Kontrolluesi “XYZ” mund të përhapë apo të vërë në dispozicion tek palë të treta të dhënat e mia personale, me kusht që kjo

gjë të jetë absolutisht e nevojshme për interesa ligjore. Kontrolluesi është i detyruar të shkatërrojë të dhënat e mia personale me përfundimin e kësaj periudhe një vjeçare.

Përkufizime të tjera

Kontratë përpunimi

Kontrata sipas së cilës kontrolluesi detyron përpunuesin të kryejë në emër të tij një pjesë të përpunimit të të dhënave personale, me qëllim reduktimin e kostos së përpunimit.

Përpunues

Çdo shoqëri e tretë që lidh një marrëdhënie kontraktore me kontrolluesin me qëllim përpunimin e të dhëna personale me kosto më të ulët në emër të kontrolluesit.

Shkelje e të dhënave

Shkelje e sigurisë së të dhënave që shkakton shkatërrimin, humbjen, ndryshimin, përhapjen e paautorizuar apo ndryshimin e të dhënave personale të transmetuara, të ruajtura apo të përpunuara.

Ligji Nr. 9887, i ndryshuar është pasuruar me përkufizime të tjera. Përkatësisht ato janë si vijon: e dhënë biometrike, e dhënë gjyqësore, e dhënë anonime, mjete përpunimi, instrumente elektronike, marketing i drejtpërdrejtë, i ngarkuar, person përgjegjës, palë e tretë, mbikëqyrje, monitorimi i të dhënave personale, komunikim, përhapje, bllokim, vendimmarrje automatike, qëllime historike, qëllime statistikore, qëllime shkencore. Gjithsesi, këto përkufizime nuk janë të një rëndësie të madhe nga pikëpamja e zbatimit të Ligjit Nr. 9887.





III. LEGJITIMIMI I PËRPUNIMIT TË TË DHËNAVE PERSONALE

Çdo operacion përpunimi i të dhënave duhet të mbështetet në një bazë të vlefshme ligjore. Me “bazë ligjore” nënkuptojmë një autorizim për përpunuar të dhënat personale brenda një fushe të caktuar. Për shembull, pëlqimi apo një detyrim që rrjedh nga ligji janë shembuj të këtyre bazave ligjore. Përpunimi i të dhënave nuk mund të bëhet pa u mbështetur në një bazë të përshtatshme ligjore.

Si bazë kryesore ligjore është pëlqimi i subjektit të të dhënave. Ligji Nr. 9887 parashikon një sërë kërkesash që duhet të plotësohen për marrjen e pëlqimit. Është e rëndësishme që kjo të kihet parasysh pasi pëlqimi ndonjëherë keqpërdoret si mjet që shkel instrumente të tjera të mbrojtjes së të dhënave personale.

Pëlqimi duhet të shprehet qartë. Nëse subjekti i të dhënave jep pëlqimin e tij një kontrolluesi, pëlqimi mund të interpretohet si një propozim për të lidhur një kontratë të caktuar ose mund të përfshihet në një marrëveshje më komplekse. Pëlqimi kurrsesi nuk duhet të kuptohet si një akt i njëanshëm i izoluar.

Gjithsesi, dhe pa një pëlqim të tillë, kontrolluesi mund të përpunojë të dhëna (shiko Nenin 6 të Ligjit Nr. 9887):

-  nëse kryen një përpunim i cili është thelbësor për përmbyshjen e një detyrimi ligjor të kontrolluesit;
-  nëse përpunimi është thelbësor për përmbyshjen e një kontrate në të cilën subjekti i të dhënave është palë ose për të hyrë në negociata që synojnë lidhjen apo ndryshimin e një kontratë me kërkesë të subjektit të të dhënave;
-  nëse është i domosdoshëm për mbrojtjen e interesave të rëndësishëm jetikë të një subjekti të të dhënave;
-  nëse është i domosdoshëm për mbrojtjen e të drejtave dhe interesave legjitime të kontrolluesit, marrësit apo çdo personi tjetër të interesuar. Megjithatë, ky përpunimin i të dhënave

personale nuk mund të jetë në kundërshtim të dukshëm me të drejtën e subjektit të të dhënave për mbrojtjen e jetës private dhe personale;



me qëllim ofrimin e mundësive për biznes ose shërbime ndaj subjektit të të dhënave (marketing i drejtpërdrejtë) - shiko më poshtë.

Si rregull, përpunimi i të dhënave sensitive është e ndaluar. Megjithatë, në disa raste kontrolluesit lejohen të përdorin të dhëna të tilla, në qoftë se ata mund të provojnë se kanë të bëjnë me një rast përjashtimor, të përcaktuar kështu sipas nenit 7 të Ligjit Nr. 9887.

Këto baza ligjore janë të ndashme. Për të shqyrtuar nëse përdorimi i të dhënave është legjitim, mjafton të përmbushet një prej tyre, dhe jo të gjithë së bashku. Prandaj, në qoftë se të drejtat dhe detyrat që rrjedhin nga një dispozitë ligjore nuk mund të ushtrohen pa përdorimin e të dhënave, atëherë nuk kërkohet marrja e pëlqimit shtesë për përdorimin e tyre. Dhe as nuk është e nevojshme të justifikohet se përpunimi kryhet në interes të publikut ose për qëllime të interesave legjitime të ushtruara nga kontrolluesit. Pëlqimi për përdorimin e të dhënave për ushtrimin e një norme ligjore është i paqartë, sepse sugjeron se ai mund të tërhiqet ose të refuzohet nëse transferimi i të dhënave është i nevojshëm për qëllime të interesave legjitime.

Shembull:

Një punëdhënës është i autorizuar me ligj të përpunojë të dhënat me një akt i cili përcakton në veçanti qëllimin e të dhënave, dhe mund të kontrollojë të dhënat vetëm në lidhje me këtë qëllim (dmth., të dhënat në lidhje me sigurimet shoqërore, tatimet, detyrimi për të paguar kontributet përkatëse, etj.). Pëlqimi për përdorimin e këtyre të dhënave për të ushtruar një normë ligjore është i paqartë.

Mbani mend:





- *Gjithmonë, përpara se të filloni përpunimin e të dhënave, sigurohuni që përmbushni të paktën një bazat ligjore të përcaktuara në nenet 6 dhe 7 të Ligjit 9887.*
- *Nëse është e nevojshme, kontrolluesi duhet të hartojë dispozitat e pëlqimit në mënyrë të qartë dhe t'i ndajë ato nga deklarata të tjera shprehjes së vullnetit të bëra nga subjektet e të dhënave.*
- *Mbledhja e të dhënave sensitive, si rregull, është e ndaluar. Megjithatë, në qoftë se këto të dhëna janë të nevojshme për tu mbledhur, kjo mund të bëhet me kusht që ose subjekti i të dhënave të japë shprehimisht në mënyrë të qartë pëlqimin e tij, ose të përmbushet një nga bazat e tjera ligjore (Neni 7 i Ligjit 9887).*

IV. CILËSIA E TË DHËNAVE

Parimet e mëposhtme garantojnë cilësinë e të dhënave:




4.1 Parimi i përdorimit përfundimtar.

Ky parim, i quajtur edhe **parimi i kufizimit të qëllimit** (neni 5 paragrafi 1, shkronja b) e ligjit Nr. 9887) do të thotë se të dhënat do të mblidhen për qëllime specifike, të përcaktuara qartë, e legjitime dhe të mos përpunohen më tej nëse përpunimi nuk është në përputhje me këto qëllime. Kjo nënkupton se:

-  pala që mbledh të dhënat nuk mund as të harrojë dhe as të fshehë këtë qëllim;
-  qëllimi i përpunimit të të dhënave duhet të përcaktohet në mënyrë të qartë;
-  qëllimi do t'i komunikohet personit të interesuar përpara mbledhjes së të dhënave personale;
-  lidhja e një kontrate me kusht dhënien e pëlqimit për përpunimin e të dhënave për qëllime krejtësisht të ndryshme (p.sh. marketingu i produkteve dhe shërbimeve të palëve të treta) është e ndaluar.

4.2 Parimi i saktësisë së të dhënave

Kontrolluesi është i detyruar të sigurojë që të dhënat të jenë të sakta, të plota dhe të përditësuara në lidhje me qëllimet për të cilat janë përpunuar (neni 5 paragrafi 1, shkronja ç) e ligjit Nr. 9887). Për këtë qëllim, gjatë përpunimit të të dhënave kontrolluesi do të:

-  të vlerësojë, kurdoherë, besueshmërinë e burimit të të dhënave,
-  do të zhvillojë një mënyrë për verifikimin e saktësisë së të dhënave (në varësi të faktit nëse të dhënat janë sensitive apo jo) dhe për të krijuar një kod sjellje në rast se të dhënat konstatohen si të pasakta,
-  të informojë marrësit e tjerë tek të cilët ka përhapur të dhëna për çdo përditësim apo korrigjim të tyre.

Mbledhja e të dhënave nga burime me origjinë të panjohur, që nuk garantojnë saktësinë e tyre do të konsiderohet si shkelje e këtij parimi. Përpunimi i të dhënave të pasakta, jo të plota ose që nuk janë të përditësuara shpesh nuk mund të kryhet për shkak të arsyeve teknike (p.sh. ndërtimi i aplikacioneve TI që përdoren për përpunimin e të dhënave personale).

4.3 Parimi i proporcionalitetit/parimi i përshtatshmërisë së të dhënave.

Në përputhje me parimin e përshtatshmërisë, të dhënat duhet të jenë të përshtatshme dhe të mos tejkalojnë qëllimin për të cilin janë përpunuar (Neni 5 paragrafi 1, shkronja c) e Ligjit Nr. 9887). Kontrolluesi duhet të përpunojë vetëm ato të dhëna, lloji dhe përmbajtja e të cilave janë të nevojshme për qëllimet e mbledhjes së të dhënave. Përshtatshmëria e të dhënave duhet të vlerësohet, të paktën, në momentin e mbledhjes së tyre. Kështu, kontrolluesi është i detyruar të verifikojë këtë gjë. Ndonjëherë, ligjvënësi shprehimisht vë theksin në dispozitat përkatëse ligjore për përshtatshmërinë e të dhënave me qëllimet e përpunimit.




4.4 Parimi i kufizimit të kohës

Kontrolluesi, me ligj kërkohet që të ruajë të dhënat në formën që lejon identifikimin e subjekteve të të dhënave për aq kohë sa është e nevojshme për të përmbushur qëllimin për të cilin ato janë përpunuar (neni 5 paragrafi 1, shkronja d) e ligjit Nr. 9887). Pas arritjes së këtij qëllimi (p.sh. realizimi i një kontrate, afati për ruajtjen e të dhënave tregohet në dispozitat ligjore) të dhënat duhet të fshihen, të bëhen anonime ose të transferohen tek subjekt i autorizuar me ligj për të marrë këto të dhëna nga kontrolluesi (p.sh. arkivi i shtetit).






Shembull:

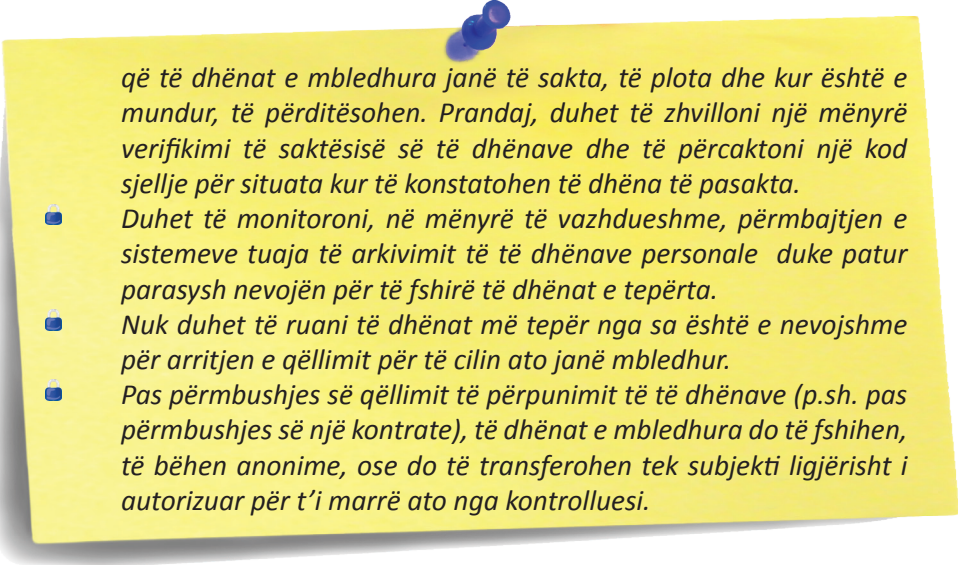
Kontrolluesi “XYZ” është i autorizuar me ligj të përpunojë të dhëna personale në lidhje me emrin, mbiemrin, adresën, arsimin, punësimin dhe eksperiencën profesionale për një periudhë një vjeçare. Sipas ligjit përkatës, qëllimi i këtij përpunimi do të jetë ekskluzivisht vetëm për kujdesin social (politika e punësimit)

Në këtë rast:

-  Kontrolluesi “XYZ” nuk duhet kurrsesi të përpunojë të dhëna të tjera personale (për shembull në lidhje me shtetësinë, të ardhurat, etj.)
-  Kontrollues “XYZ” është i detyruar të shkatërrojë të dhënat personale pas mbarimit të periudhës një vjeçare.
-  Kontrolluesi i të dhënave “XYZ” nuk duhet të përhapë të dhënat personale apo t’i vendosë ato në dispozicion palëve të treta për qëllime të tjera (si për shembull për qëllime të marketingut të drejtpërdrejtë).

Mbani mend:

-  Përpunimi fillon me mbledhjen e të dhënave. Mbledhja e të dhënave është një operacion përpunimi.
-  Duhet të mblidhni vetëm ato të dhëna që lidhen ngushtë me qëllimin e aktivitetit tuaj.
-  Nuk mund të mblidhni të dhëna “thjesht për t’i patur” për tu përdorur në të ardhmen. Grumbullim i të dhënave nuk është i lejuar.
-  Lidhja e një kontrate me kusht dhënien e pëlqimit për përpunimin e të dhënave për qëllime të tjera (p.sh. marketing i produkteve dhe shërbimeve të palëve të treta) është e ndaluar.
-  Nuk mund të përdorni të dhënat personale të mbledhura nga burimet me origjinë të panjohur apo të pabesueshme, të cilat nuk garantojnë saktësinë e të dhënave. Gjithmonë duhet të siguroheni



që të dhënat e mbledhura janë të sakta, të plota dhe kur është e mundur, të përditësohen. Prandaj, duhet të zhvilloni një mënyrë verifikimi të saktësisë së të dhënave dhe të përcaktoni një kod sjellje për situata kur të konstatohen të dhëna të pasakta.

- Duhet të monitoroni, në mënyrë të vazhdueshme, përmbajtjen e sistemeve tuaja të arkivimit të të dhënave personale duke patur parasysh nevojën për të fshirë të dhënat e tepërta.
- Nuk duhet të ruani të dhënat më tepër nga sa është e nevojshme për arritjen e qëllimit për të cilin ato janë mbledhur.
- Pas përmbushjes së qëllimit të përpunimit të të dhënave (p.sh. pas përmbushjes së një kontrate), të dhënat e mbledhura do të fshihen, të bëhen anonime, ose do të transferohen tek subjekti ligjërisht i autorizuar për t'i marrë ato nga kontrolluesi.



V. E DREJTA E SUBJEKTIT TË TË DHËNAVE PËR T'U INFORMUAR, PËR TË MARRË AKSES NË TË DHËNAT DHE TË DREJTA TË TJERA.



Përpara mbledhjes së të dhënave, kontrolluesi duhet t'i ofrojë subjektit të të dhënave informacion specifik, qëllimi i të cilin varet nëse të dhënat janë mbledhur në mënyrë të drejtpërdrejtë nga vetë subjekti i të dhënave apo nga burime të tjera (neni 18 i ligjit Nr. 9887).

Gjatë mbledhjes së të dhënave personale, kontrolluesi është i detyruar të informojë subjektin e të dhënave në lidhje me objektin dhe qëllimin për të cilin duhet të përpunohen të dhënat personale, kush do t'i përpunojë të dhënat personale dhe në çfarë mënyre, si dhe të dhënat personale të kujt do të përpunohen, përveç kur subjekti i të dhënave është tashmë në dijeni të këtij informacioni (për shembull kur dispozitat e pëlqimit të subjektit të të dhënave përmbajnë këtë informacion). Kontrolluesi duhet të informojë subjektin e të dhënave në lidhje me të drejtën e tij për akses dhe të drejtën për të korrigjuar të dhënat personale.




Në rast se kontrolluesi përpunon të dhëna personale të marra nga një subjekt i të dhënave, ai është i detyruar të udhëzojë subjektin e të dhënave nëse dhënia e të dhënave personale është e detyrueshme apo fakultative. Nëse subjekti i të dhënave, në bazë të një akti ligjor ose nënligjor, është i detyruar të japë të dhënat personale për përpunim, kontrolluesi duhet ta udhëzojë atë në lidhje me këtë fakt, si dhe për pasojat në rast refuzimi për të dhënë të dhënat personale.

Kontrolluesi është i detyruar të japë informacion dhe udhëzime në rastet kur të dhënat personale nuk janë marrë nga subjekti i të dhënave, nëse:

-  ai përpunon të dhëna personale ekskluzivisht për qëllime historike, statistikore dhe për kërkime shkencore dhe nëse dhënia e këtij informacioni është e pamundur, ose kërkon përpjekje joproportionale;
-  ai detyrohet të kryejë përpunimin e të dhënave personale në bazë

-  të një ligji të veçantë ose kur këto të dhëna janë të nevojshme për të ushtruar të drejtat dhe detyrimet që rrjedhin nga ligji i veçantë; ai përpunon të dhëna personale të bëra publike në mënyrë të ligjshme; ose
-  ai përpunon të dhëna personale, të marra me pëlqimin e subjektivit të të dhënave.

Gjatë përpunimit të të dhënave personale sipas Nenit 6, paragrafi 1, shkronja dh) dhe nenit 7 paragrafi 2, shkronja ç) e Ligjit Nr. 9887, për ushtrimin apo mbrojtjen e të drejtave ligjore, kontrolluesi është i detyruar të informojë menjëherë subjektin e të dhënave për përpunimin e të dhënave të tij personale. Qysh nga fillimi i përpunimit të të dhënave, çdo subjekt i të dhënave ka të drejtë, që me anë të një kërkesë me shkrim, të marrë nga kontrolluesi, pa pagesë sa mëposhtë:

-  konfirmim nëse të dhënat personale në lidhje me të po përpunohen ose jo dhe të paktën, informacion në lidhje me qëllimin e përpunimit, kategoritë e të dhënave të përpunuara dhe marrësit e kategoritë e marrësve, të cilëve u përhapen të dhënat personale;
-  t'i komunikohen në një formë të kuptueshme të dhënat që i janë nënshtruar një operacioni përpunimi si dhe çdo informacion të disponueshëm për burimin e tyre;
-  në rast vendimmarrje automatike, të marrë informacion për logjikën e zbatuar në marrjen e vendimit.

Megjithatë, e drejta për akses nuk mund të ushtrohet në rastet e sipërpërmendura, me përjashtim të situatave të veçanta, të parashikuara në nenin 12 paragrafi 4 dhe 5 i Ligjit Nr. 9887. Për më tepër, subjekti i të dhënave mund të kërkojë, sipas rastit, korrigjimin, fshirjen ose bllokimin e të dhënave përpunimi i të cilave nuk është në përputhje me dispozitat për mbrojtjen e të dhënave personale, në veçanti për shkak të natyrës jo të plotë ose të pasaktë të të dhënave (neni 13 i Ligji Nr. 9887).

Mbani mend:

- *Duhet të informoni në mënyrë të drejtpërdrejtë subjektin e të dhënave për faktin që do të mblidhni të dhënat e tij përpara se të filloni mbledhjen e të dhënave të tij personale. Nëse personi në fjalë nuk ka mundësi të vihet në dijeni në mënyrë të drejtpërdrejtë me përmbajtjen e këtij dokumentacioni, informacioni duhet të jepet në mënyrë individuale dhe nuk mund të bëhet në asnjë formë tjetër, p.sh. me njoftim ose një shënim.*
- *Nuk ka asnjë kufizim për formën e dhënies së informacionit subjektivit të të dhënave në lidhje me fillimin e mbledhjes së të dhënave (duhet të informohet vetë personi, me shkrim, me telefon, etj), megjithëse rekomandohet të përdoren mënyra formale (p.sh. me shkrim). Duhet të mbahet mend se në rast mosmarrëveshjes të mundshme në lidhje me përmbushjen e detyrimit të informimit, kontrolluesi është i detyruar të sigurojë dëshmi për të vërtetuar përmbushjen e këtij detyrimi*
- *Gjithmonë duhet që informacionin e mbledhur ta vini në dispozicion të subjektivit të të dhënave. Subjekti i të dhënave ka të drejtë të marrë akses në informacion, për të korigjuar ose fshirë të dhënat, apo për të kërkuar ndalimin e përpunimit të mëtejshëm të të dhënave.*

VI. DETYRIMI PËR TË NJOFTUAR

Kontrolluesit janë të detyruar të njoftojnë Komisionerin për përpunimin e synuar të dhënave personale përpara fillimit të procesit. Gjithashtu, ata duhet të njoftojnë Komisionerin kur ndryshojnë kushtet ose qëllimet e një përpunimi të të dhënave personale tashmë në proces. Njoftimi kryhet me anë të një procedure formale në përputhje me Kapitullin VI të Ligjit Nr. 9887.

Jo çdo operacion përpunimi është objekt i detyrimit për të njoftuar. Përjashtimet përcaktohen në Nenin 21 të Ligjit Nr. 9887 dhe aktet nënligjore. Kështu, çdo kontrollues i të dhënave duhet të kontrollojë nëse përpunimi i të dhënave personale që ai kryen është i përjashtuar nga detyrimi për të njoftuar në përputhje me këto dispozita.

Njoftimi duhet të përmbajë sa më poshtë:

- a) emrin dhe adresën e kontrolluesit;
- b) qëllimin e përpunimit të të dhënave personale;
- c) kategoritë e subjekteve të të dhënave dhe kategoritë e të dhënave personale;
- ç) marrësit dhe kategoritë e marrësve të të dhënave personale;
- d) propozimin për transferimet ndërkombëtare që kontrolluesi synon të kryejë;
- dh) një përshkrim të përgjithshëm të masave për sigurinë e të dhënave personale.

Komisioneri shqyrton të gjitha njoftimet dhe kur njoftimi nuk është i mjaftueshëm, ai urdhëron kontrolluesin të plotësojë përmbajtjen e njoftimit, duke përcaktuar edhe një afat kohor. Nëse kontrolluesi nuk plotëson përmbajtjen e njoftimit brenda afatit të përcaktuar, njoftimi konsiderohet i pakryer.

Komisioneri përdor njoftimet për mbajtjen e një regjistri të operacioneve të përpunimit. Ky regjistër është i arritshëm për publikun në faqen në internet të Komisionerit (me përjashtim të informacionit të parashkuar

në shkronjën dh) më sipër, i cili nuk është për t'u botuar).

Njoftimi dhe regjistrimi janë pa pagesë.

Mbani mend:

- Detyrimi për të njoftuar/regjistruar është një nga detyrimet themelore të kontrolluesit të të dhënave. Megjithatë, lutemi të mbani mend se regjistrimi nuk është detyrimi i vetëm i kontrolluesit.
- Mos-njoftimi i një sistemi arkivimi të të dhënave për qëllime regjistrimi, siç kërkohet nga ligji në fuqi, mund të çojë në përgjegjësi për shkeljen e ligjeve për mbrojtjen e të dhënave personale (Neni 40 paragrafi 1, shkronja d) e Ligjit 9887)
- Ndryshimi i informacionit që duhet të njoftohet duhet të njoftohet brenda afateve të duhura.
- Rekomandohet që njoftimi të kryhet online. Prandaj, ju duhet të vizitoni faqen në internet të Komisionerit (<http://www.kmpd.al>)

VII. TRANSFERIMI I TË DHËNAVE TEK SHTETE TË TRETA

Transferimi ndërkombëtar i të dhënave personale kryhet drejt shteteve marrëse që kanë nivel të mjaftueshëm të mbrojtjes së të dhënave personale (shiko Vendimin e Këshillit të Ministrave Nr. 934, datë 2 shtator 2009 “Për përcaktimin e shteteve me nivel të mjaftueshëm mbrojtje të të dhënave personale”).

Niveli i mbrojtjes së të dhënave personale për një shtet përcaktohet duke vlerësuar të gjitha rrethanat lidhur me përpunimin, natyrën, qëllimin dhe kohëzgjatjen e tij, shtetin e origjinës dhe destinacionin përfundimtar, aktet ligjore dhe standardet e sigurisë në fuqi në shtetin marrës.

Transferimi ndërkombëtar i të dhënave personale tek një shtet, që nuk ka nivel të mjaftueshëm të mbrojtjes së të dhënave personale mund të bëhet vetëm brenda kufijve të dispozitave të Nenit 8, paragrafi 2 i Ligjit Nr. 9887, ose me autorizim të Komisionerit.

Në kërkesën për autorizim, kontrolluesi duhet të garantojë respektimin e interesave të subjektit të të dhënave për masa mbrojtëse të përshtatshme në lidhje me mbrojtjen e privatësisë, të drejtave dhe lirive të subjektit të të dhënave jashtë Shqipërisë.

Kontrolluesit ose përpunuesit që operojnë në vendet e treta mund të garantojnë mbrojtje të përshtatshme në disa mënyra nga, ndër të tjera:

a) me anë të aplikimit të një sërë dispozitash të standardizuara të miratuara nga Komisioni Evropian që quhen “Dispozitat Kontraktore Standarde”.

Ato ofrojnë një bazë ligjore për transfertat nga Shqipëria në vende të treta. Këto dispozita ndahen në dy lloje kryesore: një grup parashikon transferim të të dhënave të kontrolluesit e regjistruar në një vend të tretë, ndërsa grupi tjetër rregullon transferimin tek përpunuesit.

b) me anë të aplikimit të dispozitave kontraktore ad hoc.

Përveç Dispozitive Kontraktore Standarde të Komisionit Evropian, kontrolluesit dhe përpunuesit në vendet e treta si dhe organizatat që transferojnë të dhëna mund të përcaktojnë kushtet e transferimit të të dhënave dhe të lidhin marrëveshje për këtë gjë. Marrëveshja duhet të sigurojë nivel të mjaftueshëm mbrojtje të të dhënave personale gjatë përpunimit të të dhënave nga kontrolluesi ose përpunuesi.




c) me anë të aplikimit të Rregullave të Detyrueshme të Korporatës (RRDK-të).

Rregullat e Detyrueshme të Korporatës janë zhvilluar dhe aplikohen nga shoqëritë shumëkombëshe për të rregulluar qarkullimin e të dhënave ndërmjet njësive të ndryshme të shoqërisë të vendosura në vende të ndryshme (gjithashtu edhe jashtë BE-së). RRDK-të lejojnë sipërmarrjet ndërkombëtare të rregullojnë shkëmbimin e të dhënave ndërmjet të njësive të tyre të shumta me një dokument të brendshëm të vetëm për mbrojtjen e të dhënave, në mënyrë që njësitë e prekura nga një shkëmbim të dhënash nuk kanë pse të lidhin marrëveshje me njësi të tjera të përfshira.

Shembull:

Një shtetas shqiptar, Z. A që jeton në Pragë dëshiron të blejë një makinë në Republikën Çeke dhe aplikon për kredi në një institucion financiar në Pragë. Institucioni financiar kërkon një raport të kredisë nga një agjenci raportimi të kredisë, ABC, në Shqipëri. Z. AAA ka dhënë pëlqimin e tij të shprehur qartë për këtë mbledhje, për përpunimin e të dhënave të tjera të duhura, si dhe për transferimin ndërkombëtar të të dhënave.

Duke qenë se:

-  Republika Çeke është një shtet anëtar i Bashkimit Evropian që ka nivel të mjaftueshëm të mbrojtjes së të dhënave personale;
-  subjekti i të dhënave, në përputhje me nenin 8 paragrafi b) i Ligjit 9887 ka dhënë pëlqimin për transferim ndërkombëtar;
-  transferimi ndërkombëtar i të dhënave është i ligjshme dhe agjencia raportuese e kredisë, ABC, përjashtohet nga kërkesa për autorizim.

Mbani mend:



- Transferimi i të dhënave në Shtete Anëtare të BE-së ose në vende të tjera të cilat janë anëtare të Zonës Ekonomike Evropiane trajtohet si transferim brenda vendit dhe nuk kërkon garanci shtesë.
- Transferimi i të dhënave në vende të treta imponon kërkesa shtesë (neni 8 paragrafi 2 i Ligjit 9887, i ndryshuar ose autorizim nga Komisioneri).
- Përpara se të transferoni të dhëna, ju duhet të kontrolloni me kujdes kushtet që duhet të plotësohen sipas ligjeve të vendeve të veçanta, p.sh. nëse kërkohet autorizim nga autoriteti për mbrojtjen e të dhënave.
- Të dhënat mund të transferohen në vende të treta vetëm për qëllime të përpunimeve, që lejohen ligjërisht në vendet të veçanta partnere.

VIII. SIGURIA E TË DHËNAVE PERSONALE: KONCEPTE BAZË, DETYRIME LIGJORE E REKOMANDIME.


Një nga detyrimet bazë të subjektit përpunues të të dhënave personale është siguria e të dhënave, pra të zbatojë masa të duhura teknike dhe organizative për mbrojtjen e të dhënave personale kundër shkatërrimit aksidental ose të paligjshëm ose humbjes aksidentale, ndryshimit, përhapjes apo aksesit të paautorizuar, veçanërisht kur përpunimi përfshin transmetimin e të dhënave në një rrjet; dhe kundër të gjitha formave të tjera të paligjshme të përpunimit. Masat e zbatuara duhet të jenë në proporcion me rrezikun dhe kategorinë e të dhënave dhe të pasqyrojnë nivelin e zhvillimit teknologjik të fushës. Garantimi i sigurisë së të dhënave është një proces i vazhdueshëm, i cili përfshin analizën e rrezikut dhe duhen marrë gjithashtu parasysh rrethanat e ndryshueshme që ndikojnë në nivelin dhe natyrën e rreziqeve ekzistuese.

Detyrimi për të siguruar të dhënat është i detyrueshëm për çdo subjekt përpunues të dhënave personale, pavarësisht nga rëndësia dhe/ose madhësia e tij.

Masat e marra të sigurisë duhet të reflektojnë nevojat reale të mjedisit të veçantë në të cilin përpunohen të dhënat. Siguria e të dhënave personale duhet të jetë pjesë përbërëse e sistemit të sigurisë së informacionit në subjektin përpunues të të dhënave. Për këtë arsye, termat përshkruese të sigurisë që rrjedhin nga standardet sigurisë së informacionit ISO-27.000 janë të zbatueshme. Këto terma kryesorë janë:

-  *konfidencialiteti, integriteti, disponueshmëria e të dhënave,*
-  *besueshmëria dhe pranimi (mos kundërshtimi) i aktivitetet e përpunimit (si ato manuale dhe ato të bazuara në IT)*

Këto terma kanë këto kuptime:

-  **Konfidencialiteti** – siguron që informacioni të mos vihet në dispozicion apo të mos përhapet tek persona të paautorizuar,

subjekte apo procese.



Integriteti – siguron që të dhënat të mos ndryshohen apo shkatërrohen në mënyrë të paautorizuar, pra ruan saktësinë dhe plotësinë e të dhënave dhe metodat e përpunimit.



Disponueshmëria – siguron që të dhënat të jenë në dispozicion dhe gati për t'u përdorur me kërkesë, brenda një kohe dhe në vendin e caktuar, të jenë në dispozicion të personave të autorizuar dhe të sistemeve të përpunimit kur kërkohet.



Besueshmëria e sistemeve TIK të aplikuar për përpunimin e të dhënave, si dhe e stafit që i vë ato në punë, duke garantuar që çdo aktivitet i tyre i aplikuar mbi të dhënat është i gjurmueshëm dhe i kontrollueshëm.



Mos kundërshtimi – të mos ketë mundësi për të mohuar përfshirjen e dikujt (të stafit apo sistemit të përpunimit të të dhënave), në përpunimin e të dhënave, në tërësi ose pjesërisht.

Subjektet përpunuese janë përgjegjëse për sigurinë e të dhënave personale për t'i mbrojtur ato kundër dëmtimit aksidental ose të paligjshëm apo shkatërrimit, humbjes aksidentale, ndryshimit, aksesit të paautorizuar dhe vënies në dispozicion, si dhe kundër çdo forme tjetër të paautorizuara përpunimi. Për këtë qëllim ata duhet të marrin masat teknike dhe organizative të përshtatshme për mënyrën e përpunimit, ndërkohë që duhet të marrin parasysh, mbi të gjitha:



mjetet teknike ekzistuese,



nivelin e rreziqeve të mundshme që mund të shkelin sigurinë apo funksionalitetin e sistemit të të dhënave personale

Kategoritë kryesore të personave përgjegjës për ruajtjen e sigurisë së të dhënave personale, janë:



Administratorët e Sistemeve të Teknologjisë së Informacionit dhe Komunikimit (më poshtë referuar “TIK”) dhe të sigurisë së tyre. Ky detyrim është i zbatueshëm kur subjekti i cili përpunon të dhëna personale ka një sistem TIK të brendshëm dhe/ose të jashtëm të instaluar për të përmbushur këto detyra.



Operatorët e të dhënave personale (të punësuarit, të kontraktuarit, etj), të cilët përpunojnë të dhëna personale me qëllim, përmbushjen

e detyrave të tyre kur punojnë për subjektin përpunues të të dhënave personale.



Të gjithë personat e caktuar nga subjekti përpunues për të përpunuar të dhënat në mënyrë manuale me anë të mjeteve jo-elektronike.

Mbani mend:

“Operatorët” nuk duhet të ngatërrohen me “përpunuesit”:

Operatori është një person fizik që kryen detyrën e përpunimit të të dhënave;

Përpunuesi është një subjekt juridik që vepron në emër të një kontrolluesi gjatë përpunimit të të dhënave.

Në rastin e një përpunuesi të përbërë nga 1 person i vetëm, ai mund të veprojë gjithashtu edhe si operator.

8.1 Detyrime të zakonshme për sigurinë e të dhënave për çdo subjekt juridik që përpunon të dhëna personale

Detyrimet bazë për sigurinë e të dhënave përcaktohen në Ligjin Nr. 9887. Këto detyrime janë cituar më poshtë (sipas renditjes në Ligj) dhe shoqërohen me shënime shpjeguese, vetëm për çështjet e sigurisë.

Transferimi Ndërkombëtar (Neni 8)

Para se të transferoni jashtë të dhënat personale kontrolloni nëse Komisioneri i ka miratuar shtetet e përfshira në transferim si vende me nivel të mjaftueshëm të sigurisë, përfshirë standardet e sigurisë në fuqi në shtetin pritës. Në nenin 9 përshkruhet në detaj procesi i marrjes së autorizimit nga Komisioneri.

Përgjegjësia për të njoftuar (Neni 22)

Përmbajtja e njoftimit: përcakton vetëm një detyrim të përgjithshëm mbi kontrolluesin për të informuar Komisionerin për masat e marra të sigurisë,

duke e njoftuar atë për sistemin e arkivimit të të dhënave personale, kjo i referohet **një përshkrimi të përgjithshëm të masave për sigurinë e të dhënave personale**. Detyrime më specifike përcaktohen në udhëzimet e Komisionerit të përshkruara më poshtë në këtë Udhëzues. Kjo qasje nuk është për të mbingarkuar ekonominë dhe sektorin publik me çështjet të kushtueshme dhe të komplikuar të sigurisë.

Masat për sigurinë e të dhënave personale (Neni 27)

Ky nen detyron kontrolluesin dhe përpunuesin të marrin masat e duhura organizative dhe teknike, për të mbrojtur të dhënat personale nga shkatërrime të paligjshme ose aksidentale, humbje aksidentale, nga aksesin ose përhapja tek persona të paautorizuar, veçanërisht kur përpunimi i të dhënave bëhet në rrjet, si dhe nga çdo formë tjetër përpunim të paligjshme.




Ai specifikon një grup masash të detyrueshëm të sigurisë që duhen marrë në mënyrë të dokumentuar. Kjo gjë bën të detyrueshme një ndarje të qartë të përgjegjësive për ruajtjen e sigurisë së informacionit, pa specifikuar saktësisht se çfarë masash organizative dhe teknike të sigurisë duhet të ndërmerren. Ai thekson rolin e autorizimit të duhur, si një kusht paraprak për të lejuar përpunimin e të dhënave personale, si dhe detyron subjektet përpunuese të të dhënave të dokumentojnë të gjitha ndryshimet e kryera mbi të dhënat që ata përpunojnë. Këto rregulla të përcaktuara në ligjin për mbrojtjen e të dhënave personale janë gjithëpërfshirëse dhe të vetë-shpjeguese, dhe duhet të ndiqen si nga subjektet e mëdha përpunuese edhe ato të vogla. Secili prej këtyre dy grupeve ka detyrime specifike të ndryshme për sigurinë, siç përcaktohen në Udhëzimet përkatëse të Komisionerit.

Konfidencialiteti i të dhënave (Neni 28)

Sipas kësaj dispozite, kanë detyrimin të ruajnë konfidencialitetin kontrolluesit, përpunuesit dhe Operatorët e tyre edhe pas ndërprerjes së funksioneve të tyre. Çdo operator nuk do të përpunojë të dhënat personale në të cilat ka akses pa autorizim paraprak, përveç nëse është e detyrueshme me ligj.

Përgjegjësitë (Neni 31)

Ky nen i jep Komisionerit detyra:

-  të nxjerrë udhëzues për masat e sigurisë në veprimtarinë e sektorëve të veçantë,
-  të mbikëqyrë ekzekutimin e sanksioneve për mos-pajtueshmëri,
-  të inkurajojë kontrolluesit të hartojnë kodet e tyre të etikës dhe t'i vlerësojë ato.

Mbani mend:

Subjektet përpunuese të të dhënave personale janë të detyruar të ndjekin jo vetëm ligjin për mbrojtjen e dhënave personale, por edhe udhëzimet specifike të Komisionerit. Ata gjithashtu nxiten të miratojnë kodet e praktikës së mirë specifike për sektorin si një element vetë-rregullimi.






Kundërvajtjet administrative (Neni 39)

Sipas këtij neni , kur nuk përbëjnë vepër penale, rastet e përpunimit të të dhënave në kundërshtim me dispozitat e Ligjit 9887 janë kundërvajtje administrative dhe janë objekt gjobe. Për sa i përket shkeljeve të sigurisë së të dhënave, kontrolluesit ose përpunuesit, që nuk marrin masat e sigurisë të të dhënave dhe nuk respektojnë detyrimin e konfidencialitetit, të parashikuar në Nenet 27 dhe 28 të ligjit për mbrojtjen e të dhënave, ndëshkohet me gjobë prej 10 000 lekë deri në 150 000 Lekë.

Përsa i përket shkeljeve të mësipërme, kur kundërvajtja është kryer nga persona juridikë, vendoset dyfishi i shumës së gjobës përkatëse. Me fjalë të tjera, në rast rrezikimi të sigurisë së të dhënave personale ligji parashikon gjoba si për kontrolluesit edhe për përpunuesit. Shuma e gjobës është në diskrecionin e Komisionerit.

8.2 Detyrimet kryesore që rrjedhin nga “Udhëzimi për detyrimet e kontrolluesve dhe përpunuesve përpara se të përpunojnë të dhëna personale”.

Ky Udhëzim detyron subjektet përpunuese të të dhënave:

-  Të marrin masa për sigurinë bazuar në analizën e riskut dhe zbutjen e tyre¹
-  Të marrin këto masa organizative në vendin e punës, në mënyrë që aksesit i operatorëve në të dhëna të kufizohet në minimumin e kërkuar për përmbushjen e detyrave të tyre siç duhet,
-  Duhet të ruhet integriteti dhe konfidencialiteti i të dhënave.
-  Të trajtojnë stafin e tyre të angazhuar me përpunimin e të dhënave për të qenë të aftë të kuptojnë çështjet e sigurisë dhe të respektojnë ligjin e përgjithshëm dhe të rregulloret e brendshme të miratuara².
-  Të ruajnë konfidencialitetin e të dhënave edhe pas përfundimit të funksionit (i cili ka lejuar aksesin)³.

Këto drejtime shumë të përgjithshme të sigurisë janë të zbatueshme si për subjektet e vogla dhe ato të mëdha përpunuese të të dhënave. Këto drejtime me të drejtë theksojnë rolin e mjeteve organizative, pasi janë të vështira dhe të shtrenjta për tu kompensuar me mjete teknike mangësi të tilla të sigurisë për shkak të organizimit të gabuar. Kërkesa për dhënie e aksesit minimale është absolutisht thelbësore, pasi është një mjet kryesor për zbutjen e rreziqeve të sigurisë.

Gjithashtu kërkon trajnimin e duhur të gjithë operatorëve. Nëse nuk zbatohet, kontrolluesit dhe përpunuesit nuk do të jenë në gjende të gjobisin punonjësit e tyre që veprojnë si operatorë të dhënave personale në rast shkelje të sigurisë, madje edhe në qoftë se ka qenë një akt neglizhence. Në rast paraqitje në gjykatë të një rasti, punonjësi, i cili ka të drejtë ligjore të trajnimit të duhur, do të fitojë rastin nëse kontrolluesi ose përpunuesi nuk e ka trajnuar atë siç duhet. Kjo e bën atë vendimtare për kontrolluesit dhe përpunuesit për të dokumentuar kryerjen e trajnimit.



¹ pika 1.1 e Udhëzimit nr. 2, datë 25.02.2010,

² pika 1.1 e Udhëzimit nr. 2, datë 25.02.2010,

³ pika 2 e Udhëzimit nr. 2, datë 25.02.2010,

8.3 Detyrime të ndryshme për sigurinë për subjektet e mëdha dhe ato të vogla, arsyet për diferencimin, çështjet kryesore.

Arsyet kryesore për të diferencuar subjektet përpunuese të të dhënave personale në bazë të përgjegjësive të tyre për sigurinë, janë:

-  Baraspeshimi i duhur ndërmjet mbrojtjes së të drejtave të subjektit të të dhënave, dhe vendosjes së një barre shtesë për kontrolluesin dhe përpunuesin, sipas rezultateve të analizës së riskut. Është e qartë se analiza e riskut ndihmon në identifikimin e klasës së subjekteve përpunuese ku të dhënat personale do të mbrohen duke përdorur një regjim më të formalizuar dhe të mirë pajisur.
-  Pozicionimi i mbrojtjes së të dhënave personale jo si pengesë për biznesit dhe si barrë administrative dhe financiare që paralizojnë ekonominë, por si një vlerë të shtuar për subjektin përpunues. Informacioni i përfshirë në të dhënat personale ka gjithmonë vlerë për subjektin (vlerësimi i tij minimal është kostoja e mbledhjes dhe përpunim të nevojshëm për ta bërë atë të disponueshëm), dhe duhet të mbrohet jo vetëm për të qenë në përputhje me detyrimet ligjore, por edhe për arsye të shëndosha ekonomike.

Vendosja e kësaj ndarje rezulton në transparencë më të madhe dhe realizëm ekonomik. Nëse i kërkojmë subjekteve të vogla të vendosin një sistem sigurie për informacionin tepër të ngarkuar (të cilin ata as nuk do ta kuptonin dhe as nuk do ta zbatonin plotësisht për arsye ekonomike) do të ishte një përjasje shumë e keqe, në kundërshtim me idenë e sigurisë së të dhënave personale. Nga ana tjetër, subjektet e mëdha duhet të plotësojnë kritere më të rrepta, pasi kjo është ekonomikisht e qëndrueshme dhe e nevojshme për të mbrojtur në mënyrë efikase informacionin e tyre të vlefshëm dhe njëkohësisht të drejtat e subjektit të të dhënave.



Për të mbuluar të gjitha fushat e përpunimit të të dhënave, si publike dhe private përdoret koncepti i subjektit përpunues, ai mbulon kontrolluesit dhe përpunuesit e të gjitha llojeve, përfshirë nën-përpunuesit.

Kjo ndarje ndërmjet subjekteve përpunuese të vogla dhe të mëdha është

hartuar si më poshtë:



Kontrollues ose përpunues të mëdhenj janë subjektet përpunuese të të dhënave personale, të cilët përpunojnë të dhëna personale dhe sensitive në mënyrë elektronike ose manuale duke shfrytëzuar 6 e më shumë persona për të kryer këtë përpunim, qoftë në mënyrë të drejtpërdrejtë ose me anë të përpunuesve;

Kontrollues ose përpunues të vegjël konsiderohen të gjithë subjektet përpunuese të të dhënave personale, të cilët:

-  Përpunojnë të dhëna personale në mënyrë elektronike ose manuale, duke angazhuar më pak se 6 persona për kryerjen e tij, qoftë në mënyrë të drejtpërdrejtë ose me anë të Përpunuesve;
-  Nuk përpunojnë të dhëna sensitive.

Kjo ndarje në thelb ndjek përfaqshen e Direktivës së BE-së për mbrojtjen e të dhënave. Ajo merr parasysh përvojën Evropiane si dhe madhësinë e Shqipërisë si vend. Çdo ndarje e tillë është e diskutueshme për ato subjekte që janë afër vijës ndarëse, dhe ky është një problem i përgjithshëm për të gjitha vendet që paraqesin një klasifikim të tillë. Duke qenë të vetëdijshëm për këtë dobësi të sistemit, asnjë nga këto vende nuk e ka braktisur këtë ndarje, dhe Rregullorja e re e BE-së për mbrojtjen e të dhënave personale e hartuar rishtazi përforcon këtë koncept. Diskutimi i vetëm që po vazhdon është si duhet përshtatur siç duhet kjo ndarje për të balancuar të drejtat e subjektit të të dhënave, sigurinë e ekonomisë, kostot dhe barrën administrative që bie mbi subjektet.

Pra, dallimet kryesore ndërmjet rregullave për subjektet e vogla dhe të mëdha janë:

-  Barra administrative dhe kostot që bien mbi subjektet e vogla janë më të pakta;
-  Subjektet e mëdha janë të detyruara të emërojnë një Person Kontakti (që pak a shumë reflekton realitetin bashkëkohor).

8.4 Rregulla shitesë për sigurinë kur delegohet përpunimi i të dhënave.

Vëmendje e veçantë i kushtohet delegimit të përpunimit (outsourcing) duke qenë se është kthyer në një praktikë të zakonshme në jetën ekonomike, e që përdoret për të marrë shërbime jo kryesore profesionale me një çmim të pranueshëm. Sa më shumë që delegohet përpunimi i të dhënave personale, rreziku i vërtetë është se siguria efektive bie në nivelin që dëmton të drejtat e subjekteve të të dhënave. Për të parandaluar një zhvillim të tillë në Shqipëri, Komisioneri miratoi një udhëzim të veçantë në lidhje me sigurinë e përpunimit të të dhënave në rast delegimi. Ai do të paraqitet dhe diskutohet në Kapitullin 5.

Mbani mend:

Mesazhi kryesor i tij është shumë i thjeshtë: nuk ka rëndësi se sa delegoni, ju (si një kontrollues ose përpunues):

- *Nuk mund të shmangeni nga detyrimet tuaja;*
- *Niveli i sigurisë që do të rezultojë nuk duhet të jetë më i ulët.*

Ky Udhëzim i Komisionerit merr parasysh gjithashtu realitetin bashkëkohor të përpunimit të të dhënave të tendencës në rritje të nën-përpunimit:





- 🔒 Zakonisht, sa më i madh dhe e profesional të jetë një përpunues, aq më shumë ai tenton të delegojë, p.sh. veprimtaritë përpunuese të të dhënave jo thelbësore të biznesit të tij.
- 🔒 Do të ishte jorealiste dhe ekonomikisht e dëmshme nëse do të ndaloheshin këto aktivitete.
- 🔒 Për këtë arsye, lejohet delegimi i përpunimit, me kusht që të gjitha palët e angazhuara (kontrolluesi dhe të gjitha palët e treta në një zinxhir delegimi) të plotësojnë disa kushte, të përcaktuara në këtë udhëzim.

IX. DETYRIMET KRYESORE QË RRJEDHIN NGA UDHËZIMI “PËR PËRCAKTIMIN E RREGULLAVE TË SIGURISË SË TË DHËNAVE PERSONALE TË PËRPUNUARA NGA KONTROLLUESIT E VEGJËL”



Subjektet përpunuese të vogla janë objekt i rregullave të kufizuara dhe gjithëpërfshirëse që duhen zbatuar. Dispozitat në lidhje me sigurinë e sistemeve TI janë të detyrueshme vetëm për ato subjekte që përpunojnë të dhënave personale në mënyrë elektronike. Subjektet që përpunojnë në mënyrë elektronike janë ato që përpunojnë të dhëna me anë të mjeteve elektronike. Për subjektet që përpunojnë të dhëna personale në mënyrë manuale zbatohen dispozitat e parashikuara në pikën 22 të kapitullit III të Udhëzimit nr. 21 datë 24.09.2012 “Për përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga Kontrolluesit e Mëdhenj”.

Personi i kontaktit nuk është i detyrueshëm për subjektet e vogla, por këshillohet që ato të autorizojnë me shkrim një person përgjegjës për mbikëqyrjen e sigurisë së të dhënave personale.

Udhëzimi përcakton standardet themelore për sigurinë e të dhënave personale ku përfshihen:

-  Analiza e riskut – që kryhet në mënyrë periodike, me qëllim identifikimin e rreziqeve kryesore ndaj të cilave sistemet janë të ekspozuara si dhe dokumentimin e tyre në mënyrë të kuptueshme për praktikën e veprimtarisë së subjekteve përpunuese;
-  Siguria fizike dhe e ambientit;
-  Siguria logjike e pajisjeve TIK të përpunimit të të dhënave personale;
-  Siguria e personelit.

Udhëzimi është hartuar në një mënyrë që dispozitat kryesore lehtësisht mund të kthehen në 2 lista:

-  Detyrat dhe aktivitetet e sigurisë që duhen kryer;
-  Lista e kontrollit për vlerësimin e pajtueshmërisë.

Ndryshe nga Udhëzimi për subjektet e mëdha, ky Udhëzim nuk kërkon zbatimin e një sistemi të plotë për Menaxhimin e Sigurisë së Informacionit (SMSI). Për pasojë këshillohet që të gjitha procedurat e sigurisë në një subjekt të vogël të hartohen në një gjuhë të thjeshtë, p.sh. duke iu referuar kushteve të veçanta të biznesit të subjektit. Një përjasje e tillë është e dobishme për t'i bërë këto procedura të thjeshta për tu zhvilluar, kuptuar dhe ekzekutuar. Një këshillë e mirë për personat që janë përgjegjës për t'i zhvilluar dhe mirëmbajtur ato është të kontrollojnë që gjatë trajnimit të kuptohen me të vërtetë nga operatorët.

Një grup i veçantë i masave të sigurisë fizike dhe mjedisore përcaktohen për subjektet që përpunojnë manualisht të dhëna personale. Ato kërkojnë kontroll të përshtatshëm të aksesit, si dhe shkatërrimin në afat ose bërjen anonime të të dhënave me përfundimin e kohës së mbajtjes.

Mënyrat dhe rrugët e transmetimit të të dhënave ose dokumentet që përmbajnë këto të dhëna duhet të kodohen. Gjithashtu, të gjitha mjetet portative elektronike që përdoren si bartës të informacionit (USB, mjete të tjera portative), duhet të kodohen përpara se të largohen nga ambientet e subjektit përpunues. Në rast përpunimi manual, të gjitha dokumentet shkresore të tepërta që shërbejnë si mbajtëse të të dhënave duhet të shkatërrohen.

X. DETYRIMET KRYESORE QË RRJEDHIN NGA “UDHËZIMI PËR PËRCAKTIMIN E RREGULLAVE TË SIGURISË SË TË DHËNAVE PERSONALE QË PËRPUNOHEN NGA SUBJEKTET E MËDHA”

Ndryshe nga subjektet e vogla, subjektet e mëdha janë të detyruara të ndjekin rregullat që rrjedhin nga standardet teknike të sigurisë së informacionit ISO-27000, pavarësisht se Udhëzimi nuk iu referohet këtyre standardeve në mënyrë të shprehur dhe as nuk e bën të detyrueshme pajtueshmërinë me to. Udhëzimi përcakton gjithashtu rregulla të veçanta për bashkëpunimin ndërmjet subjekteve të mëdha dhe Komisionerit gjatë inspektimeve.

Udhëzimi paraqet *Politikën e Sigurisë së Informacionit* (më poshtë referuar “PSI”) si dokumenti kryesor me anë të të cilit organizata që përpunon të dhënat personale i komunikon punonjësve të saj dhe kontraktorëve mënyrën e ndërtimit, zbatimit dhe operimit të Sistemit të Menaxhimit të Sigurisë së Informacionit (SMSI).




PSI-ja duhet të zhvillohet dhe zbatohet në përputhje me rregullat e sigurisë së informacionit, siç përcaktohen nga aktet ligjore vendase dhe legjislacioni ndërkombëtar i ratifikuar, që rekomandohen nga standardet e përcaktuara të sigurisë, si dhe rekomandimet e Komisionerit. Analiza e riskut është pjesë përbërëse e PSI-së. Dokumenti i PSI-së do të specifikojë qartë objektivat e sigurisë dhe do të përcaktojë masat teknike dhe organizative të nevojshme për zbutjen e kërcënimeve dhe rreziqeve që prekin sistemet e arkivimit.

Për sa i përket barrës administrative dhe kostove, Udhëzimi synon të vlerësojë investimet në siguri që mund të jenë kryer nga subjektet e mëdha. Kjo përjasje ka për qëllim të pranojë në një masë të madhe SMSI-të ekzistuese të implementuara tashmë për arsye të sigurisë së përgjithshme të informacionit. Gjithashtu nuk ka kërkesë për certifikatë të standardeve ISO 27-000, pavarësisht se është e këshillueshme. Këto

subjekte që kanë një SMSI paraqesin raportet e auditimit të SMSI-së së tyre para Komisionerit si provë e pranueshme për pajtueshmërinë me sigurinë e mbrojtjes së të dhënave, me kusht që rreziqet specifike për të dhënat personale të përfshihen në SMSI dhe të zbuten në mënyrë të përshtatshme.

Ashtu si Udhëzimi për subjektet e vogla, edhe ky Udhëzim specifikon dispozita për subjektet e mëdha në lidhje me sigurinë e sistemeve TIK të detyrueshme vetëm për ato që përpunojnë të dhëna personale në mënyrë elektronike. Për ato që përpunojnë të dhëna personale manualisht, zbatohen dispozitat e parashikuara në pikën 22 të kapitullit III të Udhëzimit. Për ta bërë transparent këtë proces, prova të tilla pranohen nga Komisioneri vetëm nëse auditimi i sigurisë së sistemit të arkivimit është kryer nga një person juridik ose fizik i pavarur dhe i paanshëm, profesionalisht i kualifikuar, i cili nuk ka marrë pjesë në zhvillimin, zbatimin dhe drejtimin e SMSI-së. Raporti i vlerësimit të sigurisë nuk duhet të jetë më i hershëm se dy vjet para kërkesës së Komisionerit për ta paraqitur atë.







Udhëzimi përshkruan në detaj se si duhet ***të hartohet dhe zbatohet SMSI-ja për mbrojtjen e të dhënave personale***. Ky sistem bazohet në identifikimin, analizimin dhe në zbutjen e rreziqeve ndaj sigurisë së të dhënave personale duke marrë parasysh dobësitë e:

-  sistemeve TIK të përdorur për përpunimin e të dhënave personale;
-  të gjitha formave jo-elektronike (manuale) të përpunimit të të dhënave personale;
-  sigurisë fizike, brenda dhe jashtë ambienteve, sigurisë së personelit dhe pajisjeve elektronike ose të lëvizshme.

Për të mos dobësuar sigurinë gjatë delegimit të përpunimit të të dhënave personale, kur Kontrolluesi përdor më shumë se një përpunues të madh, çdo përpunues duhet gjithashtu të ketë miratuar një SMSI. Kur përdor një përpunues të vogël, vetëm pjesët e zbatueshme të SMSI-së do t'i komunikohen këtij përpunuesi duke qenë ligjërish të detyrueshme në një kontratë për përpunimin e të dhënave.

SMSI-ja do të përcaktohet duke marrë parasysh: konfidencialitetin, integritetin, disoponueshmërinë, besueshmërinë e sistemeve TIK që janë përdorur për përpunimin e të dhënave dhe të personelit që i ka përdorur ato.

SMSI do të përfshijnë, në veçanti:

-  Analizën e Ndikimit në të Dhënat Personale (ANDHP), parë nga këndvështrimi i subjekteve të të dhënave, të dhënat e të cilëve janë përpunuar. Përpara përpunimit të të dhënave personale, kontrolluesi ose përpunuesi do të kryejë një vlerësim të ndikimit të operacioneve të përpunimit të parashikuara në mbrojtjen e të dhënave personale ku këto operacione përpunimi mund të paraqesin rreziqe të veçanta ndaj të drejtave dhe lirive të subjekteve të të dhënave për shkak të natyrës, shtrirjes ose qëllimit të tyre.
-  Politikën e Sigurisë së Informacionit, përfshirë sigurinë e përpunimit të të dhënave personale,
-  Analizën e sigurisë së sistemit të arkivimit të të dhënave personale,
-  Udhëzime të detajuara të sigurisë duke mbuluar fushat specifike,
-  Sigurinë fizike brenda dhe jashtë ambienteve,
-  Sigurinë e personelit dhe pajisjeve elektronike të lëvizshme ose jo.

Mbani mend:

Në rast se përpunimi i të dhënave do të kryhet me anë të platformës kompjuterike “cloud computing” ose me anë të përpunimit të lëvizshëm, do të zbatohen masa sigurie shtesë. Të gjitha pajisjet që janë përdorur si bartës të të dhënave do të kodohen.

Kontrolluesi dhe përpunuesi do të përcaktojnë hapa të qartë që do të ndërmerren në rast incidenti të shkeljes së sigurisë së të dhënave personale. Në varësi të rezultatit të analizës së riskut, do të propozohet zbutja e përshtatshme e rreziqeve në një nivel të pranueshëm. SMSI-ja duhet, gjithashtu, të përfshijë edhe marrëveshjet specifike për vazhdimësinë e veprimtarisë tregtare për hartimin e të cilave do të

zbatohen standardet teknike dhe rekomandimet e vëna në dispozicion për publikun.

Udhëzimi gjithashtu specifikon rregulla të rrepta për subjektet e mëdha që përpunojnë të dhëna personale manualisht (jo në mënyrë elektronike).

Një vëmendje e veçantë i kushtohet subjekteve që përpunojnë të dhëna personale sensitive si në mënyrë manuale ashtu edhe elektronike.

Personeli i subjektit përpunues duhet të trajnohet rregullisht për mbrojtjen e të dhënave personale, dhe përcaktohen programet e trajnimit.

Kontrolli i sigurisë së informacionit për të dhënat personale duhet të kryhet jo më pak se një herë në vit. Për sa i përket subjekteve përpunues që mbështeten plotësisht në përpunimin elektronik të të dhënave, për të minimizuar kostot, ky kontroll mund të jetë pjesë e kontrollit të përgjithshëm vjetor financiar, kur vlerësohet gjendja e veprimtarisë tregtare të subjektit.

Para se të lidhin një marrëveshje kontraktore që përmban përpunimin e të dhënave personale, kontrolluesi i të dhënave ka detyrimin të kontrollojë përpunuesin në fjalë për pajtueshmërinë e tij me ligjin për mbrojtjen e të dhënave personale

10.1 Roli i personit të kontaktit.

Çdo Kontrollues objekt i këtij udhëzimi do të autorizojë me shkrim të paktën një Person Kontakti, për mbikëqyrjen e brendshme të mbrojtjes së të dhënave personale. Subjekti duhet të njoftojë Komisionerin për autorizimin e vetëm një Person Kontakti, edhe në rast se ai mund të emërojë disa persona kontakti për mbikëqyrjen e brendshme të mbrojtjes së të dhënave personale. Nëse Subjekti zëvendëson personin e kontaktit, ai duhet të njoftojë Komisionerin në afatin e kërkuar.

Përpunuesi objekt i këtij udhëzimi duhet të emërojë të paktën një person kontakti, përgjegjës për garantimin e sigurisë së përshtatshme të të

dhënave personale, kur vepron në emër të Kontrolluesit.

Përpunuesi i vogël i kontraktuar nga subjekti përpunues objekt i këtij udhëzimi, gjithashtu këshillohet të emërojë një person kontakti.



Mbani mend:

Personi i kontaktit është i detyrueshëm për të gjithë përpunuesit e mëdhenj, dhe është i rekomandueshëm për përpunuesit e vegjël në rast se pajtohen nga një kontrollues i madh, ose përpunues i madh. Përpunuesi nuk ka detyrimin të njoftojë Komisionerin pasi emëron personin e kontaktit.

Personi i kontaktit duhet të jetë një person i besuar. Funkzioni i personit të kontaktit mund të kryhet nga një person fizik që gëzon zotësi të plota juridike dhe që përmbush kushtin e integritetit. Personi i kontaktit dorëzon vërtetimin e gjendjes gjyqësore të përditësuar, e cila mbahet nga kontrolluesi ose përpunuesi gjatë kryerjes së funksionit të tij.







Personi kontaktit duhet të kryejë në mënyrë të pavarur detyrat e tij, çdo detyrë tjetër si anëtar i bordit drejtues apo mbikëqyrës, apo drejtues i departamentit të një institucioni publik, është e papajtueshme me pozitën e personit të kontaktit. Personi i kontaktit gjithashtu duhet që ligjërisht të ketë një pozicion të atillë që e bën përfaqësues ligjor të subjektit në marrëdhëniet me të jashtmit, p.sh. kur duhet t’iu kapë përgjigje pyetjeve të Komisionerit. Ky përfaqësim është i kufizuar brenda fushës së detyrave të tij. Nenet 30-36 përcaktojnë fushën e veprimtarisë së detyrimeve të personit të kontaktit. Ato gjithashtu përcaktojnë rregullat e bashkëpunimit ndërmjet personit të kontaktit dhe Komisionerit.

Personi i kontaktit është përgjegjës për të kryerjen e analizës së përshtatshme të rreziqeve të mbrojtjes së të dhënave personale ndaj të drejtave dhe lirive të subjektit të të dhënave (Analiza e Ndikimit në të Dhënat Personale). Personi i kontaktit është përgjegjës për njoftimin e subjektit me shkrim në rastet kur konstaton se ka probabilitet të ndodhë

një shkelje e mundshme të drejtave të subjekteve të të dhënave. Kjo kryet për të kufizuar përhapjen e efekteve negative tek subjektet e të dhënave. Në rasti se njoftimi i tij nuk merret parasysh, ai është i detyruar të njoftojë Komisionerin. Kjo është për të disiplinuar reagimin e duhur dhe serioz ndaj njoftimeve të personit të kontaktit për shkelje të sigurisë.

Emërimi i personit të kontaktit duhet t'i njoftohet në çdo rast Komisionerit. Për të mos mbi-rregulluar, dhe për të mos bërë të pamundur gjetjen e një personi kontakti, deklarata e subjektit që personi i kontaktit është një person profesionist dhe etik është mëse e mjaftueshme. Gjithashtu kjo gjë nuk vendos kosto të rënda për sigurinë e të dhënave personale.

Personi i kontaktit ka këto detyra dhe përgjegjësi:

-  është përgjegjës për mbikëqyrjen e brendshme të përmbushjes së detyrimeve për mbrojtjen e të dhënave personale nga ana e Subjektit përpunues të të dhënave personale,
-  jep këshilla për personat përgjegjës,
-  është përgjegjës për zbatimin e masave teknike, organizative, të personelit, si dhe mbikëqyr zbatimin e tyre në praktikë. Në veçanti, ai do të sigurojë dokumentacionin e SMSI-së që provon hartimin dhe mirëmbajtjen e duhur të saj,
-  në rast kontraktimi të një përpunuesi nga ana e subjektit përpunues të të dhënave personale, Personi i Kontaktit është përgjegjës për mbikëqyrjen e brendshme të veprimtarisë së përpunuesit, për përmbajtjen dhe hartimin e kontratës me shkrim për Përpunuesin. Gjatë kohëzgjatjes së marrëdhënies kontraktore apo autorizimit, personi i kontaktit do të verifikojë respektimin e kushteve të miratuara, duke përfshirë edhe angazhimin dhe ndryshimin e Përpunuesve, në rast se ka.
-  është përgjegjës për mbikëqyrjen e brendshme të transferimeve ndërkombëtare të të dhënave personale,
-  është përgjegjës për dorëzimin e dokumentacionit të sistemeve të arkivimit për regjistrim të veçantë dhe shpalljen e ndryshimeve dhe çregjistrimin e sistemeve të arkivimit nga regjistri i veçantë. Ai mban të dhëna të sistemeve të arkivimit që nuk janë subjekt

regjistrimi dhe i vendos ato në dispozicion të kujtdo që ligjërisht ka të drejtë të ketë akses në to;



është përgjegjës për bashkëpunimin e nevojshëm me Komisionerin në përmbushjen e detyrave brenda përgjegjësiave të tij;



me kërkesën e Komisionerit, ai është i detyruar t'i paraqesë autorizimin me shkrim mbi bazën e të cilit ai vepron, si dhe dëshmi për shkallën e njohurive të fituara në trajnime profesionale.

Mbani mend:

Sfera e veprimtarisë së personit të kontaktit është vetë-shpjeguese. Është e rëndësishme që kompetencat e tij të vërteta të mos kufizohen për Subjektin vetëm në rast delegimi të përpunimit, në këtë rast personi kontaktit gjithashtu ndërhyr në marrëdhënien kontraktore me përpunuesin(it). Për pasojë, kontrata për përpunimin e të dhënave nga një shoqëri e tretë duhet të parashikojë përfshirjen e personit të kontaktit për të bërë këtë gjë të mundur dhe të parashikojë disa dispozita kontraktore, si p.sh. aftësinë praktike për të vlerësuar në vend sigurinë e përpunimit të të dhënave nga Përpunuesi, duke përfshirë akses të kushtëzuar në ambientet e tij, rrjetet TI, personelin, etj.

Subjekti përpunues i të dhënave personale është i detyruar t'ju ofrojë të gjithë personave të kontaktit të emëruar trajnim profesional. Komisioneri mund t'i kërkojë subjektit përpunues të paraqesë prova që trajnimi profesional realisht është zhvilluar. Kjo vendos një detyrim për të trajnuar personin e kontaktit dhe për t'i provuar Komisionerit që realisht trajnimi është kryer. Subjekti përpunues është i lirë të vendosë mënyrën e organizimit të trajnimit (axhendën, frekuencën, etj.).

Personi i kontaktit siguron mbajtjen e rregullt të një inventari të sistemeve të arkivimit të të dhënave personale të përpunuara nga Subjekti përpunues i të dhënave personale, përfshirë të dhënat personale të përjashtuara nga detyrimi për regjistrim në autoritetin e Komisionerit. Kjo vendos detyrimin për të mbajtur të përditësuar të gjithë dokumentacionin. Duke

qenë se një detyrë e tillë është mjaft punë, duhet të vlerësohet në bazë të ngarkesës së punës.

Meqenëse personi i kontaktit shërben këtu më tepër si audit se sa si një figurë ekzekutive, ai nuk është i detyruar të sigurojë dhe të mbajë personalisht këtë dokumentacion. Në një subjekt të madh, pjesa më e madhe e këtij dokumentacioni ekziston, mbahet dhe ruhet nga disa njësi të tjera organizative (p.sh., siguria, pajtueshmëria, TI-ja, ose disa departamente të biznesit), kështu që nuk ka arsye për ti publikuar ato.

Subjekti përpunues i të dhënave personale është i detyruar t'i mundësojë personit të kontaktit të zbatojë mbikëqyrjen e brendshme të mbrojtjes së të dhënave personale në mënyrë të pavarur dhe të pranojë propozimet e tij legjitime. Njoftimi i mangësive ose bërja e një kërkesë nga personi i kontaktit në lidhje me përmbushjen e detyrimeve të tij nuk duhet të bëhet nxitje apo arsye për kryerjen e një veprimi nga ana e subjektit, që mund të passjell dëme për personin e kontaktit.

Kjo specifikon mënyrën se si është interpretuar pavarësia e personit të kontaktit. Fakti që në shumicën e rasteve personi i kontaktit është punonjës i subjektit e bën atë potencialisht objekt të presioneve për ta bërë punën e tij një trillim. Për të parandaluar një situatë të tillë, janë formuluar garancitë konkrete për sigurinë e punës.

Komisioneri ka të drejtë të kërkojë ndryshimin e personit të kontaktit, në rast se ai që është aktualisht nuk ka përmbushur detyrat e tij. Është në diskrecionin e Komisionerit të gjykojë nëse ka mospërmbushje të detyrave. Kur kërkon një zëvendësim, Komisioneri nuk ka të drejtë të sugjerojë ndonjë person të caktuar për zëvendësim. Pas emërimit, personi i kontaktit i raporton Komisionerit të gjitha shkeljet e rënda të sigurisë së të dhënave personale. Është deri në gjykimin e tij të vendosë nëse një shkelje e caktuar është e rëndë apo jo. Një këshillë e mirë për të vendosur këtu është marrja në shqyrtim e masës së dëmit të mundshëm ndaj subjektit. Është në vendimin e subjektit nëse do të raportojë shkeljet me pasoja të vogla negative për subjektet e të dhënave, dhe me pasoja të mëdha negative për vetë subjektin (p.sh. dëmtim i reputacionit, humbja

e vlerës në rastin e një shoqërie ku pasuria më e madhe janë të dhënat dhe/ose shërbimet e përpunimit të të dhënave).

Mbani mend:





Personi i kontaktit është një figurë e rëndësishme për çdo rast inspektimi të Komisionerit. Nëse Komisioneri i beson personit të kontaktit, ai mund të thjeshtojë procedurat e inspektimeve duke i kërkuar personit të kontaktit të kryejë një pjesë të tyre. Kjo marrëveshje është e dobishme për të dyja palët, sidomos në rastin e marrëveshjeve komplekse të përpunimit të të dhënave ku çdo inspektimi në thellësi, pa bashkëpunimin e duhur të subjektit është praktikisht i pamundur.

XI. DETYRIMET KRYESORE QË RRJEDHIN NGA “UDHËZIMI PËR DELEGIMIN E TË DHËNAVE PERSONALE”.

Qëllimi i këtij udhëzimi është përcaktimi i rregullave në lidhje me marrëdhënien ndërmjet kontrolluesit dhe përpunuesit në rastet e delegimit të përpunimit të të dhënave, si dhe miratimi i një kontrate tip që palët duhet të përdorin në rast të këtij delegimi. Udhëzimi përfshin gjithashtu një Kontratë tip për delegimin e përpunimit të të dhënave personale tek shoqëri të treta.

Ky udhëzim zbatohet nga të gjitha shoqëritë, organizatat apo institucionet, të cilat për të përmbushur funksionet e tyre të ligjshme, hyjnë në marrëdhënie me shoqëri të treta dhe, në bazë të një kontrate, bien dakord që këto shoqëri të kryejnë përpunimin e të dhënave personale për llogari të tyre. Zbatimi i këtij udhëzimi ka për qëllim të sigurojë paprekshmërinë e të dhënave personale në çdo hallkë të këtij përpunimi.

Për të siguruar një përzgjedhje të mirë të përpunuesit, kontrolluesi duhet të shqyrtojë çështjet e mëposhtme të sigurisë:

-  Të përzgjedhë një shoqëri me emër të mirë në këtë fushë, e cila ofron garanci të qëndrueshme që sigurojnë të dhënat personale që do të përpunohen;
-  Kontrata me përpunuesin duhet të jetë në formë të shkruar dhe të përmbajë dispozita të veçanta që rregullojnë mbrojtjen e të dhënave personale;
-  Në rast se përpunuesi është shoqëri e huaj, kontrolluesi sigurohet se vendet ku përpunuesi vepron janë pjesë e vendeve që ofrojnë mbrojtje të mjaftueshme për të dhënat personale sipas legjislacionit shqiptar. Kontrolluesi duhet t'i referohet listës së vendeve që ofrojnë mbrojtje të mjaftueshme të miratuar me VKM. Nr. 934, datë 2.9.2009 “Për Përcaktimin e Shteteve me Nivel të Mjaftueshëm të Mbrojtjes së të Dhënave Personale”;
-  Kontrolluesi sigurohet që përpunuesi ofron masa të përshtatshme mbrojtëse për të dhënat që do të përpunohen. Për këtë qëllim

kontrolluesi mund t'i referohet standardeve të sigurisë ISO-27000.

Përpunuesi duhet t'i raportojë kontrolluesit çdo shkelje të sigurisë për të garantuar zbatimin e standardeve të përshtatshme të sigurisë dhe për të bërë rregullime pas çdo shkelje të mundshme të tyre, si dhe për të lejuar që kontrolluesi të vihet në dijeni dhe të ketë të gjithë informacionin përkatës në rast se duhet të inspektohet nga Komisioneri. Në rast nënkontraktimi të përpunimit, shoqëria e nënkontraktuar është e detyruar të njoftojë shoqërinë kontraktuese si dhe kontrolluesin.

Në rastet kur përpunuesi kryen përpunimin e të dhënave me anë të nënkontraktimit/nën-delegimit të përpunimit tek një shoqëri tjetër, shoqëria e nënkontraktuar është objekt i të njëjtave rregulla të përshtatshme të sigurisë. Çdo kontratë nënkontraktimi/nën-delegimi të përpunimit e të dhënave nga shoqëri të treta duhet të jetë në formë të shkruar dhe të ketë marrë miratimin paraprak të kontrollorit, pas një verifikimi paraprak nga ana kontrolluesit që shoqëria e nënkontraktuar ka të njëjtin nivel sigurie me shoqërinë e kontraktuar.

Kontrata për delegimin e përpunimit tek shoqëri të treta duhet të jetë në formë të shkruar. Palët e përfshira mund të zgjedhin opsionin për të lidhur një kontratë të veçantë për vendosjen e rregullave për mbrojtjen e të dhënave personale, ose t'i përfshijnë ato si pjesë të kontratës së biznesit tyre. Për qëllime të mbrojtjes së të dhënave personale, të dyja rastet janë të pranueshme, për sa kohë që ato të vendosin rregulla të qarta dhe sigurojnë mbrojtje të mjaftueshme të të dhënave personale dhe nivelin e sigurisë në përputhje me legjislacionin shqiptar.

Mbani mend:

Në çdo rast delegimi i përpunimit nuk mund të ketë një nivel sigurie më të ulët se ai i rënë dakord ndërmjet kontrolluesit dhe shoqërisë së kontraktuar.

LIGJ
Nr. 9887, datë 10.03.2008, ndryshuar me ligjin Nr. 48/2012

“PËR MBROJTJEN E TË DHËNAVE PERSONALE”

Në mbështetje të neneve 78 dhe 83 pika 1 të Kushtetutës, me propozimin e Këshillit të Ministrave,

KUVENDI I REPUBLIKËS SË SHQIPËRISË
VENDOSI:

KREU I
DISPOZITA TË PËRGJITHSHME

Neni 1
Objekti

Ky ligj ka për objekt përcaktimin e rregullave për mbrojtjen dhe përpunimin e ligjshëm të të dhënave personale.

Neni 2
Parim i përgjithshëm

Përpunimi i ligjshëm i të dhënave personale bëhet duke respektuar dhe garantuar të drejtat dhe liritë themelore të njeriut dhe, në veçanti, të drejtën e ruajtjes së jetës private.

Neni 3
Përkufizime

Në këtë ligj termat e mëposhtëm kanë këto kuptime:

1. “Të dhëna 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.
2. “E dhënë gjyqësore” është çdo e dhënë lidhur me vendimet në fushën e gjykimeve penale, civile, administrative apo me dokumentimet në regjistrat penalë, civilë, ato të dënimeve administrative etj.
3. “E dhënë anonime” është çdo e dhënë, që në origjinë ose gjatë përpunimit, nuk mund t’i shoqërohet një individ, të identifikuar ose të identifikueshëm.
4. “Të dhëna sensitive” është çdo informacion për personin fizik, që ka të bëjë me origjinën e tij, racore ose etnike, mendimet politike, anëtarësimin në sindikata, besimin, fetar apo filozofik, dënimin penal, si dhe të dhëna për shëndetin dhe jetën seksuale.
5. “Kontrollues” është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër që, vetëm apo së bashku me të tjerë, përcakton qëllimet dhe mënyrat e përpunimit të të dhënave personale, në përputhje me ligjet dhe aktet nënligjore të fushës, dhe përgjigjet për përmbushjen e detyrimeve të përcaktuara në këtë ligj.
6. “Subjekt i të dhënave personale” është çdo person fizik, të cilit i përpunohen të dhënat personale.
7. “Përpunues” është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër që përpunon të dhëna personale në emër të kontrolluesit.
8. “Sistem arkivimi” është çdo grup i strukturuar i të dhënave personale, të cilat janë të aksesueshme në bazë të kriterëve specifike, të centralizuara, të decentralizuara ose të shpërndara në një bazë, funksionale ose gjeografike.
9. “Mjete përpunimi” janë mjetet automatike, gjysmautomatike dhe mekanike që përpunojnë të dhëna personale.
10. “Instrumentet elektronike” janë kompjuteri, programet kompjuterike dhe çdo mjet, elektronik ose automatik, me të cilat bëhet përpunimi.
11. “Tregtim i drejtpërdrejtë” është komunikimi me çdo mjet dhe mënyrë i materialit reklamues, duke përdorur të dhënat personale të personave fizikë ose juridikë, të agjencive ose njësive të tjera, me ose pa

ndërmjetësim.

12. “Përpunim i të dhënave personale” është çdo veprim ose grup veprimesh, të cilat janë kryer mbi të dhënat personale, me mjete automatike ose jo, të tilla si mbledhja, regjistrimi, organizimi, ruajtja, përshtatja ose ndryshimi, rikthimi, konsultimi, shfrytëzimi, transmetimi, shpërndarja ose ndryshe duke vënë në dispozicion, shtrirja ose kombinimi, fotografimi, pasqyrimi, hedhja, plotësimi, seleksionimi, bllokimi, asgjësimi ose shkatërrimi, edhe në qoftë se nuk janë të regjistruara në një bankë të dhënash.

13. “Marrës” është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër të cilit i janë dhënë të dhënat e një palë të tretë ose jo. Autoritetet, të cilat mund të marrin të dhëna në kuadrin e një hetimi të veçantë, nuk konsiderohen si marrës.

14. “I ngarkuar” është personi që kryen përpunimin e të dhënave, me autorizim nga titullari ose personi përgjegjës.

15. “Palë e tretë” është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër, përveç subjektit të të dhënave, kontrolluesit, përpunuesit dhe personave, të cilët, nën autoritetin e drejtpërdrejtë të kontrolluesit apo përpunuesit, janë të autorizuar të përpunojnë të dhëna.

16. “Transmetim” është transferimi i të dhënave personale te marrësit.

17. “Mbikëqyrje” është ndjekja me kujdes e përpunimit të të dhënave personale nga të gjithë kontrolluesit dhe përpunuesit, nëpërmjet bashkëpunimit, kontrollit, hetimit administrativ dhe inspektimit, për parandalimin e shkeljeve dhe, kur ka vend, edhe vendosja e sanksioneve administrative për të siguruar zbatimin e urdhrave, të udhëzimeve dhe rekomandimeve të Komisionerit, duke respektuar të drejtat dhe liritë themelore të njeriut.

18. “Monitorim i të dhënave personale” është puna e vazhdueshme, gjithëpërfshirëse, efikase dhe e planifikuar e institucionit në këto drejtime: udhëheqje, drejtim, organizim, ndihmë, bashkëpunim, takime sensibilizimi e njohjeje, orientim, raportim në Kuvend, publikim, shpjegime të ndryshme, dhënie përgjigjeje të ankimeve, veprimtari, seminare e leksione, aktivitete, dokumentim, hartim rregullash, marrëveshje, kontrata, udhëzime, vendime, rekomandime, kontroll i zbatimit të gjobave, krijim e hapje e regjistrave, si dhe për çështje të tjera që lidhen me ushtrimin e rregullt të veprimtarisë.

19. “Komunikim” është komunikimi i të dhënave personale një ose më shumë subjekteve të caktuara, të ndryshme nga i interesuari, nga përfaqësuesi i titullarit në territorin e vendit, nga përgjegjësit dhe të ngarkuarit, në çdo formë, edhe përmes vënies në dispozicion ose për konsultime.
20. “Përhapje” është komunikimi i informacionit për të dhënat personale palëve të papërcaktuara, në çfarëdo forme, edhe përmes vënies në dispozicion ose konsultimit.
21. “Bllokim” është ruajtja e të dhënave personale duke pezulluar përkohësisht çdo veprim tjetër përpunimi.
22. “Transferim ndërkombëtar” është dhënia e të dhënave personale marrësve në shtetet e huaja.
23. “Vendimmarrje automatike” është një lloj vlerësimi për individët, i kryer krejtësisht në mënyrë automatike, pa ndërhyrjen e individit.
24. “Pëlqim i subjekteve të të dhënave” është çdo deklaratë me shkrim, e dhënë shprehimisht me vullnet të plotë e të lirë dhe duke qenë në dijeni të plotë për arsyen pse të dhënat do të përpunohen, çka nënkupton që subjekti i të dhënave pranon që të përpunohen të dhënat e tij.
25. “Qëllimi historik” është qëllimi për studime, hulumtime, kërkime dhe dokumentim të figurave, fakteve dhe rrethanave të së kaluarës.
26. “Qëllimi statistikor” është qëllimi për hulumtime statistikore, prodhim të të dhënave statistikore edhe nëpërmjet sistemit informativ statistikor.
27. “Qëllimi shkencor” është qëllimi për studime dhe hulumtime sistematike, që finalizon zhvillimin e dijeve shkencore në një sektor të caktuar.

Neni 4 **Fusha e zbatimit**

1. Ky ligj zbatohet për përpunimin e të dhënave personale, plotësisht ose pjesërisht, nëpërmjet mjeteve automatike, si dhe për përpunimin me mjete të tjera të të dhënave personale, që mbahen në një sistem arkivimi apo kanë për qëllim të formojnë pjesë të sistemit të arkivimit.
2. Ky ligj zbatohet për përpunimin e të dhënave personale nga:
 - a) kontrollues të vendosur në Republikën e Shqipërisë;

b) misionet diplomatike ose zyrat konsullore të shtetit shqiptar;
c) kontrollues, të cilët nuk janë të vendosur në Republikën e Shqipërisë, por që e ushtrojnë veprimtarinë nëpërmjet përdorimit të çdo mjeti, që ndodhet në Republikën e Shqipërisë.

3. Në rastet e parashikuara në shkronjën “c” të pikës 2 të këtij neni, kontrolluesi cakton një përfaqësues, i cili duhet të jetë i vendosur në Republikën e Shqipërisë. Parashikimet e këtij ligji, që zbatohen nga kontrolluesit, zbatohen edhe për përfaqësuesit e tyre.

3/1. Ky ligj zbatohet edhe për autoritetet zyrtare që përpunojnë të dhëna personale në fushat e parashikuara në pikën 2, të nenit 6, të këtij ligji.

4. Ky ligj nuk zbatohet për përpunimin e të dhënave:

- a) për persona fizikë, për qëllime thjesht familjare ose personale;
- b) vetëm për rastet kur jepet informacion për persona publikë zyrtarë ose punonjës të administratës publike (shtetërore), nëpërmjet të cilit pasqyrohet aktiviteti publik, administrativ ose çështje lidhur me detyrën e tyre.

KREU II

PËRPUNIMI I TË DHËNAVE PERSONALE

Neni 5

Mbrojtja e të dhënave personale

1. Mbrojtja e të dhënave personale bazohet:

- a) në përpunimin në mënyrë të drejtë dhe të ligjshme;
- b) në grumbullimin për qëllime specifike, të përcaktuara qartë, e legjitime dhe në përpunimin në përputhje me këto qëllime;
- c) në mjaftueshmërinë e të dhënave, të cilat duhet të lidhen me qëllimin e përpunimit dhe të mos e tejkalojnë këtë qëllim;
- ç) në saktësinë që të dhënat duhet të kenë dhe, kur është e nevojshme, duhet të përditësohen; duhet ndërmarrë çdo hap i arsyeshëm për të fshirë apo korrigjuar të dhëna të pasakta apo të paplota, në lidhje me qëllimin për të cilin janë mbledhur apo për të cilin përpunohen më tej;
- d) në mbajtjen në atë formë, që të lejojë identifikimin e subjekteve të

të dhënave për një kohë, por jo më tepër sesa është e nevojshme për qëllimin, për të cilin ato janë grumbulluar ose përpunuar më tej.

2. Kontrolluesi është përgjegjës për zbatimin e këtyre kërkesave në të gjitha përpunimet automatike ose me mjete të tjera të të dhënave.

Neni 6

Kriteret ligjore për përpunimin

1. Të dhënat personale përpunohen vetëm:

a) nëse subjekti i të dhënave personale ka dhënë pëlqimin;

b) nëse përpunimi është thelbësor për përmbushjen e një kontrate, për të cilën subjekti i të dhënave është palë kontraktuese, apo për diskutime ose ndryshime të një projekti/kontrate me propozimin e subjektit të të dhënave;

c) për të mbrojtur interesat jetikë të subjektit të të dhënave;

ç) për përmbushjen e një detyrimi ligjor të kontrolluesit;

d) për kryerjen e një detyre ligjore me interes publik ose ushtrimin e një kompetence të kontrolluesit ose të një pale të tretë, së cilës i janë përhapur të dhënat;

dh) nëse është thelbësor për mbrojtjen e të drejtave dhe interesave legjitime të kontrolluesit, marrësit apo personave të tjerë të interesuar. Por, në çdo rast, përpunimi i të dhënave personale nuk mund të jetë në kundërshtim të hapur me të drejtën e subjektit të të dhënave për mbrojtjen e jetës personale dhe private.

2. Përpunimi i të dhënave personale, të përcaktuara në kuadër të veprimtarive të parandalimit dhe ndjekjes penale, për kryerjen e një vepre penale kundër rendit publik dhe të veprave të tjera në fushën e të drejtës penale, si dhe në fushën e mbrojtjes dhe sigurisë kombëtare, kryhet nga autoritetet zyrtare të përcaktuara në ligj.

3. Kontrolluesi apo përpunuesi, që merret me përpunimin e të dhënave personale, me qëllim ofrimin e mundësive për biznes apo të shërbimeve, mund të përdorë për këtë qëllim të dhëna personale të marra nga lista publike të dhënash. Kontrolluesi apo përpunuesi nuk mund të vazhdojë përpunimin më tej të të dhënave të specifikuar në këtë paragraf, nëse subjekti i të dhënave ka shprehur mospajtim ose ka kundërshtuar

përpunimin e mëtejshëm të tyre. Asnjë e dhënë personale shtesë nuk mund t'i bashkëlidhet të dhënave të specifikuar më lart, pa pëlqimin e subjektit të të dhënave.

4. Kontrolluesit i lejohet të mbajë në sistemin e vet të arkivimit të dhënat personale edhe pasi subjekti ka kundërshtuar përpunimin, sipas pikës 3 të këtij neni. Këto të dhëna mund të përdoren përsëri vetëm nëse subjekti i të dhënave personale jep pëlqimin.

5. Mbledhja e të dhënave personale, që lidhen në mënyrë unike me një subjekt të dhënash, për arsye të tregtimit të drejtpërdrejtë, lejohet vetëm nëse subjekti i të dhënave ka dhënë pëlqimin e shprehur qartë.

Neni 7

Përpunimi i të dhënave sensitive

1. Me përjashtim të rasteve të parashikuara në pikat 2 dhe 3 të këtij neni, ndalohet përpunimi i të dhënave, që zbulojnë origjinën racore ose etnike, mendimet politike, anëtarësinë në sindikata besimin fetar apo filozofik, dënimet penale, si dhe shëndetin dhe jetën seksuale.

2. Përpunimi i të dhënave sensitive bëhet vetëm nëse:

a) subjekti i të dhënave ka dhënë pëlqimin, që mund të revokohet në çdo çast dhe e bën të paligjshëm përpunimin e mëtejshëm të të dhënave;

b) është në interesin jetik të subjektit të të dhënave ose të një personi tjetër dhe subjekti i të dhënave është fizikisht ose mendërisht i paaftë për të dhënë pëlqimin e vet;

c) autorizohet nga autoriteti përgjegjës për një interes të rëndësishëm publik, nën masa të përshtatshme mbrojtëse;

ç) lidhet me të dhëna, që janë bërë haptazi publike nga subjekti i të dhënave ose është i nevojshëm për ushtrimin apo mbrojtjen e një të drejte ligjore;

d) të dhënat përpunohen për qëllime historike, shkencore ose statistikore, nën masa të përshtatshme mbrojtëse;

dh) të dhënat kërkohen për qëllime të mjekësisë parandaluese, diagnostikimit mjekësor, sigurimit të kujdesit shëndetësor, kurimit, menaxhimit të shërbimeve të kujdesit shëndetësor dhe përdorimi i tyre kryhet nga personeli mjekësor ose persona të tjerë, që kanë detyrimin

për ruajtjen e fshehtësisë;

e) të dhënat përpunohen nga organizatat jofitimprurëse politike, filozofike, fetare ose sindikaliste, për qëllime të veprimtarisë të tyre të ligjshme, vetëm për anëtarët, sponsorizuesit ose personat e tjerë, që kanë lidhje me veprimtarinë e tyre. Këto të dhëna nuk u bëhen të ditura një pale të tretë, pa pëlqimin e subjektit të të dhënave, përveç kur parashikohet ndryshe në ligj;

ë) përpunimi është i nevojshëm për përmbushjen e detyrimit ligjor dhe të të drejtave specifike të kontrolluesit në fushën e punësimit, në përputhje me Kodin e Punës.

Neni 8

Transferimi ndërkombëtar

1. Transferimi ndërkombëtar i të dhënave personale kryhet, me marrës, nga shtete me një nivel të mjaftueshëm të mbrojtjes së të dhënave personale. Niveli i mbrojtjes së të dhënave personale për një shtet përcaktohet duke vlerësuar të gjitha rrethanat lidhur me përpunimin, natyrën, qëllimin dhe kohëzgjatjen e tij, shtetin e origjinës dhe destinacionin përfundimtar, aktet ligjore dhe standardet e sigurisë në fuqi në shtetin marrës. Shtetet, që kanë nivel të mjaftueshëm të mbrojtjes së të dhënave, përcaktohen me vendim të Komisionerit.

2. Transferimi ndërkombëtar i të dhënave personale me një shtet, që nuk ka nivel të mjaftueshëm të mbrojtjes së të dhënave personale mund të bëhet nëse:

a) autorizohet nga akte ndërkombëtare, të ratifikuara nga Republika e Shqipërisë dhe që janë të zbatueshme në mënyrë të drejtpërdrejtë;

b) subjekti i të dhënave ka dhënë pëlqimin për transferim ndërkombëtar;

c) transferimi është i nevojshëm për kryerjen e kontratës ndërmjet subjektit të të dhënave dhe kontrolluesit ose për zbatimin e masave parakontraktore, të marra si përgjigje ndaj kërkesës së subjektit, ose transferimi është i nevojshëm për përmbushjen apo kryerjen e një kontrate ndërmjet kontrolluesit dhe një pale të tretë, në interes të subjektit të të dhënave;

d) është i nevojshëm për mbrojtjen e interesave jetësorë të subjektit të

të dhënave;

dh) është i nevojshëm apo përbën një kërkesë ligjore për një interes të rëndësishëm publik ose për ushtrimin dhe mbrojtjen e një të drejte ligjore;

e) është bërë nga një regjistër, i cili është i hapur për këshillime dhe siguron informacion për publikun në përgjithësi.

3. Shkëmbimi i të dhënave personale me përfaqësitë diplomatike të qeverive të huaja ose institucionet ndërkombëtare në Republikën e Shqipërisë vlerësohet transferim ndërkombëtar.

Neni 9

Transferimi ndërkombëtar i të dhënave që duhet të autorizohen

1. Transferimi ndërkombëtar i të dhënave personale me një shtet, që nuk ka nivel të mjaftueshëm të mbrojtjes së të dhënave, në raste të tjera nga ato të parashikuara në nenin 8 të këtij ligji, bëhet me autorizim të komisionerit kur parashtrihen siguri të mjaftueshme në lidhje me mbrojtjen e privatësisë dhe të të drejtave e lirive themelore të njeriut, si dhe në lidhje me ushtrimin e së drejtës përkatëse.

2. Komisioneri, pasi bën vlerësimin sipas përcaktimeve të pikës 1 të këtij neni dhe të pikës 1 të nenit 8, mund të japë autorizimin për transferimin e të dhënave personale në shtetin marrës, duke përcaktuar kushte dhe detyrime.

3. Komisioneri nxjerr udhëzime për lejimin e disa kategorive të transferimeve ndërkombëtare të të dhënave personale në një shtet që nuk ka nivel të mjaftueshëm të mbrojtjes së të dhënave personale. Në këto raste, kontrolluesi përjashtohet nga kërkesa për autorizim.

4. Kontrolluesi, përpara transferimit të të dhënave, bën kërkesë për autorizim te komisioneri. Në kërkesë kontrolluesi duhet të garantojë respektimin e interesave për ruajtjen e sekretit të subjektit të të dhënave jashtë Republikës së Shqipërisë.

KREU III PËRPUNIMI I VEÇANTË I TË DHËNAVE

Neni 10

Përpunimi për qëllime historike, shkencore dhe statistikore

1. Të dhënat personale, të mbledhura për çfarëdolloj qëllimi, mund të përpunohen më tej për qëllime historike, shkencore ose statistikore, duke siguruar se nuk janë përpunuar, për të marrë masa ose vendime për një individ.
2. Transmetimi i të dhënave sensitive për kërkimet shkencore bëhet vetëm kur ekziston një interes i rëndësishëm publik. Të dhënat personale përdoren vetëm nga persona, të cilët janë të detyruar të ruajnë konfidencialitetin.
3. Në rastet kur përdorimi i të dhënave bëhet në një formë, që lejon identifikimin e subjektit të të dhënave, të dhënat duhet të kodohen menjëherë, në mënyrë që subjektet të mos jenë më të identifikueshme. Të dhënat personale të koduara përdoren vetëm nga persona, të cilët janë të detyruar të ruajnë konfidencialitetin.

Neni 11

Përpunimi i të dhënave personale dhe e liria të shprehurit

1. Komisioneri përcakton me udhëzim të veçantë kushtet dhe kriteret kur, për qëllime gazetarie, letrare dhe artistike, mund të bëhen përjashtime nga detyrimet që rrjedhin nga nenet 5, 6, 7, 8, 18 dhe 21 të këtij ligji.
2. Përjashtimet, sipas këtij neni, mund të lejohen deri në atë masë, për aq sa ato pajtojnë të drejtën për mbrojtjen e të dhënave personale me rregullat që administrojnë lirinë e informimit.
3. Veprimet e kontrolluesit ose përpunuesit, në kundërshtim me pikat e mësipërme dhe kodin etik përbëjnë kundërvajtje administrative.

KREU IV TË DREJTAT E SUBJEKTIT TË TË DHËNAVE

Neni 12 E drejta për akses

1. Çdo person ka të drejtë që pa pagesë me kërkesë me shkrim, të marrë nga kontrolluesi:

a) konfirmimin nëse të dhënat personale po i përpunohen ose jo, informacion për qëllimin e përpunimit, për kategoritë e të dhënave të përpunuara dhe për marrësit e kategoritë e marrësve, të cilëve u përhapen të dhënat personale;

b) në një formë të kuptueshme, të dhënat personale dhe informacionin e disponueshëm për burimin e tyre;

c) në rastet e vendimeve automatike, sipas nenit 14 të këtij ligji, informacion për logjikën e përfshirë në vendimmarrje.

Informacioni për të dhënat komunikohet në formën, në të cilën ishin në kohën kur është bërë kërkesa.

2. Kontrolluesi, brenda 30 ditëve nga data e marrjes së kërkesës, informon subjektin e të dhënave ose i shpjegon atij arsyet e mosdhënies së informacionit.

3. E drejta për akses, sipas pikës 1 të këtij neni, ushtrohet në përputhje me parimet kushtetuese të lirisë së shprehjes dhe informacionit, lirisë së shtypit dhe sekretit profesional dhe mund të kufizohet, nëse cenon interesat e sigurisë kombëtare, politikën e jashtme, interesat ekonomike dhe financiarë të shtetit, parandalimin dhe ndjekjen e veprave penale.

4. E drejta e aksesit nuk mund të ushtrohet në rastet e parashikuara në pikën 1 të nenit 10 të këtij ligji.

5. Në rast se aksesimi mohohet, duke argumentuar se cenohen interesat e sigurisë kombëtare, politika e jashtme, interesat ekonomike dhe financiarë të shtetit, parandalimi dhe ndjekja e veprave penale ose liria e shprehjes dhe informimit apo liria e shtypit, subjekti i të dhënave mund t'i kërkojë komisionerit të kontrollojë përjashtimin në rastin konkret. Komisioneri informon subjektin e të dhënave për masat e marra.

Neni 13

E drejta për të kërkuar bllokimin, korrigjimin ose fshirjen

1. Çdo subjekt i të dhënave ka të drejtë të kërkojë bllokimin, korrigjimin ose fshirjen e të dhënave pa pagesë, kur vihet në dijeni se të dhënat rreth tij nuk janë të rregullta, të vërteta, të plota ose janë përpunuar dhe mbledhur në kundërshtim me dispozitat e këtij ligji.
2. Kontrolluesi, brenda 30 ditëve nga data e marrjes së kërkesës së subjektit të të dhënave, duhet ta informojë atë për përpunimin e ligjshëm të të dhënave, kryerjen ose moskryerjen e bllokimit, korrigjimit apo të fshirjes.
3. Kur kontrolluesi nuk bën bllokimin, korrigjimin ose fshirjen e të dhënave të kërkuara prej tij, subjekti i të dhënave ka të drejtë të ankohet te komisioneri.

Neni 14

Vendimmarrja automatike

1. Çdo person ka të drejtë të mos jetë subjekt i vendimeve, të cilat shkaktojnë efekte ligjore për të ose ndikojnë në mënyrë të rëndësishme tek ai dhe kur vendimi është bazuar vetëm në përpunimin automatik të të dhënave, që synojnë të vlerësojnë disa aspekte personale, që lidhen me të, veçanërisht, efektivitetin në punë, besueshmërinë ose sjelljen.
2. Një person mund të jetë subjekt i një vendimi të marrë, sipas pikës 1 të këtij neni, kur vendimi:
 - a) është marrë gjatë lidhjes ose zbatimit të një kontrate, nëse kërkesa e paraqitur nga subjekti i të dhënave për lidhjen ose zbatimin e kontratës është përmbushur, ose nëse ka masa të përshtatshme për të mbrojtur interesat e tij të ligjshëm, të tillë si mundësi që e lejojnë atë të parashtrijë pikëpamjet e tij;
 - b) autorizohet nga një ligj, i cili, gjithashtu, parashikon masa për të mbrojtur interesat e ligjshëm të subjektit të të dhënave.

Neni 15

E drejta e subjektit të të dhënave për të kundërshtuar

1. Subjekti i të dhënave ka të drejtë të kundërshtojë, në çdo kohë, mbështetur në ligj, përpunimin e të dhënave rreth tij, sipas shkronjave “d” dhe “dh” të nenit 6 të këtij ligji, përveç kur parashikohet ndryshe me ligj.
2. Subjekti i të dhënave ka të drejtë pa pagesë t’i kërkojë kontrolluesit të mos fillojë ose, nëse përpunimi ka filluar, të ndalojë përpunimin e të dhënave personale, që lidhen me të, për qëllime të tregtimit të drejtpërdrejtë si dhe të informohet përpara përhapjes për herë të parë të të dhënave personale për këtë qëllim.

Neni 16

E drejta për t’u ankuar

1. Çdo person, që pretendon se i janë shkelur të drejtat, liritë dhe interesat e ligjshëm për të dhënat personale, ka të drejtë të ankohet ose të njoftojë komisionerin dhe të kërkojë ndërhyrjen e tij për vënien në vend të së drejtës së shkelur. Pas këtij ankimi, në përputhje me Kodin e Procedurës Civile, subjekti i të dhënave mund të ankohet në gjykatë.
2. Në rast se subjekti i të dhënave ka bërë ankim, kontrolluesi nuk ka të drejtë të ndryshojë të dhënat personale deri në dhënien e vendimit përfundimtar.

Neni 17

Kompensimi i dëmit

Çdo person, të cilit i është shkaktuar një dëm, si rezultat i përpunimit të paligjshëm të të dhënave personale, ka të drejtë t’i kërkojë kontrolluesit kompensim, sipas rregullave të përcaktuara në Kodin Civil.

KREU V DETYRIMET E KONTROLLUESIT DHE TË PËRPUNUESIT

Neni 18 Detyrimi për informim

1. Kontrolluesi, kur mbledh të dhëna personale, duhet të informojë subjektin e të dhënave për fushën dhe qëllimin, për të cilin do të përpunohen të dhënat personale, për personin që do t'i përpunojë të dhënat, për mënyrën e përpunimit, përveç rastit kur subjekti i të dhënave është në dijeni të këtij informacioni. Kontrolluesi duhet të informojë subjektin e të dhënave për të drejtën për akses, si dhe të drejtën për korrigjim të të dhënave të tij.

2. Në rast se kontrolluesi përpunon të dhëna personale, të marra nga subjekti i të dhënave, ai është i detyruar të informojë subjektin e të dhënave nëse dhënia e të dhënave personale është e detyrueshme apo vullnetare. Nëse subjekti i të dhënave, në bazë të një akti ligjor ose nënligjor, është i detyruar të japë të dhëna personale për përpunim, kontrolluesi e informon edhe rreth këtij fakti, si dhe rreth pasojave të refuzimit të dhënies së të dhënave personale.

3. Kontrolluesi nuk është i detyruar të japë informacion dhe të informojë për rastet kur të dhënat personale nuk janë marrë nga subjekti i të dhënave, nëse:

a) ai përpunon të dhëna personale ekskluzivisht për qëllime historike, statistikore dhe për kërkime shkencore dhe nëse dhënia e këtij informacioni është e pamundur, ose kërkon përpjekje joproporcionale;

b) ai detyrohet të kryejë përpunimin e të dhënave personale në bazë të një parashikimi ligjor;

c) ai përpunon të dhëna të bëra publike;

ç) ai përpunon të dhëna personale, të marra me pëlqimin e subjektit të të dhënave.

4. Kontrolluesi, gjatë përpunimit të të dhënave personale, sipas shkronjës “dh” të pikës 1 të nenit 6 dhe shkronjës “ç” të pikës 2 të nenit 7, në lidhje me ushtrimin apo mbrojtjen e të drejtave të ligjshme, është i detyruar të informojë subjektin e të dhënave rreth përpunimit të të dhënave të tij.

5. Detyrimi për informim, që rregullohet me këtë nen, mund të kryhet nga përpunuesi në emër të kontrolluesit.

Neni 19

Detyrimi për korrigjim ose fshirje

1. Kontrolluesi kryen vetë ose me kërkesë të subjektit të të dhënave bllokimin, korrigjimin ose fshirjen e të dhënave personale, kur vëren se janë të parregullta, të pavërteta, të paplota ose janë përpunuar në kundërshtim me dispozitat e këtij ligji.
2. Kontrolluesi, brenda 30 ditëve nga marrja e kërkesës së subjektit të të dhënave, informon subjektin e të dhënave për kryerjen apo moskryerjen e bllokimit, korrigjimit ose të fshirjes.
3. Kontrolluesi informon marrësin e të dhënave personale për korrigjimin ose fshirjen e të dhënave personale, të transmetuara para korrigjimit apo fshirjes.

Neni 20

Detyrimet e përpunuesit

1. Kontrolluesit, për përpunimin e të dhënave personale, mund të punësojnë përpunues, të cilët garantojnë përdorimin e ligjshëm dhe të sigurt të të dhënave. Çdo përpunues i të dhënave personale ka këto detyrime:
 - a) të përpunojë të dhënat vetëm në përputhje me udhëzimet e kontrolluesit; të mos i transmetojë ato, përveç kur ka marrë udhëzim nga kontrolluesi;
 - b) të marrë të gjitha masat e sigurisë, sipas këtij ligji dhe të punësojë operatorë, të cilët kanë detyrimin për ruajtjen e fshehtësisë;
 - c) të krijojë, në marrëveshje me kontrolluesin, kushtet e nevojshme teknike dhe organizative për përmbushjen e detyrimeve të kontrolluesit, për të siguruar të drejtat e subjekteve të të dhënave personale;
 - ç) t'i dorëzojë kontrolluesit, pas përfundimit të shërbimit të përpunimit, të gjitha rezultatet e përpunimit dhe dokumentacionit, që përmban të

dhëna ose t'i mbajë apo t'i shkatërrojë ato me kërkesë të kontrolluesit;
d) të vërë në dispozicion të kontrolluesit të gjithë informacionin e nevojshëm, për të kontrolluar përputhshmërinë me detyrimet, që rrjedhin sipas shkronjave të mësipërme.

2. Detyrimet e pikës 1 përcaktohen në kontratën e shkruar e kontrolluesit me përpunuesin.

KREU VI NJOFTIMI

Neni 21

Përgjegjësia për të njoftuar

1. Çdo kontrollues duhet të njoftojë komisionerin për përpunimin e të dhënave personale, për të cilat është përgjegjës. Njoftimi duhet të bëhet para se kontrolluesi të përpunojë të dhënat për herë të parë ose kur kërkohet ndryshimi i gjendjes së njoftimit të përpunimit, sipas nenit 22 të këtij ligji, të njoftuar më parë.

2. Përjashtohet nga detyrimi për të njoftuar përpunimi i të dhënave personale, me qëllim mbajtjen e një regjistri, i cili, në përputhje me ligjin ose aktet nënligjore, siguron informacion për publikun në përgjithësi.

3. Përjashtohen nga detyrimi për të njoftuar të dhënat personale që përpunohen, me qëllim mbrojtjen e institucioneve kushtetuese, të interesave të sigurisë kombëtare, politikës së jashtme, interesave ekonomikë ose financiarë të shtetit, apo për parandalimin e ndjekjen e veprave penale.

4. Rastet e tjera, për të cilat njoftimi nuk është i nevojshëm, përcaktohen me vendim të Komisionerit.

Neni 22

Përmbajtja e njoftimit

Njoftimi duhet të përmbajë:

- a) emrin dhe adresën e kontrolluesit;
- b) qëllimin e përpunimit të të dhënave personale;
- c) kategoritë e subjekteve të të dhënave dhe kategoritë e të dhënave personale;
- ç) marrësit dhe kategoritë e marrësve të të dhënave personale;
- d) propozimin për transferimet ndërkombëtare që kontrolluesi synon të kryejë;
- dh) një përshkrim të përgjithshëm të masave për sigurinë e të dhënave personale.

Neni 23

Procedura e shqyrtimit

Komisioneri shqyrton të gjitha njoftimet dhe kur njoftimi është i pamjaftueshëm, ai urdhëron kontrolluesin të plotësojë përmbajtjen e njoftimit, duke përcaktuar edhe afatin kohor.

Nëse kontrolluesi nuk plotëson përmbajtjen e njoftimit brenda afatit të përcaktuar, njoftimi konsiderohet i pakryer.

Neni 24

Kontroli paraprak

1. Autorizimi i komisionerit kërkohet për:

- a) përpunimin e të dhënave sensitive, sipas shkronjës “c” të pikës 2 të nenit 7 të këtij ligji;
- b) përpunimin e të dhënave personale, sipas pikës 1 të nenit 9 të këtij ligji.

2. Nëse përpunimi i të dhënave, sipas pikës 1 të këtij neni, autorizohet nga një dispozitë ligjore, nuk kërkohet autorizim nga komisioneri.

Neni 25

Fillimi i përpunimit

1. Përpunimi i të dhënave fillon pas njoftimit.

2. Përpunimi i të dhënave, për të cilat kërkohet autorizim, sipas pikës 1 të nenit 24 të këtij ligji, mund të fillojë vetëm pas marrjes së autorizimit.

Neni 26

Publikimi i përpunimeve

1. Për të dhënat që kërkohet autorizim, merret vendim i veçantë dhe pasqyrohet në regjistrin që administrohet nga komisioneri, i cili është i hapur për njohje për çdo person.

2. Regjistrimi duhet të përmbajë informacionin, sipas nenit 22 të këtij ligji, përveç informacionit të përcaktuar në shkronjën “dh” të nenit 22 të këtij ligji, i cili nuk publikohet.

3. Kontrolluesi i përjashtuar nga detyrimi për njoftim duhet të bëjë të disponueshme, të paktën, të dhënat për emrin dhe adresën, kategoritë e të dhënave personale të përpunuara, qëllimet e përpunimeve, kategoritë e marrësve.

Nëse do të bëhet transferim ndërkombëtar i të dhënave, kontrolluesi është i detyruar të njoftojë Komisionerin.

4. Ky nen nuk zbatohet për përpunime për mbajtjen e një regjistri, i cili, në përputhje me ligjin apo aktet nënligjore, siguron informacion për publikun në përgjithësi.

5. Komisioneri vendos për çregjistrimin e kontrolluesit, kryesisht ose me kërkesën e tij, nëse qëllimi ose qëllimet, për të cilat është kryer njoftimi dhe regjistrimi, pushojnë së ekzistuari.

KREU VII

SIGURIA E TË DHËNAVE PERSONALE

Neni 27

Masat për sigurinë e të dhënave personale

1. Kontrolluesi ose përpunuesi merr 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 kur përpunimi i të dhënave bëhet në rrjet, si dhe nga çdo formë tjetër e paligjshme përpunimi.

2. Kontrolluesi merr këto masa të veçanta sigurie:

a) përcakton funksionet ndërmjet njësive organizative dhe operatorëve për përdorimin e të dhënave;

b) përdorimi i të dhënave bëhet me urdhër të njësive organizative ose të operatorëve të autorizuar;

c) udhëzon operatorët, pa përjashtim, për detyrimet që kanë, në përputhje me këtë ligj dhe rregulloret e brendshme për mbrojtjen e të dhënave, përfshirë edhe rregulloret për sigurinë e të dhënave;

ç) ndalon hyrjen në mjediset e kontrolluesit ose të përpunuesit të të dhënave të personave të paautorizuar;

d) hyrja në të dhënat dhe programet bëhet vetëm nga personat e autorizuar,

dh) ndalon hyrjen në mjetet e arkivimit dhe përdorimin e tyre nga persona të paautorizuar;

e) vënia në punë e pajisjeve të përpunimit të të dhënave bëhet vetëm me autorizim dhe çdo mjet sigurohet me masa parandaluese ndaj vënies së autorizuar në punë;

ë) regjistron dhe dokumenton modifikimet, korrigjimet, fshirjet, transmetimet etj.

2/1. Kontrolluesi është i detyruar të dokumentojë masat tekniko-organizative të përshtatura dhe të zbatuara për garantimin e mbrojtjes së të dhënave personale, në përputhje me ligjin dhe rregullore të tjera.

3. Të dhënat e regjistruara nuk përdoren për qëllime të ndryshme, që nuk janë në përputhje me qëllimin e grumbullimit. Ndalohet njohja ose çdo përpunim i të dhënave të regjistruara në dosje për një qëllim të ndryshëm nga e drejta për të hedhur të dhëna. Përjashtohet nga ky rregull rasti kur të dhënat përdoren për të garantuar sigurinë kombëtare, sigurinë publike, parandalimin dhe hetimin e kryerjes së një vepre penale, apo ndjekjen e autorëve të saj, ose për shkelle të etikës për profesionet e rregulluara.

4. Dokumentacioni i të dhënave mbahet për aq kohë sa është i nevojshëm për qëllimin, për të cilin është grumbulluar.

5. Niveli i sigurisë duhet të jetë i përshtatshëm me natyrën e përpunimit

të të dhënave personale.

Rregulla të hollësishme për sigurimin e të dhënave përcaktohen me vendim të komisionerit.

6. Procedurat e administrimit të regjistrimit të të dhënave, të hedhjes së të dhënave, të përpunimit dhe nxjerrjes së tyre përcaktohen me vendim të komisionerit.

Neni 28

Konfidencialiteti i të dhënave

Kontrolluesit, përpunuesit dhe personat, që vihen në dijeni me të dhënat e përpunuara, gjatë ushtrimit të funksioneve të tyre, detyrohen të ruajnë konfidencialitetin dhe besueshmërinë edhe pas përfundimit të funksionit. Këto të dhëna nuk përhapen, përveç rasteve të parashikuara me ligj.

Çdo person që vepron nën autoritetin e kontrolluesit, nuk duhet t'i përpunojë të dhënat personale, tek të cilat ka akses, pa autorizimin e kontrolluesit, përveçse kur detyrohet me ligj.

KREU VIII

KOMISIONERI PËR MBROJTJEN E TË DHËNAVE PERSONALE

Neni 29

Komisioneri

1. Komisioneri për mbrojtjen e të dhënave personale është autoriteti përgjegjës i pavarur, që mbikëqyr dhe monitoron, në përputhje me ligjin, mbrojtjen e të dhënave personale, duke respektuar e garantuar të drejtat dhe liritë themelore të njeriut.

2. Komisioneri është person juridik publik.

3. Informacioni i siguruar nga komisioneri, gjatë ushtrimit të detyrës, përdoret vetëm për qëllime mbikëqyrjeje, në përputhje me legjislacionin për mbrojtjen e të dhënave personale. Komisioneri është i detyruar të ruajë konfidencialitetin e të dhënave edhe pas mbarimit të detyrës.

Neni 30 Të drejtat

1. Komisioneri ka këto të drejta:

- a) kryen hetim administrativ dhe ka të drejtën e aksesit në përpunimet e të dhënave personale, si dhe ka të drejtë të mbledhë të gjithë informacionin e nevojshëm për përmbushjen e detyrave të mbikëqyrjes;
- b) urdhëron bllokimin, fshirjen, shkatërrimin ose pezullon përpunimin e paligjshëm të të dhënave personale;
- c) jep udhëzime përpara se përpunimet të kryhen dhe siguron publikimin e tyre.

2. Komisioneri, në rast shkeljesh serioze, të përsëritura ose të qëllimshme të ligjit nga një kontrollues ose përpunues, veçanërisht në rastet e përsëritura të moszbatimit të rekomandimeve të tij, vepron sipas nenit 39 të këtij ligji dhe e denoncon publikisht ose e raporton çështjen në Kuvend dhe në Këshillin e Ministrave.

2/1. Për rastet që shkelja përbën vepër penale, bën kallëzimin përkatës.

Neni 31 Përgjegjësitë

1. Komisioneri është përgjegjës për:

- a) dhënien e mendimeve për projekt-aktet, ligjore dhe nënligjore, që kanë të bëjnë me të dhënat personale, si dhe projektet që kërkohen të zbatohen nga kontrolluesit vetëm apo në bashkëpunim me të tjerë;
- a/1) dhënien e rekomandimeve për zbatimin e kërkesave të ligjit për mbrojtjen e të dhënave personale dhe siguron publikimin e tyre;
- b) dhënien e autorizimit, në raste të veçanta, për përdorimin e të dhënave personale për qëllime jo të përcaktuara në grumbullimin e tyre, duke respektuar parimet e nenit 5 të këtij ligji;
- c) dhënien e autorizimit për transferimin ndërkombëtar të të dhënave personale, në përputhje me nenin 9 të këtij ligji;
- ç) nxjerrjen e udhëzimeve, ku përcaktohet koha e mbajtjes së të dhënave personale, sipas qëllimit të tyre, në veprimtarinë e sektorëve të veçantë;
- d) sigurimin e së drejtës së informimit dhe të ushtrimit të së drejtës së

- korrigjimit e të përditësimit të të dhënave;
- dh) dhënien e autorizimit për përdorimin e të dhënave sensitive, në përputhje me shkronjën “c” të pikës 2 të nenit 7 të këtij ligji;
- e) kontrollimin e përpunimit të të dhënave, në përputhje me ligjin, kryesisht ose me kërkesë të një personi edhe, kur një përpunim i tillë është i përjashtuar nga e drejta e informacionit dhe vënien në dijeni të personit se kontrolli është kryer, si dhe verifikimin nëse procesi është i ligjshëm ose jo;
- ë) zgjidhjen e ankimeve të subjektit të të dhënave për mbrojtjen e të drejtave dhe të lirive të tij, për përpunimet e të dhënave personale dhe vënien e tij në dijeni për zgjidhjen e ankesës së paraqitur;
- f) nxjerrjen e udhëzimeve për marrjen e masave të sigurisë në veprimtarinë e sektorëve të veçantë;
- g) kontrollin e zbatimit të gjobave;
- gj) nxitjen e kontrolluesit për hartimin e kodeve të etikës dhe vlerësimin e tyre;
- h) publikimin dhe shpjegimin e të drejtave për mbrojtjen e të dhënave dhe publikimin periodikisht të veprimtarive të zhvilluara prej tij;
- i) bashkëpunimin me autoritetet mbikëqyrëse për të dhënat personale të shteteve të huaja, për mbrojtjen e të drejtave të individëve rezidentë në këto shtete;
- j) përfaqësimin e autoritetit mbikëqyrës në fushën e mbrojtjes së të dhënave personale në veprimtaritë kombëtare dhe ndërkombëtare;
- k) ushtrimin e detyrave të tjera ligjore.
2. Komisioneri krijon një regjistër për dokumentimin e të gjitha njoftimeve dhe autorizimeve, që ai kryen në ushtrim të kompetencave të tij, në fushën e mbrojtjes së të dhënave personale.
3. Komisioneri paraqet raport vjetor përpara Kuvendit dhe raporton përpara tij sa herë i kërkohet.
- Gjithashtu, ai mund t’i kërkojë Kuvendit të dëgjohet për çështje që i çmon të rëndësishme.

Neni 32
Detyrimi për bashkëpunim

1. Institucionet publike dhe private bashkëpunojnë me komisionerin, duke i siguruar të gjithë informacionin që ai kërkon për përmbushjen e detyrave, si dhe e njoftojnë atë për zbatimin e rekomandimeve të dhëna menjëherë pas mbarimit të afatit të caktuar për kryerjen e tyre.
2. Komisioneri ka akses në sistemin e kompjuterave, në sistemet e arkivimit, që kryejnë përpunimin e të dhënave personale dhe në të gjithë dokumentacionin, që lidhet me përpunimin dhe transferimin e tyre, për ushtrimin e të drejtave dhe të detyrave që i janë ngarkuar me ligj.

Neni 33
Zgjedhja dhe qëndrimi në detyrë

Komisioneri zgjidhet nga Kuvendi, me propozimin e Këshillit të Ministrave, për një mandat 5- vjeçar, me të drejtë rizgjedhjeje.

Neni 34
Papajtueshmëria e funksionit

Funksioni i komisionerit është i papajtueshëm me çdo funksion tjetër shtetëror, me anëtarësimin në partitë politike dhe pjesëmarrjen në veprimtaritë e tyre, si dhe me çdo veprimtari tjetër fitimprurëse, me përjashtim të mësimdhënies.

Neni 35
Kriteret për t'u zgjedhur

Komisioner mund të zgjidhet shtetasi shqiptar, që plotëson kushtet e mëposhtme:

- a) ka arsim të lartë juridik;
- b) ka njohuri dhe veprimtari të shquara në fushën e të drejtave dhe lirive

themelore të njeriut;

c) shquhet për aftësi profesionale dhe figurë të pastër etiko-morale;

ç) ka vjetërsi pune në profesionin e juristit jo më pak se 10 vjet;

d) nuk është dënuar me vendim të formës së prerë për kryerjen e një vepre penale;

dh) nuk është larguar nga puna ose shërbimi civil me masë disiplinore.

Neni 36

Mbarimi i mandatit

1. Mandati i komisionerit mbaron para kohe kur:

a) dënohet nga gjykata me vendim të formës së prerë për kryerjen e një vepre penale;

b) nuk paraqitet pa arsye në detyrë për më shumë se 1 muaj;

c) jep dorëheqjen;

ç) deklarohet i paaftë me vendim gjykate të formës së prerë.

2. Komisioneri mund të shkarkohet nga Kuvendi:

a) për shkelje të dispozitave të këtij ligji apo akteve të tjera ligjore;

b) kur kryen veprimtari, që krijon konflikt interesash;

c) kur zbulohen raste të papajtueshmërisë së funksionit të tij.

3. Në rast se vendi i komisionerit mbetet vakant, Këshilli i Ministrave, brenda 15 ditëve, i propozon Kuvendit kandidaturën e re. Kuvendi zgjedh komisionerin brenda 15 ditëve nga paraqitja e kandidaturës.

Neni 37

Zyra e komisionerit

Kuvendi vendos për pagën e komisionerit, strukturën organizative dhe klasifikimin e pagave për punonjësit e zyrës së komisionerit për mbrojtjen e të dhënave personale. Punonjësit e kësaj zyre gëzojnë statusin e nëpunësit civil.

Neni 38
Buxheti

Komisioneri ka buxhetin e vet të pavarur, i cili financohet nga Buxheti i Shtetit dhe donatorë, të cilët nuk paraqesin konflikt interesi. Administrimi i këtyre donacioneve bëhet sipas marrëveshjeve me donatorët dhe legjislacionin shqiptar në fuqi.

Neni 38/a
Publikimi

1. Udhëzimet, vendimet e Komisionerit, me përjashtim të atyre të dhëna në zbatim të shkronjës “b” të nenit 30 dhe të nenit 39 të këtij ligji, botohen në Fletoren Zyrtare.
2. Raporti vjetor dhe raportet e veçanta bëhen publike.

KREU IX
SANKSIONE ADMINISTRATIVE

Neni 39
Kundërvajtjet administrative

1. Rastet e përpunimit të të dhënave në kundërshtim me dispozitat e këtij ligji kur nuk përbëjnë kundërvajtje penale përbëjnë kundërvajtje administrative dhe dënohen 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;
 - a/1) kontrolluesit, që përdorin të dhëna personale në kundërshtim me kreun III, “Përpunimi i veçantë i të dhënave”, dënohen me 15 000 deri në 200 000 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;

c) kontrolluesit, që nuk përmbushin detyrimin për të korrigjuar ose fshirë të dhënat, të përcaktuar në nenin 19 të këtij ligji, dënohen me 15 000 deri në 300 000 lekë;

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

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

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

dh/1) kontrolluesit dhe përpunuesit, që veprojnë në kundërshtim me pikën 2 të nenit 32 të këtij ligji, dënohen me 100 000 deri në 1 000 000 lekë.

2. Personat juridikë, për kundërvajtjet e mësipërme, dënohen me dyfishin e gjobës së përcaktuar në pikën 1 të këtij neni.

3. Maksimumi i gjobës dyfishohet në rastin kur veprohet në kundërshtim me pikën 2 të nenit 16 të këtij ligji dhe kur të dhënat përpunohen pa autorizim, sipas shkronjës “b” të pikës 1 të nenit 31 të këtij ligji.

4. Gjobat vendosen nga Komisioneri, kur vërehet se janë shkelur detyrimet e përcaktuara në ligj.

Neni 40

Ankimi

Ndaj dënimit administrativ me gjobë bëhet ankimi në gjykatë në afatet dhe sipas procedurave që rregullojnë gjykimin administrativ.

Neni 41

Ekzekutimi i gjobave

1. Gjobat paguhen nga kundërvajtësi jo më vonë se 30 ditë nga komunikimi

i tyre.

Me kalimin e këtij afati, vendimi i dhënë shndërrohet në titull ekzekutiv dhe ekzekutohet në mënyrë të detyrueshme nga zyra e përmbarimit, me kërkesë të komisionerit.

2. Gjobat arkëtohen në Buxhetin e Shtetit.

KREU X DISPOZITA TË FUNDIT

Neni 42 Aktet nënligjore

Ngarkohet Këshilli i Ministrave të nxjerrë aktet nënligjore në zbatim të neneve 7, 8 e 21 të këtij ligji.

Neni 43 Shfuqizime

Ligji nr. 8517, datë 22.7.1999 “Për mbrojtjen e të dhënave personale”, shfuqizohet.

Neni 44 Hyrja në fuqi

Ky ligj hyn në fuqi 15 ditë pas botimit në Fletoren Zyrtare.

Shpallur me dekretin nr. 5671, datë 21.03.2008 dhe nr. 7451, datë 08.05.2012 të Presidentit të Republikës së Shqipërisë,

Bamir Topi

Ekspertët e Projektit IPA

“Forcimi i Zyrës së Komisionerit për Mbrojtjen e të Dhënave Personale në Shqipëri për Harmonizimin me Standardet e Bashkimit Evropian”



JUDr Jiří Maštalka

Jiří Maštalka është diplomuar në Universitetin Charles në Pragë. Ai ka një doktoratë në juridik. Ka një përvojë profesionale 11 vjeçare në Zyrën për Mbrojtjen e të Dhënave Personale, si edhe në hartimin e dokumenteve ligjore për çështjet që lidhen me mbrojtjen e të dhënave personale. Ai ka një eksperiencë të gjerë si ekspert në transpozimin e legjislacionit të BE-së për mbrojtjen e të dhënave personale në vendet e mundshme kandidate për në BE (këshilltar i përhershëm binjakëzimi për projektin e binjakëzimit BA-2004-IB-OT-0). Ka punuar si ekspert afatshkurtër për asistencë teknike në Ish Republikën Jugosllave të Maqedonisë në projektin “Krijimi i një Drejtorie për Mbrojtjen e të Dhënave Personale dhe Zbatimin e Parimeve për Mbrojtjen e të Dhënave Personale”, si edhe në rolin e ekspertit kryesor për çështje ligjore dhe procedurale në projektin e financiar nga BE-ja “Forcimi i Zyrës së Komisionerit për Mbrojtjen e të Dhënave Personale në Shqipëri për Harmonizim me Standardet e Bashkimit Evropian” (EuropeAid/129606/C/SER/AL). Ai ka botuar një sërë artikujsh, leksionesh dhe fjalimesh profesionale për mbrojtjen dhe përpunimin e të dhënave personale. Aktualisht ai është anëtar i Departamentit Ligjor dhe i Marrëdhënieve me Jashtë të Zyrës për Mbrojtjen e të Dhënave Personale në Çeki.



Dr Stefan Szyszko

Stefan Szyszko është doktor i shkencave teknike nga Universiteti i Teknologjisë në Varshavë, 1982. Gjatë periudhës 1976-1992 ai ka punuar si shkencëtar për Universitetin e Teknologjisë në Varshavë (Poloni), RWTH Ahen (Gjermani), UMIST DIAS (Mbretëri e Bashkuar), ESA Këln, Gjermani, duke zhvilluar sisteme IT-je mbështetëse të vendimeve, rrjete neurale, sisteme ekspertësh për diagnostikime teknike, në bashkëpunim me industrinë e makinave, atë kimike, hapësinore dhe të energjisë bërthamore. Që nga viti 1997 ai punon për sektorin polak nga viti 2006. Ka qenë përgjegjës për zhvillimin e bazave të të dhënave statistikore dhe kundër mashtrimit, në bashkëpunim me Autoritetin polak të Mbikëqyrjes së Sektorit Financiar dhe Ministrinë e Financës. Ai ka marrë pjesë aktivisht në hartimin dhe vlerësimin e projekteve ligjore që mbulojnë ligjin polak dhe evropian për mbrojtjen e të dhënave personale. Që nga viti 2007 ai ka luajtur një rol aktiv si ekspert i lartë i BE-së për mbrojtjen e të dhënave personale, duke marrë pjesë në shumë projekte të BE-së në Maqedoni dhe Shqipëri. Ndërkohë, që nga viti 1999 ai ka bashkëpunuar ngushtë me Autoritetin Mbikëqyrës për Mbrojtjen e të Dhënave Personale në Poloni dhe tani është anëtar i grupit të ekspertëve të Komisionerit, të cilët po hartojnë kuadrin e ri të ligjit polak për mbrojtjen e të dhënave personale në lidhje me sigurinë e të dhënave. Në vitin 2010 ai u bë anëtar i Task-Forcës së përbashkët për mbrojtjen e të dhënave personale në Insurance Europe. Që nga viti 2008 ai është anëtar i Shoqatës Polake të Koordinatorëve për Mbrojtjen e të Dhënave Personale.