

**Republika e Kosovës**

**Republika Kosova-Republic of Kosovo**

***Qeveria-Vlada-Government***

**PROJEKTLIGJI PËR MBROJTJEN E INFORMACIONIT TË KLASIFIKUAR**

**DRAFT LAW ON PROTECTION OF CLASSIFIED INFORMATION**

**NACRT ZAKONA O ZAŠTITI KLASIFIKOVANIH INFORMACIJA**

|  |  |  |
| --- | --- | --- |
| **Kuvendi i Republikës së Kosovës,**Në mbështetje të Nenit 65 (1) të Kushtetutës së Republikës së Kosovës, Miraton:**LIGJ PËR MBROJTJEN E INFORMACIONIT TË KLASIFIKUAR****KREU I** **DISPOZITAT E PËRGJITHSHME****Neni 1****Qëllimi**1. Qëllimi i këtij ligji është themelimi i një sistemi unik për mbrojtjen e informacionit të klasifikuar që kanë të bëjnë me interesat e sigurisë së Republikës së Kosovës.2. Me këtë ligj themelohet Agjencia për Mbrojtjen e Informacionit të Klasifikuar (ne tekstin e metejme: (AMIK) ku përcaktohet misioni, organizimi, funksionimi, detyrat dhe përgjegjësitë e saj3. Ky ligj eshte ne harmoni me legjislacionin e BE-së, si në vijim:3.1 - Vendimi i Këshillit të 23 shtatorit 2013 mbi rregullat e sigurisë për mbrojtjen e informacionit të klasifikuar të BE-së;3.2 Rregullorja (BE) 2016/679 e Parlamentit Evropian dhe e Këshillit e datës 27 prill 2016 për mbrojtjen e personave fizikë në lidhje me përpunimin e të dhënave personale dhe lëvizjen e lirë të këtyre të dhënave dhe shfuqizimin e Direktivës 95/46 / EC (Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave) **Neni 2****Fushëveprimi** Ky ligj zbatohet për të gjitha institucionet publike që ushtrojnë kompetenca ekzekutive, legjislative dhe gjyqësore, për personat fizik dhe juridik, që bazuar në parimin e nevojës për njohje, në ushtrimin e detyrës mund të kenë qasje në informacionin e klasifikuar të Republikës se Kosovës, shteteve dhe organizatave tjera ndërkombëtare.**Neni 3****Përkufizimet**1. Shprehjet e përdorura në ketë ligj kanë këto kuptime:1.1. **Informacion i klasifikuar,** është çdo dokument ose material, pavarësisht nga forma, natyra ose mënyra e transmetimit të tij, i përgatitur ose që përgatitet, për të cilin është vendosur një nivel i caktuar klasifikimi në interes të sigurisë së Republikës së Kosovës dhe në përputhje me legjislacionin në fuqi që kërkon mbrojtje ndaj çdo shkeljeje, përvetësimi, përhapjeje, humbjeje ose qasje të ndonjë individi të paautorizuar dhe të çdo lloj tjetër komprometimi sigurie;1.2. **Qasje -** aftësinë apo mundësinë për të marrë njohuri rreth informacionit të klasifikuar;1.3. **Nevojë për njohje -** është nevoja për të pasur qasje tek informacioni i klasifikuar, në kuadrin e një pozicioni të caktuar dhe me qëllim përmbushjen e një detyre specifike;1.4. **Klasifikim** - akti apo procesi përmes të cilit një informacioni i përcaktohet niveli i klasifikimit dhe afati i ruajtjes së këtij klasifikimi;1.5. **Agjenci -** Agjencia për Mbrojtjen e Informacionit të Klasifikuar (AMIK);1.6. **Autoritet i Sigurimit Kombëtar**, është autoriteti i brendshëm shtetëror i një shteti përgjegjës për kontrollin dhe zbatimin e standardeve të sigurimit të informacionit të klasifikuar. AMIK është Autoritet i Sigurimit Kombëtar në Republikën e Kosovës. 1.7. **Autoritet verifikues**, është Agjencia për Mbrojtjen e informacionit të klasifikuar. , si njësi strukturore e specializuara për kryerjen e verifikimeve të sigurisë ndaj individëve që do të njohin, do të prodhojnë, do të ruajnë, do të administrojnë, do të transportojnë dhe do të transmetojnë informacion të klasifikuar; 1.8. **Pyetësori i sigurisë**, është formulari që plotëson çdo individ që kërkon të njihet me informacion të klasifikuar dhe mbi bazën e të cilit kryhet verifikimi i sigurisë si dhe vlerësohen të dhënat për të lëshuar ose jo “Certifikatën e Sigurimit të Personelit”. 1.9. **Certifikata e Sigurimit të Personelit (**CSP), është dokumenti zyrtar i AMIK-ut ose i një autoriteti kompetent të sigurisë së një vendi tjetër, i cili vërteton nga pikëpamja e sigurisë se një individ i plotëson kushtet e përcaktuara për njohjen, ruajtjen, administrimin dhe transferimin e informacionit të klasifikuar. 1.10. “**Brifimi”/“Debrifimi**”, janë tërësi instruksionesh dhe udhëzimesh sigurie lidhur me procedurat e sigurimit të informacionit të klasifikuar dhe përgjegjësitë individuale për shkeljet e rregullave të sigurisë, të cilave u nënshtrohen individët që kërkojnë të kenë mundësinë për njohje të informacionit të klasifikuar ose janë të pajisur me CSP. 1.11 **Shkelje sigurie**, është një veprim ose mosveprim në kundërshtim me përcaktimet e legjislacionit në fuqi që rezulton ose mund të rezultojë në vjedhjen, humbjen, dëmtimin, komprometimin apo përhapjen e paautorizuar të informacionit të klasifikuar. 1.12 **Verifikimi i sigurisë**, është tërësia e masave dhe e procedurave të aplikuara ndaj një personi fizik apo juridik , mbi bazën e të cilave do të vlerësohet lëshimi, refuzimi, pezullimi i përkohshëm ose heqja e “Certifikatës së Sigurimit të Personelit”. 1.13 **Rrezik i papranueshëm sigurie**, konsiderohen rrethanat e përshkruara në këtë Ligj , në bazë të të cilave AMIK-u refuzon dhënien e CSP-së ose vlerëson se duhet të ndërmarrë masën e heqjes ose të pezullimit të përkohshëm të saj. 1.14 **Rrethana të urgjencës së jashtëzakonshme**, konsiderohen kushtet e pamundësisë objektive për të ndjekur procedurat normale të pajisjes me CSP, për shkak të ushtrimit të një detyre afatshkurtër zyrtare të pjesëmarrjes në një aktivitet të paparashikuar ndërkombëtar, zgjatjes së afateve të misioneve ushtarake në vende të ndryshme etj. 1.15 **Oficer sigurie**, në vazhdim OS, është punonjësi përgjegjës ose struktura e ngarkuar nga titullari i ministrisë apo i institucionit shtetëror për mbikëqyrjen dhe zbatimin e kërkesave për sigurimin e personelit dhe disiplinat e tjera të informacionit të klasifikuar;1.16 **Operator Ekonomik** - është cdo person fizik ose juridik, ose çdo grup personash të tillë që ofrojnë në treg furnizimin me mallra, punime dhe/ose shërbime;.1.17 **Autoritet i Klasifikimit** – Presidenti, Kryetari i Kuvendit Kryeministri Kryetari i Gjykates Supreme dhe Kryeprokurori i Shtetit, Drejtori i AKI-së, Ministri i Punëve të Brendshme, Ministri i MFSK-së, Komandanti i FSK-së, Drejtori i Përgjithshëm i Policisë si dhe çdo person i autorizuar nga ta që ka kompetencë origjinere apo të deleguar për të klasifikuar informacione,1.18 **Kontratë e klasifikuar -** çdo kontratë të lidhur nga një institucion publik që përmban informacione të klasifikuara sipas këtij ligji;1.19 **Deklasifikim -** ndryshimin e autorizuar të statusit të informacioneve nga informacioni i klasifikuar në informacion të paklasifikuar;1.20 **Dokument -** çdo mjet fizik apo elektronik mbi të cilin është regjistruar informacioni.1.21 **Degradim -** vendimin që informacioni i klasifikuar dhe i ruajtur në një nivel të përcaktuar klasifikohet dhe ruhet në nivel më të ulët klasifikimi.1.22 **Informacion i Qeverisë së huaj** nënkupton:1.22.1. informacioni i dhënë Republikës së Kosovës nga një qeveri e huaj apo organizatë qeveritare ndërkombëtare; 1.22.2. informacioni i prodhuar nga Republika e Kosovës në pajtim me, apo si rezultat i një marrëveshje të përbashkët me një qeveri të huaj apo organizatë qeveritare ndërkombëtare me pritjen apo kërkesën që një informacion, marrëveshje e tillë apo të dyja të mbahen sekret.1.23. **Material -** dokumente si dhe çdo makineri, pajisje ose armatim që është prodhuar apo që është në prodhim e sipër.1.24. **Përpunim -** çdo veprim apo sërë veprimesh që bëhen ndaj të dhënave personale, me apo pa mjete automatike, siç është mbledhja, regjistrimi, organizimi, ruajtja, adaptimi apo ndryshimi, kërkimi, konsultimi, shfrytëzimi, publikimi me transmetim, përhapja apo çdo formë tjetër e vënies në dispozicion, rreshtimit apo kombinimit, bllokimit, shlyerjes apo asgjësimit.1.25. **Institucion publik -** të gjitha institucionet dhe organet e përcaktuara në nenin 2.1 të këtij ligji.1.26. **Interesat e sigurisë -** i referohet mbrojtjes, veprimtarive të zbatimit te ligjit dhe zbulimit, marrëdhënieve me jashtë apo të sigurisë të Republikës së Kosovës, përfshirë integritetin e saj territorial, integritetin e institucioneve të saja, rregullin kushtetues si dhe stabilitetin dhe zhvillimin ekonomik.1.27**. Bashkëshort/e -** çdo marrëdhënie të krijuar përmes martesës së ligjshme dhe për nevojat e këtij ligji përfshinë edhe çdo marrëdhënie jashtëmartesore midis dy personave fizikë.1.28 **Titullar i institucionit publik -** zyrtarët e zgjedhur në pozita zgjedhëse në institucionet publike dhe zyrtaret e emëruar nga zyrtarët e zgjedhur.1.29. **Bartësit e autorizuar të informacioneve të klasifikuara -** personi i cili ka në posedim informacionin e klasifikuar, ka CSP të vlefshme të sigurisë dhe i plotëson kushtet tjera që lejojnë qasjen në informacionin e klasifikuar, përveç nëse përcaktohet ndryshe me ligj.1.30 “**Autoritet Kontraktues**”, është çdo subjekt shtetëror, që merr përsipër të bëjë një prokurim të klasifikuar dhe të hyjë në marrëdhënie kontraktuale. 1.31 “**Operator Ekonomik**”, është çdo Person Fizik, ose Juridik, ose çdo grup personash të tillë, që ofrojnë në treg furnizimin me mallra, punime dhe/ose shërbime. 1.32 “**Kontratë e Klasifikuar**”, është çdo kontratë, nënkontratë, zbatimi i së cilës kërkon qasje tek informacioni i klasifikuar, ose përdorimin, ruajtjen, administrimin, qarkullimin, transmetimin dhe transportimin e informacionit, ose materialit të klasifikuar. 1.33 “**Palë Kontraktuese**”, është çdo Person Fizik, ose Juridik, që ka zotësinë juridike për të negociuar dhe lidhur kontrata të klasifikuara.1.34 **Certifikata e sigurisë së personelit –** është dokumenti zyrtar i AMIK-ut, ose i një Autoriteti Kompetent të Sigurisë së një vendi tjetër, i cili vërteton, nga pikëpamja e sigurisë, se një person fizik paraqet rrezik të pranueshëm për qasje në informacione të klasifikuara1.35 “**Certifikata e Sigurimit Industrial**”, me tej CSI është dokumenti zyrtar i AMIK-ut, ose i një Autoriteti Kompetent të Sigurisë së një vendi tjetër, i cili vërteton, nga pikëpamja e sigurisë, se një operator ekonomik, ka kapacitetet dhe aftësitë organizative, teknike, fizike dhe i plotëson standardet e përcaktuara për njohjen, ruajtjen dhe administrimin e informacionit të klasifikuar, në një projekt/program, apo kontratë/nënkontratë të klasifikuar.**KREU II - SIGURIMI I INFORMACIONIT****Neni 4****Autoriteti Klasifikues**1. Autoriteti për klasifikimin e informacionit ushtrohet nga:* 1. Presidenti
	2. Kryetari i Kuvendit
	3. Kryeministri

1.4 Kryetari i Gjykates Supreme 1.5 Kryeprokurori i Shtetit1.6 Drejtori i AKI-së1.7 Ministri i Punëve të Brendshme1.8 Ministri i MFSK-së1.9 Komandanti i FSK-së* 1. Drejtori i Përgjithshëm i Policisë

2. Autoritetet per klasifikimin e informacionit të parapara në paragrafin 1 të këtij neni, kanë të drejtë të bartin kompetencen e klasifikimin tek drejtuesit e institucioneve ne vartesi të tyre.3. Kërkesa për dhënien e autorizimit nga Autoriteti klasifikues i dërgohet AMIK-ut, e cila pas shqyrtimit dhe vlerësimit, rekomandon për dhënien ose jo të autorizimit.4. Çdo autorizim i kompetencës për klasifikim bëhet me shkrim dhe e identifikon qartë titullarin me emër dhe titull të pozitës dhe ky autorizim vlen vetëm për kohën sa është titullar i institucionit përkatës.5. Çdo titullar i institucionit përkatës nuk mund të bëjë klasifikimin e informacionit të institucionit dhe njësive përkatëse në varësi të tij, pa marrë autorizimin nga Autoriteti Klasifikues.6. Agjencia harton, mirëmbanë dhe rregullisht e përditëson një regjistër me emrat e titullarëve që kanë kompetencë klasifikimi.**Neni 5****Kategoritë e Informacionit që klasifikohen**1. Informacioni klasifikohet vetëm nëse është e nevojshme dhe nëse bie brenda një apo më shumë prej këtyre kategorive: 1.1 projekte ,plane sisteme apo operacione që kanë të bëjnë me mbrojtjen dhe sigurinë e rendit Kushtetues të Republikës së Kosovës;1.2 informacion i qeverive të huaja, marrëdhënie apo veprimtari ndërkombëtare të Republikës së Kosovës, të cilat do të mbrohen nga ekspozimi i pa autorizuar.1.3 veprimtari, burime informative dhe metoda të Institucioneve të inteligjencës që lidhen me sigurinë e Republikës së Kosovës.1.4 sisteme, instalime, infrastruktura, projekte, plane apo shërbime të mbrojtjes që lidhen me interesat e sigurisë të Republikës së Kosovës; 1.5 veprimtari shkencore, teknologjike, ekonomike, financiare që lidhen me interesat e sigurisë së Republikës së Kosovës; 1.6 sistemet kriptologjike; çështjet/problemet kriptologjike1.7. plane operimi dhe përdorimi të sistemit të komunikimit të informacioneve të klasifikuara dhe kriptologjisë;1.8. vlerësimet e rrezikut/raporte inspektimi lidhur me mangësitë të sistemit të kriptologjisë;1.9. plane për identifikimin, zvogëlimin dhe menaxhimin e rrezikut që paraqitet në sistemin e komunikimit elektronik.1.10. plane, projekte, programe për sigurimin e sistemeve të komunikimit të informacionit të klasifikuar;1.11. informacionet e mbledhura nëpërmjet operacioneve specifike dhe interceptimeve elektronike.**Neni 6****Ndalimi i klasifikimit të informacionit**1. Ndalohet klasifikimi i informacionit kur ai bëhet me qëllim që:1.1. të fshehë shkeljet e ligjit, keqperdorimin e autoritetit, mos efikasitetin apo gabimin administrativ; 1.2. ti privojë të drejtën e njohjes një personi, organizate apo institucioni;1.3. të pengojë apo të vonojë dhënien e informacionit qe nuk kërkon mbrojtje në interes të sigurisë së Republikës së Kosovës.1.4. të ndalojë konkurrencën.**Neni 7****Nivelet e Klasifikimit**1. Informacioni nisur nga përmbajtja, vlera dhe interesi shtetëror klasifikohet në njërin nga këto nivele: 1.1. “TEPËR SEKRET”, përhapja dhe publikimi i paautorizuar i të cilit sipas vlerësimit të arsyeshëm do të shkaktonte dëm jashtëzakonisht të rëndë për interesat e sigurisë së Republikës së Kosovës; 1.2. “SEKRET”, përhapja dhe publikimi i paautorizuar i të cilit do t’i dëmtonte seriozisht interesat e sigurisë së Republikës së Kosovës; 1.3. “KONFIDENCIAL”, përhapja dhe publikimi i paautorizuar i të cilit do të mund t’i dëmtonte interesat e sigurisë së Republikës së Kosovës; 1.4. “I KUFIZUAR”, përhapja dhe publikimi i paautorizuar i të cilit do të ishte e pafavorshme për interesat e sigurisë së Republikës së Kosovës. 2. Autoriteti i Klasifikimit i shmanget klasifikimit të tepërt të informacioneve dhe atyre u cakton vetëm nivel të tillë të klasifikimit që është i nevojshëm për të ruajtur interesat e Republikës së Kosovës.3. Procedurat e klasifikimit të informacioneve, duke përfshirë edhe klasifikimin e pjesëve të dokumenteve, dokumenteve të ndara dhe shënjëzimet që mbajnë informacionet e klasifikuara përcaktohen me akt nënligjor që propozohet nga AMIK dhe miratohet nga Qeveria.**Neni 8****Kohëzgjatja e klasifikimit**1. Informacioni klasifikohet për aq kohë sa e kërkon interesi i sigurisë së Republikës së Kosovës.2. Afatet e ruajtjes së klasifikimit janë:2.1. informacioni i klasifikuar: “I KUFIZUAR” një (1) vit; 2.2. informacioni i klasifikuar: “KONFIDENCIAL” pesë (5) vite; 2.3. informacioni i klasifikuar: “SEKRET” pesëmbëdhjetë (15) vite; dhe 2.4. informacioni i klasifikuar: “TEPËR SEKRET” pesëdhjete (50) vite. 3. Llogaritja e afateve të ruajtjes së klasifikimit fillon nga data e prodhimit të informacionit të klasifikuar.4. Në rast se Autoriteti Klasifikues konsideron se informacioni duhet të mbrohet më gjatë se sa që është paraparë në paragrafin 2 ai nxjerr vendim të ri për klasifikim në pajtim me nenin 8 të këtij ligji. Vendimi i tillë nuk guxon të merret më herët se gjashtë (6) muaj para datës së paraparë për deklasifikim sipas paragrafit 1. të këtij neni.**Neni 9****Kushtet për prodhim, shfrytëzim dhe qarkullim të informacionit të klasifikuar**1. Prodhimi i informacionit të klasifikuar bëhet vetëm duke u bazuar në listën e informacionit të klasifikuar të aprovuar nga autoriteti klasifikues, në pajtim me procedurën e përcaktuar me legjislacionin në fuqi2. Prodhimi, shfrytëzimi, shumëfishimi, transferimi, transportimi fizik, arkivimi, ruajtja dhe shkatërrimi i informacionit të klasifikuar bëhet në përputhje me standardet si në vijim: 2.1. Siguria e personelit;2.2. Siguria fizike;2.3. Siguria e informacionit;2.4. Siguria industriale;2.5. Siguria e sistemeve të komunikimit të informacionit.3. Procedurat për zbatimin e këtij neni, rregullohen me akt nënligjor të propozuar nga AMIK dhe të miratuar nga Qeveria.**Neni 10****Deklasifikimi**1. Informacioni deklasifikohet atëherë kur nuk ka më nevojë për mbrojtje dhe kur publikimi i tij nuk përbën më rrezik për sigurinë e Republikës së Kosovës2. Autoriteti i Klasifikimit, nga i cili informacioni i klasifikuar e ka origjinën, e bën deklasifikimin e saj. 3. Rastet e deklasifikimit të informacionit të klasifikuar janë:3.1 kur publikimi i tij diktohet nga interesat shtetërorë më të rëndësishme se nevoja për ta mbajtur të klasifikuar;3.2 ndodhinë e një ngjarje apo të një date të veçantë siç përcaktohet nga autoriteti i klasifikimit. 4. Përhapja dhe publikimi i paautorizuar i informacionit të klasifikuar nuk përbën shkak për deklasifikimin e tij.5. Autoriteti klasifikues i cili ka bërë deklasifikimin e informacionit obligohet ti njofton të gjitha institucionet të cilat e kane ne posedim informacionin e klasifikuar;6. Procedurat për zbatimin e këtij neni, rregullohen me akt nënligjor të propozuar ngaAMIK dhe te miratuar nga Qeveria.**Neni 11****Asgjësimi dhe shkatërrimi i informacionit të klasifikuar**1. Në çdo institucion shtetëror titullari i institucionit apo i autorizuari i tij krijon komisionet për asgjësimin dhe shkatërrimin e informacionit të klasifikuar.2. Komisioni për asgjësim shqyrton dhe vendos për asgjësimin e informacionit të klasifikuar kur ky informacion nuk ka vlerë për ruajtje të mëtutjeshme, dhe nuk duhet të deklasifikohet.3. Komisioni për shkatërrim duke u bazuar në vendimin e Komisionit për asgjësim, kryen të gjitha procedurat për shkatërrimin e informacionit të klasifikuar, dhe përgatit raportin përfundimtar. 4. Informacioni i cili duhet të dorëzohet në rrjetin arkivor nuk duhet të asgjësohet dhe shkatërrohet, por deklasifikohet.5. Procedurat për zbatimin e këtij neni, rregullohen me akt nënligjor të propozuar nga AMIK dhe te miratuar nga Qeveria.**Neni 12****Degradimi dhe Ngritja e Nivelit të Klasifikimit**1. Autoriteti i klasifikimit, nga i cili e ka origjinën informacioni i klasifikuar, është përgjegjës për degradimin ose ngritjen e nivelit të klasifikimit të një informacioni të tillë.2. Autoriteti kompetent i klasifikimit e degradon ose ngrit nivelin e klasifikimit nëse njoftohet për fakte që tregojnë qartë që informacioni i klasifikuar nuk kërkon nivelin e mbrojtjes i cili akordohet në nivelin ekzistues të klasifikimit. **Neni 13****Propozimi i shtetasve**1. Kur një shtetas apo nëpunës i Republikës së Kosovës, që nuk ka autoritet klasifikimi, vlereson se një informacion i caktuar nën kontrollin e shtetit, ka vlerat e nevojshme për t'u klasifikuar, i propozon institucionit përkatës klasifikimin e këtij informacioni. Ky institucion vendos brenda 10 ditëve, nëse informacioni do të klasifikohet ose jo dhe njofton shtetasin apo nëpunësin për vendimin e marrë.2. Nga momenti i propozimit për klasifikimin e informacionit përkatës, poseduesi i tij obligohet ta mbron informacionin nga qasja e paautorizuar**KREU III - SIGURIA E PERSONELIT** **Neni 14****Siguria e personelit**1. Siguria e personelit, është tërësia e masave dhe e procedurave mbi bazën e të cilave vlerësohet nëse një person, duke ju përmbajtur besnikërisë, besueshmërisë dhe sigurisë së tij, mund të autorizohet për të patur qasje tek informacioni i klasifikuar, pa e rrezikuar sigurinë e këtij informacioni.2. Lëshimi, refuzimi, pezullimi i përkohshëm ose revokimi i “Certifikatës së Sigurimit të Personelit” (në tekstin e mëtëjmë: CSP), bëhet në pajtim me paragrafin 1 të këtij neni.3. Procedurat për zbatimin e këtij neni rregullohen me akt nënligjor të miratuar nga Qeveria.**Neni 15****Certifikata e Sigurisë se Personelit** 1. Autoritetit Verifikues ia lëshon CSP vetëm atij personi i cili pas kryerjes te një procedure te verifikimit te sigurisë ne pajtim me legjislacionin ne fuqi është përcaktuar si rrezik i pranueshëm për sigurinë.2.CSP tregon qarte nivelin e informacionit te klasifikuar, ne te cilën personi qe e ka kaluar procedurën e verifikimit te sigurisë mund te këtë qasje. CSP për një nivel te caktuar te klasifikimit i jep bartësit qasje edhe ne informacionet me nivel me te ulet te klasifikimit 3.Çdo titullar i institucionit publik obligohet qe brenda 15 diteve te zbatoj vendimin e Autoritetit Verifikues dhe nuk jep qasje ne informacione te klasifikuar nje personi te cilit i është refuzuar CSP.**Neni 16****Kriteret për njohjen e informacionit të klasifikuar**1. Të drejtë për njohjen, ruajtjen, administrimin dhe transferimin e informaciont të klasifikuar e kane vetëm personat, që: 1.1 sigurojnë të drejtën e njohjes nga titullari i institucionit ose Oficeri i Sigurimit Industrial i Kontraktorit për shkak të detyrës që kryejnë; * 1. kanë zotësi të plotë për të vepruar;

1.3 jane te informuar më parë për njohjen e procedurave të sigurisë së informacionit të klasifikuar dhe të përgjegjësive individuale për shkeljet e sigurisë dhe te kete nenshkruar deklaraten e ruajtjes se informacionit;  1.4 janë të pajisur me CSP, me përjashtim të rasteve për njohjen me informacionin e klasifikuar në nivelin “I kufizuar”.2. Vetëm Presidenti i Republikës së Kosovës, Kryetari i Kuvendit si dhe Kryeministri janë të autorizuar të kenë qasje në informacione të klasifikuara me qëllim të kryerjes së detyrës zyrtare të tyre pa i pambushur kërkesat e përcaktuara ne paragrafin 1 te këtij neni, me kusht qe te kenë nevoje për te qene ne dijeni te këtyre informacioneve.**Neni 17****Listat e funksioneve/pozitave për njohjen e informacionit të klasifikuar** 1. Institucionet shtetërore të cilat, për shkak të veprimtarisë që kryejnë, prodhojnë informacion të klasifikuar ose gjatë bashkëpunimit me institucione të tjera e përfitojnë këtë kategori informacioni, kanë për detyrë të miratojnë dhe të dërgojnë me shkrim në AMIK listën e funksioneve/pozitave që për shkak të detyrave zyrtare mund të njihen me informacionin e klasifikuar dhe nivelin përkatës të CSP-së.2. Rishikimi i këtyre listave bëhet periodikisht dhe në përputhje me ndryshimet e strukturës organizative të institucionit përkatës. Për cdo ndryshim eventual obligohet titullari i institucionit që ta njoftoj AMIK-un.**Neni 18****Kushtet për fillimin e verifikimit të sigurisë**1. Verifikimi i sigurisë fillon vetëm pasi personi aplikues ka pranuar dhe ka dhënë pëlqimin me shkrim që të mblidhen të dhëna dhe të kryhen procedurat e verifikimit të sigurisë, sipas kërkesave të pyetësorit të sigurisë. 2. Trajtimi i të dhënave personale dhe i informacioneve të grumbulluara në procesin e verifikimit të sigurisë kryhet në përputhje me kërkesat e legjislacionit në fuqi për mbrojtjen e të dhënave personale.**Neni 19****Kërkesat e përgjithshme të vlerësimit të sigurisë****1.** AMIK-u, si Autoritet i vetëm Verifikues ne Republikën e Kosovës përgjegjës për zhvillimin e procedurës se verifikimit te sigurisë duhet t’iu përmbahet kërkesave të përgjithshme të vlerësimit të sigurisë, të cilat janë, si më poshtë por nuk kufizohet në:  1.1.Verifikimi i saktë i identitetit, gjeneraliteteve dhe statusit të shtetësisë, në të shkuarën dhe të tashmen, për çdo person;1.2. Kontrolli i të dhënave, në funksion të sigurisë së Republikës së Kosovës. 1.3. Statusi financiar i aplikantit, me qëllim verifikimi, nëse ai mund të ndodhet nën presion për shkak të paqëndrueshmërisë, vështirësive serioze financiare apo të zotërimit të ndonjë pasurie të pajustifikuar. 1.4. Informacioni për edukimin arsimor të personit pas moshës 18-vjeçare ose për periudhën e gjykuar si të përshtatshme nga autoriteti verifikues 1.5. Informacioni për punësimin e individit duke marrë në konsideratë referencat e punëve të mëparshme, bazuar në raportet e punëdhënësve.  1.6. Informacioni për pjesëmarrjen në operacione ushtarake apo kohëzgjatjen e shërbimit në forcat e armatosura. 1.7. Vlerësimi i përgjithshëm, nëse personi mund të vihet nën presion nga një forcë e huaj jomiqësore. **Neni 20****Kriteret themelore të vlerësimit të sigurisë**1. Kriteret themelore, mbi bazën e të cilave vlerësohet ekzistenca ose jo e rrezikut të papranueshëm të sigurisë për informacionet e klasifikuara që shërbejnë si bazë për të lëshuar, pezulluar apo refuzuar pajisjen ose mbajtjen e mëtejshme të një CSP-je, janë rastet kur një individ rezulton se: 1.1. ka qenë, është ose tenton të angazhohet fshehurazi, vetëm, në bashkëpunim apo në përbërje të një organizate ilegale, në veprimtari spiunazhi, terrorizmi, tradhtie, rebelimi apo dhune të armatosur ndaj rendit kushtetues apo ka nxitur aktivisht dikë të kryejë veprimtari spiunazhi, terrorizmi, tradhtie, rebelimi apo dhune të armatosur ndaj rendit kushtetues; 1.2. është apo ka qenë bashkëpunëtor në spiunazh, terrorizëm, tradhti, rebelim apo dhunë të armatosur ndaj rendit kushtetues, ka dyshime të ketë qenë i tillë apo bashkëpunëtor i përfaqësuesve të organizatave, shteteve të huaja, duke përfshirë këtu shërbimet e inteligjencës të cilat mund të cenojnë sigurinë e vendit tonë dhe/ose të shteteve anëtare të NATO-së, BE-së, përveç rasteve kur këto bashkëpunime janë të autorizuara për shkak të detyrës; 1.3. është apo ka qenë anëtar i një organizate, e cila me mjete të dhunshme, armiqësore, të paligjshme, ka qëllim të rrëzojë qeverinë apo të ndryshojë rendin kushtetues; 1.4. është apo ka qenë mbështetës i një organizate të përshkruar si në pikën 1.3, të këtij neni, ose është apo ka qenë i/e lidhur ngushtë me ndonjë anëtar të një organizate të tillë; 1.5. qëllimisht ka fshehur, ka keq prezantuar apo ka falsifikuar një informacion të një rëndësie të madhe, të një natyre sigurie të veçantë apo qëllimisht ka gënjyer gjatë plotësimit të pyetësorit të sigurisë apo intervistës së sigurisë; 1.6. rezulton i dënuar për një ose më shumë vepra penale te kryera me dashje. 1.7. ka një historik varësie nga alkooli, përdorimi i drogave të jashtëligjshme, apo keqpërdorimi i drogave të ligjshme; 1.8. ka sjellje të keqe, tendenca kriminale e përfshirje në krim të organizuar, gjë që sjell rrezikun e dobësisë përballë shantazhit apo mund të influencohet seriozisht nga presione të ndryshme; 1.9. me anë të veprimeve konkrete ka shprehur mungesë besnikërie, besueshmërie dhe sigurie; 1.10. ka kryer shkelje sigurie apo në mënyrë të përsëritur ka nëpërkëmbur rregullat e sigurisë së informacionit të klasifikuar apo ka tentuar dhe ka arritur të kryejë aktivitet të paautorizuar në sistemet e komunikimit të informacionit të klasifikuar; 1.11. vuan nga çrregullime mendore kronike. **Neni 21** **Intervista e sigurisë**1. AMIK mund te zhvillojë intervista me persona të cilët kanë aplikuar për t’u pajisur me CSP dhe në drejtim të tyre janë ndërmarrë procedurat e verifikimit të sigurisë. 2. AMIK mund te zhvillojë intervista me persona të tretë të paanshëm, të cilët njohin të shkuarën dhe aktivitetet e personit që i është nënshtruar verifikimit të sigurisë.**Neni 22****Vlefshmeria e CSP**1. CSP e nivelit TEPER SEKRET vlenë për periudhën 5 vjecare2. CSP e nivelit SEKRET vlenë për periudhën 7 vjecare.3. CSP e nivelit KONFIDENCIAL vlenë për periudhën 10 vjecare**Neni 23****Zgjatja e afatit të CSP-së në rrethanat e urgjencës së jashtëzakonshme**1. Në kushtet e rrethanave të urgjencës së jashtëzakonshme, AMIK-u ka të drejtë të zgjatë afatin e CSP-së së një individi vetëm një herë, deri në 60 ditë kalendarike gjatë ciklit të vlefshmërisë së saj, me kushtet e mëposhtme: Te 1.1 Individi, për të cilin kërkohet zgjatja e afatit, duhet të mbajë një CSP të vlefshme, lëshuar me procedurë të plotë. Përjashtohen rastet e zgjatjes së afateve për një CSP e cila është e lëshuar në kushtet e rrethanave të urgjencës së jashtëzakonshme. 1.2 Ekziston një kërkesë zyrtare që sqaron rrethanat e urgjencës së jashtëzakonshme dhe provon rrethanat e pamundësisë për të aplikuar sipas procedurave normale për ripajisjen me CSP të re, kur: 1.3 një individ ndodhet në kushtet e ushtrimit të një detyre afatshkurtër zyrtare, për të cilën ka qenë e pamundur ndjekja e procedurave, sipas afateve kohore të parashikuara;1.4 një individ ka nevojë për pjesëmarrje në një aktivitet të paparashikuar ndërkombëtar, për të cilin ka qenë e pamundur ndjekja e procedurave, sipas afateve kohore të parashikuara;1.5 një individ, i cili ka qenë i pajisur me CSP, ndodhet në kushtet e zgjatjes së afateve të pjesëmarrjes në misione ushtarake jashtë vendit dhe të pamundësisë për të aplikuar, sipas procedurave normale për ripajisjen me CSP të re. Zgjatja e afateve të CSP-së me kushtëzimet e sipërpërmendura lejohet për CSP-në e nivelit “Konfidencial”, “Sekret” dhe “Tepër sekret”.2. Te gjithe individeve te cileve ju eshte vazhduar CSP ne rrethanat dhe kushtet e jashtezakonshme, obligohen qe ne forme te shkruar te deklarohen se i kane kuptuar te gjitha obligimet e tyre per ruajtjen e informacionit te klasifikuar.**Neni 24****Përsëritja e Verifikimit të Sigurisë**1. Personat të cilëve u është lëshuar CSP i nënshtrohen një verifikimi të ri të sigurisë në intervalet e rregullta si në vijim: 1.1. çdo dhjete (10) vjet për personat me CSP të sigurisë që u lejon atyre qasje në informacionet e klasifikuara ne nivelin “KONFIDENCIALE”; 1.2. çdo shtate (7) vjet për personat me CSP që u lejon atyre qasje në informacionet e klasifikuara ne nivelin“SEKRET” 1.3 çdo pesë (5) vjet për personat me CSP që u lejon atyre qasje në informacionet e klasifikuara ne nivelin “TEPËR SEKRET”. 2. Autoriteti Verifikues apo drejtuesi i institucionit publik, ku personi i verifikuar është i punësuar, mund t’i kërkojë këtij personi që t’i nënshtrohet një procedure të re të verifikimit të sigurisë madje edhe para skadimit të vlefshmërisë së CSP nëse ai/ajo ka indikacione që kanë ndodhur ngjarje apo janë paraqitur rrethana që ngrisin dyshim nëse personi i verifikuar ende përbën rrezik të pranueshëm për sigurinë.**Neni 25****Refuzimi, heqja dhe pezullimi i përkohshëm i CSP-së****1.** AMIK-u merr vendim për refuzimin, heqjen ose pezullimin e përkohshëm të CSP-së, në rastet kur ka pranuar informacion, sipas të cilit vlerësohet se pajisja ose mbajtja e mëtejshme e CSP-së nga një person i caktuar përbën rrezik të papranueshëm sigurie, referuar kritereve të përgjithshme dhe themelore të vlerësimit të sigurisë. 2. Njoftimi për vendimin e marrë nga AMIK-u për refuzim, heqje ose pezullim të përkohshëm të CSP-së i komunikohet me shkrim titullarit institucionit përkatës publik i cili ka iniciuar kërkesën për zhvillimin e procedurës se verifikimit te sigurisë.**Neni 26****E drejta e Ankesës** 1. Personit te cilit iu ka refuzuar Certifikata e Sigurise se Personelit ka te drejt te ushtroj ankese prane AMIK brenda afatit 15 dite nga data e pranimit te njoftimit; 2. Ankesa shqyrtohet nga Komisioni i Ankesave;**Neni 27****Komisioni i Ankesave** 1. Komisioni i Ankesave përbehet nga 5 anëtarë me nga një përfaqësues te institucioneve te mëposhtme:* 1. Ministria e FSK së
	2. Ministria e Puneve te Brendshme
	3. Këshilli Prokurorial i Kosovës
	4. Këshilli Gjyqësor i Kosovës;
	5. Agjencia e Kosoves per Inteligjencë

2. Me propozim te titullarve te institucioneve perkatse Qeveria me vendim themelon Komision e ankesave3. Personi i autorizuar nga AMIK bene prezantimin e rastit para anetareve te Komisionit te ankesave  4. Mandati i anëtareve te komisionit është 3 vjet dhe me mundësi vazhdimi5. Anëtarët e komisionit te ankesave duhet jene profesional, me integritet te larte dhe te posedojnë CSP te nivelit adekuat me informacionet qe do te shqyrtohen gjate procedurës se ankesës6. Komisioni i ankesave pasi ta këtë shqyrtuar ankesën rekomandon Drejtorin e AMIK për marrjen e një vendimi.7. Rregullat dhe procedurat e punës se komisionit te ankesave dhe çështjet tjera ne lidhje me shqyrtimin e ankesave rregullohet me akt nenligjor te propozuar nga AMIK dhe te miratuar nga qeveria**Neni 28****Afatet dhe kohëzgjatja që mbulon verifikimin e sigurisë**1. Afati i përgjithshëm për kryerjen e procedurave të verifikimit dhe lëshimit të CSP-së nga AMIK-u është deri në 120 ditë kalendarike.
2. Ky afat mund të jetë më i gjatë kur verifikimet kushtëzohen nga kryerja e procedurave në bashkëpunim me autoritetet e sigurimit kombëtar të vendeve të tjera.

3. Verifikimi i sigurisë mbulon një periudhë jo më pak se 10 vitet e fundit. Kur kjo periudhë është e pamjaftueshme, verifikimi shtrihet nga mosha 18 vjeç deri në moshën aktuale. 4. Ne rast se Autoriteti Verifikues nuk ka mundësi te mbledh dhe te përpunoj te gjitha informacionet e kërkuara qe te kryhet verifikimi i sigurisë brenda afateve kohore te përcaktuara ne paragrafin 1 te këtij neni Autoriteti Verifikues me vendim mund te zgjasë afatin kohore deri ne 60 dite kalendarik. Me vendimin e marre njoftohet drejtuesi i institucionit perkates.**Neni 29****Detyrimi i personave fizik per mbrojtjen e informacionit te klasifikuar**1. Çdo person ka për detyrë të mbrojë informacionet e klasifikuara sipas këtij ligji, pavarësisht se si i është dhënë qasja në to apo se si e ka pranuar, apo në çfarëdo forme tjetër, ka arritur të posedojë informacione të klasifikuara. 2. Me rastin e largimit nga institucioni publik, shkëputjes së marrëdhënies së punës apo të ndonjë marrëdhënie tjetër kontraktuese, zyrtarit apo personit të kontraktuar i ndalohet të largojë apo të shpalos në çfarëdo forme informacionet e klasifikuara nga kontrolli i institucionit publik. **Neni 30****Bashkëpunimi ndërinstitucional** 1. Gjate zhvillimit te procedurës se verifikimit te sigurisë, Autoriteti Verifikues bashkëpunon me institucionet tjera publike te Republikës se Kosovës sipas nevojës. Institucionet tjera publike obligohen te ofrojnë informacionet sipas kërkesës.2. Bashkëpunimi ndërmjet AMIK dhe Agjencisë se Kosovës për Inteligjence, Ministrisë për Punë të Brendshme, Ministrinë për Forcën e Sigurisë së Kosovës, si dhe me institucionet tjera të sigurisë publike do të jetë i rëndësisë primare. 3. Gjate zhvillimit te procedurës se verifikimit te sigurisë, Autoriteti Verifikues sipas nevojës bashkëpunon me institucione homologe te shteteve tjera.**Neni 31****Verifikimi i sigurise per punonjesite e AKI-se**1. Verifikimi i sigurise per punonjesit e AKI-se kryhet nga AKI ne perputhje me ligjin e AKI-se si dhe duke zbatuar kriteret dhe standardet e percaktuara me kete ligj per sa i perket verifikimit te sigurise se personelit.2. AMIK pajis punonjesit e AKI-se me CSP sipas kerkeses se AKI-se.**Neni 32****Dosja e Sigurisë**1. Certifikata e Sigurisë, pyetësori i plotësuar i sigurisë dhe të gjitha dokumentet dhe materialet tjera relevante që kanë të bëjnë me verifikimin e sigurisë, mbahen nga Autoriteti Verifikues në dosjen e sigurisë.2. Përveç të dhënave të përcaktuara në paragrafin 1 të këtij neni, dosja e sigurisë përmban edhe informacione mbi ndryshimet e mëvonshme lidhur me informacionet e paraqitura në pyetësorin e sigurisë. 3. Drejtuesi i institucionit publik dhe personi i verifikuar kanë detyrë që ta informojnë menjëherë Autoritetin Verifikues për çdo zhvillim, ngjarje apo rrethanë të re që mund të rezultojnë në ndryshimin e informacioneve të dhëna në pyetësorin e sigurisë apo që në një mënyrë tjetër mund të ndikojnë negativisht në verifikimin e sigurisë të personit përkatës.4. Autoriteti Verifikues klasifikon dhe mbanë dosjen e sigurisë në mënyrë që i jep dosjes së sigurisë nivelin e klasifikimit dhe të mbrojtjes të cilin e konsideron të nevojshëm për t’i ruajtur interesat e sigurisë të Kosovës. **Neni 33****Përpunimi i të Dhënave**1. Autoriteti Verifikues mund të përpunojë të dhënat personale të personit të verifikuar që gjenden në dosjen e sigurisë vetëm me qëllim të ushtrimit të funksioneve dhe përgjegjësive të tij të përcaktuara me këtë ligj. 2. Autoriteti Verifikues nuk ia transferon institucioneve tjera publike të dhënat personale që gjenden në dosjen e sigurisë, përveç nëse ekziston një interes publik me prioritet pa i rrezikuar interesat e sigurisë të Republikës së Kosovës dhe vetëm për nevojat e: 2.1. veprimtarive lidhur me zbatimin e ligjit; 2.2. veprimtarive lidhur me zbulimin; 2.3. hetimet parlamentare. 3. Institucioni publik që i pranon të dhënat e tilla mund ti shfrytëzojë dhe përpunojë ato vetëm nëse kjo është absolutisht e nevojshme dhe për qëllime të specifikuara në paragrafin 2. të këtij neni dhe duhet ti sigurojë mbrojtje nga publikimi i paautorizuar që kërkohet për nivelin përkatës të klasifikimit. 4. Agjencitë e zbatimit të ligjit mund ti shfrytëzojnë dhe përpunojnë të dhënat të përcaktuara në paragrafin 2. të këtij neni për nevojat e ndjekjes penale vetëm si mjetin e fundit kur të dhënat e tilla nuk mund të mblidhen në forma tjera apo nëse ndjekja penale do të pengohej seriozisht në mungesë të qasjes në të dhënat e tilla.**KREU IV****SIGURIA INDUSTRIALE****Neni 34****Mbrojtja e informacionit të klasifikuar në fushën industriale**1. Mbrojtja e informacionit të klasifikuar në fushën industriale bëhet përmes përcaktimit të masave dhe procedurave të parandalimitnga përhapja e paautorizuar, humbja, apo shkeljet e sigurisë së informacionit të klasifikuar, i cili trajtohet në kushtet e zbatimit të një projekt/program/kontratë/nënkontratë të klasifikuar.2. Përcaktimi i standardeve, kur një Person Fizik, ose Juridik, ka aftësinë për të patur qasje tek informacioni i klasifikuar dhe zotëron kapacitetet e kërkuara për administrimin e këtij informacioni, përpara se të japë një ofertë, të negociojë, ose të marrë pjesë në një kontratë të klasifikuar, ose të punojë për një projekt të klasifikuar, i cili përfshin qasjen tek informacioni i klasifikuar, bëhet në përputhje me kërkesat e legjislacionit në fuqi.**Neni 35****Kushtet për lidhjen e një kontrate te klasifikuar**1. Operatorët Ekonomik të interesuar për të marrë pjesë në një prokurim të klasifikuar në nivelin “TEPËR SEKRET”, “SEKRET” dhe “KONFIDENCIAL”, duhet të jenë të pajisur më parë me nivelin e kërkuar të CSI. Personeli që përfaqëson Operatorin Ekonomik në prokurimin e klasifikuar dhe individët e tjerë, që do të kenë qasje tek informacioni i klasifikuar, duhet të jenë të certifikuar përshtatshmërish, sipas kërkesave të legjislacionit në fuqi.2. Operatorët Ekonomik të interesuar për të marrë pjesë në një prokurim të klasifikuar në nivelin “I KUFIZUAR”, nuk pajisen me CSI. 3. Personeli që përfaqëson Operatorin Ekonomik në këtë prokurim dhe të gjithë personat që do të kenë qasje tek informacioni i klasifikuar, brifohen dhe nënshkruajnë deklaratën për ruajtjen e informacionit të klasifikuar, përpara fillimit të procedurave të prokurimit të klasifikuar.**Neni 36****Pajisja me Certifikatë te Sigurisë Industriale**1. CSI lëshohet nga AMIK-u, sipas kërkesave të legjislacionit në fuqi2. Për Operatorët Ekonomik të vendeve të tjera, CSI lëshohet nga Autoritetet e Sigurimit Kombëtar, ose çdo Autoritet Kompetent Sigurie i vendit, ku është i regjistruar Operatori Ekonomik. Kjo certifikatë konsiderohet e vlefshme në funksion të pjesëmarrjes në një prokurimin të klasifikuar, vetëm pas konfirmimit me shkrim nga AMIK-u, adresuar Autoritetit Kontraktues. AMIK-u, përpara, se të konfirmojë CSI, bashkëpunon me Autoritetet Homologe për kryerjen e verifikimeve përkatëse. 3. Vetëm pas marrjes së konfirmimit nga AMIK, Autoriteti Kontraktues i jep Operatorit Ekonomik të drejtën e qasjes tek informacioni i klasifikuar.4. Operatori ekonomik i cili ofron shërbime në fushën e sigurisë mund të fillojë procedurat për pajisje me CSI para se të ketë një kontratë të klasifikuar me institucionet publike, duke bërë kërkesë te AMIK me arsyetimet përkatëse për nevojën e CSI.5. Procedurat për mbrojtjen e informacionit të klasifikuar në fushën industriale përcaktohen me akt nënligjor të propozuar nga AMIK dhe të miratuar nga Qeveria.**Neni 37****Kriteret themelore te vlerësimit të sigurisë industriale**1. Procedurat e verifikimit për lëshimin e CSI kryhen në përputhje me kërkesat e legjislacionit në fuqi dhe përfshijnë aspekte që lidhen me: 1.1 Strukturën e pronësisë së Operatorit Ekonomik, qëndrueshmërinë e tij financiare, reputacionin tregtar, aftësinë dhe kapacitetet teknike, si dhe aspektet e sigurisë. 1.2 Pronarët/aksionarët dhe stafin menaxherial, që për shkak të funksioneve do të kenë qasje tek informacioni i klasifikuar; 1.3 Personin e propozuar në pozitën e OS, zëvendësit të tij dhe punonjësit, që do të kenë qasje tek informacioni i klasifikuar.2. AMIK-u ka të drejtë të kërkojë informacion nga institucionet shtetërore që e gjykon të nevojshme, për verifikimin e rrezikut të mundshëm të sigurisë së Operatorit Ekonomik dhe të kategorive të personave që janë të përfshirë në prokurime të klasifikuara apo në zbatim të kontratës së klasifikuar.**Neni 38****Kushtet për lidhjen e nën kontratave të klasifikuara**1. Kontraktori, në çdo rast, përpara fillimit të negociatave për lidhjen e një nënkontrate të klasifikuar, duhet të marrë më parë miratimin me shkrim nga Autoriteti Kontraktues. 2. Nuk lejohet që Autoriteti Kontraktues, të autorizojë një Kontraktor me të cilin ka lidhur një kontratë të klasifikuar në nivelin “TEPËR SEKRET”, për të hyrë në marrëdhënie kontraktuale në kushtet e një nënkontrate të klasifikuar.3.Te gjitha kriteret për lidhjen/zbatimin e një kontrate te klasifikuara zbatohen përshtatshmërishtë edhe me nënkontraktorin.**Neni 39****Transporti dhe vizitat ndërkombëtare**1. Transporti i materialit të klasifikuar gjatë zbatimit të kontratës së klasifikuar, kryhet në rrugë tokësore, detare, hekurudhore dhe ajrore duke ju përmbajtur rregullave të sigurisë sipas kërkesave të legjislacionit në fuqi.2. Standardet e sigurisë së informacionit të klasifikuar në fushën e sigurisë industriale aplikohen edhe gjatë vizitave ndërkombëtare.**KAPITULLI I****SIGURIMI I SISTEMEVE TË KOMUNIKIMIT DHE INFORMACIONIT****Neni 40****Kuptimi i sigurisë së Sistemeve të Komunikimit të Informacionit**1. Siguria e sistemit të komunikimit të informacionit të klasifikuar është tërësia e standardeve për mbrojtjen e informacionit të klasifikuar, burimeve dhe shërbimeve të sistemit në mjetet e komunikimit që përpunojnë, ruajnë apo transmetojnë informacion të klasifikuar.2. AMIK është autoritet kombëtar i akredimit të sigurisë të sistemit te komunikimit elektronik qe përpunon, ruan apo transmeton informacione te klasifikuara.**Neni 41****Garantimi i sigurisë së informacionit**1. Garantimi i Sigurisë së Informacionit është praktika e garantimit të sigurisë së informacionit dhe menaxhimit të rrezikut që lidhet me përdorimin, përpunimin dhe transmetimin e informacionit apo të të dhënave në sisteme apo përpunime të tjera që përdoren për këtë qëllim.2. Garantimi i sigurisë së Informacionit është mbrojtja e sistemeve të Komunikimit dhe Informacionit në ekuilibër me parimet e Konfidencialitetit, Integritetit, Disponueshmerise, Autentifikimit dhe Mos-mohueshmërinë.**Neni 42****Sistemet e Komunikimit dhe Informacionit**1.Mekanizmat dhe procedurat e menaxhimit të sigurisë vendosen me qëllim pengimin, parandalimin, detektimin, rezistimin dhe rikuperimin nga impaktet e incidenteve që prekin objektivat e sigurisë së informacionit të klasifikuar, duke përfshirë raportimin e incidenteve të sigurisë. Këto masa përfshijnë:1.1 Sigurimin e Informacionit të mjaftueshëm për të mundësuar hetimin e komprometimit të qëllimshëm apo aksidentale të objektivave të sigurisë në përputhje me demin që mund të shkaktohet;1.2 Identifikimin dhe autentifikimin e besueshëm të personave, pajisjeve dhe shërbimeve të autorizuara për qasjen . Informacioni që kontrollon qasjen ne Sistemet e Komunikimit dhe Informacionit kontrollohet dhe mbrohet në përputhje me nivelin e klasifikimit të Informacionit për të cilin lejon qasjen.1.3 Kontrollon qasjen në informacion të klasifikuar në përputhje me parimin “nevojë për njohje”1.4 Menaxhimin e Integritetit, origjinës dhe disponueshmërisë së informacionit të klasifikuar 1.5 Kontrollin e lidhjeve të Sistemeve të Komunikimit dhe Informacionit që trajtojnë informacion të klasifikuar;1.6 Përcaktimin e nivelit të besueshmërisë së mekanizmave mbrojtës të sigurisë së Sistemeve të Komunikimit dhe Informacionit;1.7 Vlerësimin dhe verifikimin e funksionimit të saktë të mekanizmave mbrojtës të sigurisë së Sistemeve të Komunikimit dhe Informacionit përgjatë gjithë jetëgjatësisë së tyre;1.8 Hetimin e aktivitetit të përdoruesve dhe të Sistemeve të Komunikimit dhe Informacionit;1.9 Garantimin e jo-mohueshmërisë që dërguesi i informacionit të pajisjet me vërtetimin e marrjes së mesazhit nga marrësi dhe marrësi të pajiset me vërtetimin e identitetit të dërguesit;**KAPITULLI II - SIGURIA FIZIKE** **Neni 43****Siguria Fizike**1. Siguria fizike është tërësia e masave fizike, teknike ,elektronike dhe procedurale për ruajtjen e zonave, ndërtesave, zyrave, dhomave, hapësirave dhe pajisjeve ku prodhohet, regjistrohet, shfrytëzohet, transmetohet, ruhet, arkivohet dhe shkatërrohet informacioni i klasifikuar.2. Institucionet shtetërore kanë për detyrë të marrin masa për sigurimin fizik të zonave, ndërtesave, zyrave, dhomave, hapësirave dhe pajisjeve ku prodhohet, regjistrohet, shfrytëzohet, transmetohet, ruhet, arkivohet dhe shkatërrohet informacioni i klasifikuar, në pajtim me standardet dhe procedurat e përcaktuara përmes akteve nënligjore, i cili është në përputhje me standardet relevante të përcaktuara nga Organizata e Traktatit të Atlantikut të Veriut dhe të Bashkimit Evropian.3. Titullari i institucionit miraton me urdhër ndarjen e zonave të sigurisë i cili shoqërohet me planin dhe skemën e sigurisë fizike të objektit ku mbahet dhe administrohet informacioni i klasifikuar.4. Në Institucionet shtetërore ku punohet me informacionin e klasifikuar në varësi të volumit të informacionit të klasifikuar, krijohet strukturë e sigurisë/oficer i sigurisë.5. AMIK në bashkëpunim me institucionet shtetërore në mënyrë periodike kryen dezinfektimin elektronik të ndërtesave, zyrave, dhomave, ambienteve ku prodhohet, regjistrohet, shfrytëzohet, transmetohet, ruhet, arkivohet dhe shkatërrohet informacioni i klasifikuar.6. Rregullat për transportimin fizik të informacionit të klasifikuar, përcaktohet me akt nënligjor.**Neni 44****Njësia e informacionit të klasifikuar**1. Çdo institucion publik që prodhon dhe administron informacion të klasifikuar, duhet që brenda organizimit të strukturës së vetë të caktojë zyrtarin apo njësinë përkatëse si dhe të sigurojë zyrat apo hapësirat përkatëse, ku mbahet dhe administrohet informacioni i klasifikuar.2. Institucionet publike mbajnë Regjistrat për informacionin e klasifikuar sipas modelit të përcaktuar nga Agjencia.3. Modeli për shenjezimin e informacioneve te klasifikuara është unik dhe përcaktohet nga AMIK dhe obligohen te gjitha institucionet publike për zbatimin e tij. 4. Procesi i themelimit, mbajtjes dhe administrimit të njësisë apo zyrtarit përkatës, zyrave apo hapësirat përkatëse duke përfshirë edhe mbajtjen e Regjistrave për informacionin e klasifikuar, përcaktohet me akt nënligjor të miratuar nga Qeveria, sipas propozimit të Agjencisë. **Neni 45****Regjistrat**Çdo drejtues i institucionit publik që prodhon dhe administron informacion te klasifikuar duhet të krijoj standardet minimale te sigurise te mbrojtjes se informacionit te klasifikuar, si dhe te caktoj persona pergjegjes per administrimin e ketyre informacioneve.**Neni 46****Informacioni i huaj**1. Institucionet shtetërore e ruajnë informacionin e klasifikuar të shteteve të huaja apo të organizatave ndërkombëtare sipas standardeve që sigurojnë një shkalle mbrojtjeje, të njëjte me atë që kërkohet nga shteti apo organizata ndërkombëtare.2. Çdo institucion, përpara nënshkrimit të një marrëveshjeje ose protokolli teknik qe përfshin shkëmbimin e informacionit te klasifikuar, duhet të marrë më parë mendimin e AMIK. 1. Nënshkrimi i një marrëveshje apo protokolli teknik, që përfshin shkëmbimin e informacionit të klasifikuar, duhet të jetë paraprirë nga nënshkrimi i marrëveshjes së përgjithshme për sigurimin e informacionit te klasifikuar midis autoriteteve te sigurisë kombëtare të shteteve palë.

**Neni 47****Informacioni i klasifikuar i NATO-s dhe BE-së**1. Sistemi i Regjistrit të informacionit të klasifikuar të NATO-s dhe BE-së përbehet nga Zyra e Regjistrit Qendror në AMIK, Zyrat e Nënregjistrit të informacionit të klasifikuar të NATO-s e BE-së dhe pikat e kontrollit, që krijohen ne ministri dhe institucione shtetërore. 2. Informacioni i klasifikuar i NATO-s dhe BE-së shkëmbehet dhe administrohet vetëm përmes këtij Sistemi. 3. Sistemi i Regjistrit te informacionit te klasifikuar të NATO-s dhe BE-së është përgjegjës për regjistrimin, shpërndarjen dhe administrimin e informacionit të klasifikuar, te shkëmbyer ne kuadrin e bashkëpunimit me NATO-n dhe BE-në.4. Institucionet shtetërore janë të obliguara që ta mbrojnë informacionin e klasifikuar të NATO-s dhe të BE-se sipas standardeve qe sigurojnë shkalle mbrojtjeje të njëjte me atë që kërkohet respektivisht nga NATO-ja dhe BE-ja.5. Zyra e Regjistrit Qendror të informacionit të klasifikuar të NATO-s dhe BE-së në AMIK është struktura përgjegjëse për drejtimin e shkëmbimit, mbikëqyrjen dhe kontrollin e aspekteve të sigurimit të informacionit të klasifikuar të NATO-s dhe BE-së brenda Sistemit të Regjistrit.**Neni 48****Informacioni i Paklasifikuar i NATO-s, BE-s, shteteve dhe organizatave të tjera ndërkombëtare**Informacioni i Paklasifikuar, i NATO-s BE-s, shteteve dhe organizatave të tjera ndërkombëtare është informacioni i cili nuk përmban asnjë prej niveleve të klasifikimit, por që përdoret vetëm për arsye zyrtare nga institucionet shtetërore dhe nuk është i hapur për publikun.**Neni 49****Inspektimi i institucionve publike dhe Operatoreve ekonomik** **1.** AMIK zhvillon inspektime lidhur me zbatimin e masave te sigurise per mbrojtjen e informacineve te klasifikuara tek institucionet publike dhe operatoret ekonomik qe kane ne administim informacione te klasifikuara.2. Inspektimi zhvillohet mbi baze te rregullta kohore dhe me njoftim paraprak te institucionit publike.3. Objekt i inspektimit pa njoftim paraprak behen vetem ato institucione apo operator ekonomik qe kemi informacione te besushme qe ka shkelje te sigurise sa i perket adminitrimit te informacionve te kalsifikuara. 4. Objekt i inspektimit jane disiplinat e me poshtme:* 1. Siguria e personelit
	2. Siguria industriale

4.3 Siguria e e sistemeve te komunikimit dhe informaciont * 1. Siguria fizike

4.5 Adminitrimi i informacionve te klasifikuara 5. Pas perfundimit te inspektimit te masave te sigurise, AMIK harton raport te hollesishem lidhur me gjetjet si dhe propozon marrjen e masave perkatese per rritjen e shkalles se sigurise se informaconit te kalsifikuar.6. Raporti i drejtohet drejtuesit te institucionit publike perkates. 7. Ne koordinim me drejtuesin e institucionit publik hartohet plani per zbatimin e rekomandime qe rezulutojne nga raporiti i inspektimit.8. AMIK mbikqyre zbatimin e rekomandimeve tek institucioni publike dhe nese te njejta nuk zbatohen brenda afateve te parapara paraprarakisht, njofton me shkrim mbikeqyrsin e drejtperdrejte te derjtuesit te institucionit perkates i cili ishte objeket i inspektimit.**KREU VI** **AGJENCIA PËR MBROJTJEN E INFORMACIONIT TË KLASIFIKUAR (AMIK)****Neni 50****Themelimi i Agjencisë**1. Agjencia për Mbrojtjen e Informacionit të Klasifikuar (AMIK) themelohet si agjenci e sigurisë kombëtare në fushën e mbrojtjes se informacionit te klasifikuar, për të gjitha institucionet publike të Republikës së Kosovës dhe kontraktuesve të tyre qe ne çfarëdo forme mund të kenë në administrim informacionet e klasifikuara.  2. Agjencia për mbrojtjen e informacioneve te klasifikuara dhe të gjithë të punësuarit dhe personeli i angazhuar në të duhet të jenë politikisht i paanshëm, profesional, pa paragjykime në gjykimin e tyre dhe të veprojnë vetëm në pajtim me ligjin dhe që nuk marrin udhëzime nga ndonjë person apo institucion.3. AMIK është autoritet qendror me seli në Prishtinë.**Neni 51** **Përgjegjësit e AMIK në Fushën e Mbrojtjes se Informacionit të Klasifikuar**1. AMIK-u është institucion qendrori i pavarur në fushën e mbrojtjes së informacionit të klasifikuar me mandat për te organizuar, drejtuar e kontrolluar masat për ruajtjen, klasifikimin dhe administrimin e informacionit te klasifikuar dhe verifikimin e sigurisë për të gjitha institucionet e RKS si dhe kontraktueseve te tyre, që ka përgjegjësi për:1.1 hartimit të politikave* 1. ndjekjes së procedurave
	2. mbikëqyrjes së institucioneve dhe kontraktuesve në kontratat e klasifikuara
	3. edukimit të sigurisë,
	4. sigurimin e personelit
	5. sigurimin fizik
	6. sigurimin e informacionit
	7. sigurimin industrual
	8. sigurimin e sistemeve të komunikimit dhe informacionit

1.10 zhvillimit te negociatave për lidhjen e marrëveshjeve te sigurisë me shtete përkatëse 1.11 mbikëqyrë zbatimin e traktateve apo instrumenteve ndërkombëtare mbi mbrojtjen e informacioneve të klasifikuara dhe propozon marrjen e masave lidhur me këtë;2. AMIK është autoritet kompetent i sigurisë për Republikën e Kosovës, lidhur me mbrojtjen e informacionit të klasifikuar të shteteve të huaja dhe organizatave ndërkombëtare3. AMIK bashkëpunon me institucionet publike, operatoret ekonomik të interesuar dhe autoritetet homologe të shteteve dhe organizatave ndërkombëtare për kryerjen e detyrave të parashikuara sipas legjislacionit në fuqi4. Plani strategjik i punes te AMIK permban objektivat e pergjithshme dhe specifike per arritjen e stadardeve te sigurise per mbrojtjen e informaiconve te klasifikuara, i cili pas shqyrtimit nga KSK i propozohet qeverise per miratim. 5. Organizimi dhe funksionimi i brendshëm i AMIK rregullohet me akt nënligjor të propozuar nga AMIK dhe të miratuar nga Qeveria.**Neni 52****Agjencia për mbrojtjen e Informacionit të Klasifikuar****1.** AMIK vepron në bazë të këtij ligji në pajtueshmëri me Kushtetutën dhe të gjitha ligjet tjera në fuqi në Kosovë.2. AMIK është person juridik.3. AMIK është autoritet i sigurisë kombëtare **Neni 53****Përgatitja dhe Ofrimi i Buxhetit** 1. Drejtori i AMIK përgatit dhe i paraqet Kryeministrit projekt buxhetin vjetor për AMIK2. AMIK-u është organizatë buxhetore autonome me kod të vet buxhetor.3. Kuvendi i Kosovës i vë ne dispozicion AMIK-ut buxhetin vjetor te mjaftueshem per te kryer detyrat dhe pergjegjesit per te mbrtojtur informacionin e klasifikuar në pajtim me legjislacionin ne fuqi.**Neni 54****Emërimi i Drejtorit të Agjencisë**1. Kryeministri pas konsultimit me Presidentin emëron Drejtorin e Agjencisë brenda njëzet (20) ditësh pune nga dita kur pozita mbetet e lirë.
2. Drejtori i Agjencisë shkarkohet nëpërmjet procesit të njëjtë me të cilin është emëruar.
3. Drejtori i Agjencisë emërohet për një mandat pesë (5) vjeçar, i cili mund të vazhdohet.
4. Drejtori i Agjencisë, në pajtueshmëri me këtë Ligj, Rregulloren mbi Organizimin e Brendshëm dhe ligjet tjera në fuqi, është përgjegjës për të gjitha aspektet e menaxhimit të Agjencisë.

5. Në kryerjen e përgjegjësive të veta, drejtori i Agjencisë ndihmohet nga Zv. Drejtori, udhëheqësit e njësive organizative dhe personeli me kualifikim të duhur sipas nevojës, në pajtueshmëri me rregullat dhe procedurat e parashtruara me këtë Ligj dhe Rregulloren e Organizimit të Brendshëm.**Neni 55****Zëvendësdrejtori i Agjencisë**1. Zëvendësdrejtori i Agjencisë ndihmon drejtorin e Agjencisë dhe drejton aktivitetet të njësive organizative të Agjencisë nën mbikëqyrjen e drejtorit të Agjencisë.2. Zëvendësdrejtori i Agjencisë duhet të ketë arsimim universitar dhe emërohet mbi baza të profesionalizmit dhe përvojës së dëshmuar dhe pa marr parasysh përkatësinë politike, për një mandat pesëvjeçar (5), cili mund të përtërihet dhe do të rrjedhë pavarësisht nga mandati i drejtorit të Agjencisë.3. Tre (3) kandidatë për zv. Drejtor të Agjencisë propozohen nga Drejtori i AMIK tek Kryeministri për emërim.4. Kryeministri i Republikës së Kosovës, emëron zëvendës Drejtorin e Agjencisë brenda njëzet (20) ditësh pune nga dita kur pozita mbetet e lirë.5. Zëvendësdrejtori i Agjencisë shkarkohet nëpërmjet procesit të njëjtë me të cilin është emëruar.6. Zëvendësdrejtori i Agjencisë përkohësisht kryen dhe ushtron përgjegjësitë e drejtorit të Agjencisë gjatë mungesës apo paaftësisë të drejtorit. Në rast të paaftësisë të përhershme, zëvendësdrejtori i Agjencisë kryen dhe ushtron përgjegjësitë e drejtorit të Agjencisë deri në kohën kur zëvendësimi i Drejtorit të Agjencisë emërohet në mënyrë formale.Neni 56**Kriteret për emërimin e Drejtorit te përgjithshëm**1. Kriteret për emërim të Drejtorit te përgjithshëm te AMIK janë: * 1. të jetë vetem shtetas i Republikës së Kosovës;
	2. të ketë diplomë universitare;
	3. të ketë të paktën 8 vite pervoje pune profesionale ne institucionet e sigurisë, prej tyre se paku (5) vjet përvojë pune në pozitë udhëheqëse;
	4. të mos ketë qenë i dënuar për vepër penale, me vendim të formës së prerë;
	5. të mos jetë ndëshkuar për shkelje të rënda disiplinore, brenda pesë (5) viteve të fundit gjatë të cilave ka punuar në institucione publike;

1.6. të mos ketë konflikt interesi me detyrën apo siç parashihet në Ligjin për Parandalimin e Konfliktit të Interesit në Ushtrimin e Funksionit Publik;**Neni 57****Drejtori i Agjencisë**1. Drejtori i Agjencisë do t'i përgjigjet drejtpërdrejt Kryeministrit.1. Drejtori i Agjencisë:
	1. keshillon Kryeministrin e Republikës së Kosovës për çështje të mbrojtjes së informacionit të klasifikuar.
	2. raporton dhe njofton te Kryeministri i Republikës së Kosovës për aktivitetet e Agjencisë;
	3. ofron informata për Kryeministrit e Republikës së Kosovës sa i përket klasifikimit të informacioneve dhe verifikimin e sigurisë;
	4. mbron dhe ndihmon ne mbrojtjen e informacionit të klasifikuar nga shpalosja e pa autorizuar;
	5. vendosë dhe koordinon marrëdhëniet me agjencitë e huaja homologe;
	6. siguron se Agjencia nuk ndërmerr asnjë veprim që mund të krijojë dyshim të arsyeshëm se Agjencia është e angazhuar në avancimin, mbrojtjen apo dëmtimin e interesave të cilido komunitet apo cilësdo parti apo organizatë politike;
	7. siguron se Agjencia nuk ndërmerr asnjë veprim me qëllim të ndikimit në procese politike, opinion publik dhe media në Kosovë;
	8. përgatitë raportin vjetor te punës dhe propozon marrjen e masave te nevojshme per rritjen e shkalles se sigurisë se informacioneve te klasifikuara;
	9. inicion dhe nënshkruan Memorandume të Mirëkuptimit dhe Bashkëpunimit me institucione dhe organe tjera;
	10. raporton para Komisionit përkatës parlamentar te paktën një here ne vit;

**Neni 58****Kushtet specifike për punonjësit e Agjencisë**1. Personat e zgjedhur për punësim në Agjenci duhet të plotësojnë standardet strikte të sigurisë, të cilat përcaktohen në pajtim me ligjin në fuqi dhe në harmoni me procedurat e përcaktuara në rregulloret e shpallura nga drejtori i Agjencisë dhe të miratuara nga Qeveria. Kandidati duhet të vlerësohet stabil, i besueshëm dhe me karakter, vlerësim dhe diskrecion të shkëlqyeshëm. Çfarëdo dyshimi në lidhje me cilindo nga faktorët e sipërpërmendur zgjidhet në favor të sigurisë së Kosovës. 2. Kandidatët nuk punësohen nga Agjencia nëse nuk e kalojnë kushtin e sigurisë.3. Përveç kërkesave të përgjithshme për punësim që zbatohen ndaj punonjësve të tjerë të qeverisë, mund të aplikohen kushte speciale për punonjës të Agjencisë në lidhje me ekspertizën, shëndetin, detyrat e punës, dhe kërkesat e sigurisë që janë në përputhje me interesat e sigurisë së Kosovës.4. Rregullorja e Organizimit të Brendshëm të Agjencisë, përcakton kërkesat për secilën pozitë në Agjencisë, si dhe do të parashtrojë kërkesat specifike për punësim në Agjencisë.5. Në përputhje me rregullat e brendshme dhe kur është e nevojshme, Agjencia mund të kontraktojë palë të treta për shërbime ndihmëse.**Neni 59****Kualifikimet për punësim në Agjenci**1. Agjencia nuk mund të rekrutojë kandidatët nëse nuk i plotësojnë kushtet në vijim:* 1. të jenë shtetas të Kosovës;
	2. të kenë kualifikime të duhura arsimore dhe profesionale ashtu siç përcaktohet me Rregulloren për Organizimin e Brendshëm;
	3. të kryejnë ekzaminimin mjekësor të kërkuar për pozitë;
	4. të jenë të liruar nga shërbimi ushtarak, nëse është e zbatueshme; dhe
	5. të jenë të aftë të plotësojnë kërkesat e sigurisë që do të përcaktohen me kete ligj dhe akte nenligjore

2. Rregullat dhe procedurat për kërkesat e përgjithshme dhe procedurat e rekrutimit, marrëdhëniet e punës, të trajnimit, avancimit në karrierë si dhe emertimet e pozitave përcaktohen me rregulloren per marrëdhënien e punes në AMIK të miratuar nga Qeveria.**Neni 60****Statusi i të punësuarve të AMIK-ut**Punonjësit e AMIK-ut kanë status te veçantë sipas këtij ligji. Për çështjet të cilat nuk rregullohen më ketë ligj apo aktet nënligjore që derivojnë nga ky ligj, do të zbatohet përshtatshmërisht legjislacioni që rregullon çështjet e shërbimit civil**Neni 61****Të drejtat e punonjësve të Agjencisë**1. Punonjësit e Agjencisë kanë të drejtë për:
	1. për punësim të përhershëm deri në plotësimin e kushteve për pensionim, me përjashtim të individëve të cilët janë të punësuar në bazë të kontratës për shërbim për një periudhë fikse, si dhe atyre që shkarkohen me arsye, në bazë të legjislacionit në fuqi;
	2. të merr pushim në pajtim me legjislacionin në fuqi dhe mundësinë për të vazhduar punën e njëjtë apo të ngjashme kur të mbarojë pushimi;
	3. për shpërblim për detyrat dhe kryerjen e detyrave siç përcaktohet me këtë ligj;
	4. të merr rrogë dhe pagesa në pajtim me legjislacionin në fuqi;
	5. për avancim të karrierës dhe zhvillim profesional nëpërmjet trajnimit dhe mjeteve tjera;

**Neni 62****Sjelljet e ndaluara të Punonjësit**1. Punonjësit e Agjencisë nuk duhet të jenë anëtarë të subjekteve politike apo marrin udhëzime prej tyre, apo individëve jashtë Agjencisë si dhe nuk duhet të shprehin publikisht bindjet dhe preferencat e tyre politike2. Punonjësit nuk mund të kryejnë çfarëdo aktiviteti apo detyra tjera publike apo profesionale me pagesë, të cilat nuk janë në përputhje me punën e Agjencisë apo krijojn konflikt interesi.3. Punonjësit e Agjencisë nuk mund të kenë punësim tjetër gjatë kohës sa janë të punësuar të Agjencisë. 4. Punonjësit e Agjencisë nuk kanë të drejtën për veprime që kanë për qëllim ndërprerjen e aktivitetit apo ndonjë formë tjetër të ndalesës kolektive të punës.5. Punonjësit e Agjencisë, pa pajtimin paraprak të drejtorit të Agjencisë, nuk mund të japin deklarata publike apo përndryshe komentojnë punën e Agjencisë, apo ofrojnë informacion personave të paautorizuar mbi të dhënat, dokumentet, kontaktet, qëllimet, dijen apo personelin e Agjencisë. 6. Në rast se kandidon në zgjedhjet për Kuvendin e Republikës së Kosovës apo për organet e qeverisjes lokale, detyrohet të kërkojë lirimin nga detyra dhe nuk mund të ripranohet më në Agjenci.**Neni 63****Detyrimet ligjore personale të punonjësit**1. Secili punonjës i Agjencisë do t’i kryej detyrat që i jepen në pajtim me këtë ligj dhe ligjet tjera relevante dhe është personalisht përgjegjës për zbatimin e ligjshëm të detyrave të Agjencisë, ashtu siç është përcaktuar me këtë Ligj, dhe që janë në kuadër të detyrave të dhëna punonjësit të caktuar.2. Nëse një punonjës beson se ai apo ajo ka pranuar një urdhër jo te ligjshem, ai apo ajo duhet të informojë urdhërdhënësin në lidhje me shqetësimin e tij apo të saj.3. Në rastet kur urdhërdhënësi përsërit urdhrin, Punonjësi do të kërkojë një konfirmim me shkrim të urdhrit të tillë. Nëse Punonjësi vazhdon të ketë rezervime, ai apo ajo do t'ia përcjellë urdhrin eprorit të parë të urdhërdhënësit dhe do t'ia raportojë çështjen Drejtorit.4. të sigurojë mbrojtjen dhe mospërhapjen e paautorizuar të informacionit të klasifikuar, për të cilin ka marrë dijeni gjatë ose jashtë kryerjes së detyrës, detyrim ky që vazhdon edhe pasi ai ndërpret marrëdhëniet e punës me Agjencinë; 5. të mos e përdorë informacionin e mbledhur gjatë ushtrimit të detyrës për qëllime të tjera, jashtë atyre të përcaktuara me ligj; 6. të sigurojë mbrojtjen dhe mospërhapjen e të dhënave personale dhe të atyre që lidhen me veprimtarinë profesionale të personave, të mbrojtura sipas ligjit, me të cilat njihet gjatë ushtrimit të detyrës. **Neni 64** **Pagat dhe kompensimi për punonjësit e Agjencisë**  1. Pagesat dhe kompensimet shtesë, për personelin e Agjencisë, përcaktohen me akt nënligjor të propozuar nga drejtori dhe të miratuar nga Qeveria;2.Perveç pagës bazë punonjësit e AMIK mund te pranojnë ligjërisht lloje tjera te shtesave te pagës, mëditje dhe beneficione, duke u bazuar në faktorët qe përfshin vështirësinë në punë, punën jashtë orarit apo shkathtësi speciale;  3. Në rast të vdekjes në detyrë apo për shkak të ushtrimit të detyrave të tij në kuadër të AMIK, Qeveria do t’i paguajë familjes së punonjësit të ndjerë apo trashëgimtarit(ve) ligjor të tij pagën mujore të punonjësit të AMIK për një periudhë kohore prej një (3) viti nga vdekja e punonjësit;**Neni 65****Ndërprerja e punësimit**1. Punësimi i punonjësve të Agjencisë ndërpritet në këto raste:* 1. dorëheqja vullnetare nga Agjencia;
	2. përfundimi i kontratës
	3. arritja e moshës së pensionimit;
	4. paaftësia e përhershme për kryerjen e detyrave zyrtare për shkak të kushteve shëndetësore, me kusht që Punonjësi nuk ka të drejtë të transferohet në një pozitë tjetër të përshtatshme brenda Agjencisë;
	5. humbja e shtetësisë së Kosovës;
	6. dënimi te formës se prerë për vepër penale.
	7. përjashtimi nga agjencia si rezultat i procedurës disiplinore.

**Neni 66****Kartelat e identifikimit**Punonjësve të Agjencisë ju lëshohen kartelat e identifikimit. Lloji, forma dhe përmbajtja e kartelës së identifikimit të Punonjësit të Agjencisë përcaktohet me vendim të nxjerrur nga Drejtori i AMIK.**Neni 67****Rregullorja dhe Organizimi i Brendshëm**Organizimi i brendshëm i Agjencisë përcaktohet me Rregulloren e Organizimit të Brendshëm e cila miratohet ne Qeveri.**Neni 68****Zbatimi i standardeve të BE-së dhe NATO-s**1. AMIK është Autoritet i Sigurisë së Republikën së Kosovës që kujdeset për arritjen e standardeve te sigurisë për mbrojtjen e informacionit te klasifikuar ne përputhje me kërkesat qe derivojnë nga direktivat e sigurisë se NATO-se dhe BE-se.2.Agjencia shkëmben informacione të klasifikuara me të gjitha shtetet anëtare të NATO-s dhe BE–së si dhe shteteve te tjera. 3. Sipas direktivave të NATO-s dhe BE-së, Agjencia njeh certifikatat e sigurisë se personelit dhe certifikatat e sigurisë industriale të shteteve me të cilat ka nënshkruar marrëveshje të sigurisë.**KAPITULLI III****SHKELJET E SIGURISE DHE KOMPROMENTIMI I INFORMACIONIT TE KLASIFIKUAR****Neni 69**1. Shkelja e sigurisë ndodh si rezultat i një akti, apo mosveprimi nga një individi i cili vepron me kundërshtim me rregullat e sigurisë te përcaktuar me këtë ligj dhe aktet tjera nënligjore.2. Kompromentimi I informacioni te klasifikuar ndodh atëherë kur, si rezultat i shkeljes se sigurisë ka shkaktuar zbulim tërësor apo pjesor te informacionit tek një person i paautorizuar.3. Çdo shkelje apo dyshim për shkelje te sigurisë duhet te raportohet menjëherë tek autoriteti kompetent i sigurisë AMIK.4. Kur dihet apo kur ka arsye te mjaftueshme për te pohuar se informacioni I klasifikuar është kompromentuar apo humbur autoriteti i sigurisë duhet te merr masa ne përputhje me ligjin dhe aktet nënligjore duke: * 1. informuar autoritetin origjiner
	2. siguruar se rasti po hetohet nga një person neutral ne lidhje me çështjen
	3. përcaktuar demin potencial qe i shkaktohet interesave te Republikës se Kosovës apo shteteve dhe organizatave tjera
	4. marr masat e përshtatshme për parandalimin e një përsëritje
	5. te njoftoj autoritetet përkatëse për veprimin e kryer

5. Çdo individ përgjegjës për shkelje e rregullave te sigurisë te përcaktuara me këtë ligj dhe aktet nënligjore do ti nënshtrohet ndëshkimeve disiplinore ne përputhje me legjislacionin ne fuqi.6. Çdo individ përgjegjës për kompromentim apo humbje te informacioni te klasifikuar do ti nënshtrohet nddeshkimeve disiplinore/apo veprimeve ligjore ne përputhje me ligjet dhe aktet nenligjore te aplikuara. **KREU VII****MBROJTJA E DOSJEVE DHE TË DHËNAVE****Neni 70****Humbja e Informacioneve të Klasifikuara**1. Për çfarëdo humbje, humbje të dyshuar, thyerje apo thyerje të dyshuar të sigurisë së informacioneve të klasifikuara, si dhe për çfarëdo qasje aktuale apo të dyshuar të paautorizuar në informacione të klasifikuara, të gjithë bartësit e autorizuar të informacioneve të klasifikuara menjëherë i raportojnë për këtë institucionit të tyre përkatës publik, prokuroris se shtetit si dhe Agjencisë. 2. Agjensia me iniciativen e vet ose me kerkes te autoritetit përkatës ne rastet e shkeljeve te sypozuara me kete ligj,menjëherë i merr të gjitha masat e nevojshme për të:2.1 hetuar rastin;2.2 identifikuar shkakun e humbjes, 2.3 gjurmuar ndonjë hapje nga persona të paautorizuar për tu qasur në informacioneve të tilla;2.4 larguar ndonjë efekt të dëmshëm dhe për të parandaluar humbje të mëtejme të informacioneve të klasifikuara;3. Në rast se shkelja e supozuar dyshohet se përbën vepër penale, e njofton prokurorin e shtetit. **KREU VIII****Neni 71****Sanksionet Penale** 1. Personi i cili pa autorizim publikon informacionin e klasifikuar sipas këtij ligji si ”KONFIDENCIALE” dhe cilido bartës i autorizuar i informacionit të tillë të klasifikuar i cili nuk e mbron informacionin e klasifikuar siç kërkohet me këtë ligj, kryen vepër penale dhe dënohet me burgim prej një deri pesë (5) vite.2. Personi i cili publikon pa autorizim informacionin e klasifikuar sipas këtij ligji si “SEKRET”, dhe cilido bartës i autorizuar i informacionit të tillë të klasifikuar nuk e mbron informacionin e klasifikuar siç kërkohet me këtë ligj, kryen vepër penale dhe dënohet me burgim prej tri deri dhjetë vite. 3. Personi i cili publikon pa autorizim informacionin e klasifikuar sipas këtij ligji si “TEPËR SEKRET”, dhe cilido bartës i autorizuar i informacionit të tillë të klasifikuar i cili nuk e mbron informacionin e klasifikuar siç kërkohet me këtë ligj, kryen vepër penale dhe dënohet me burgim prej pesë (5) deri dymbëdhjetë (12) vite.**NENI 72****DISPOZITAT KALIMTARE DHE PËRFUNDIMTARE** 1. Pas emërimit drejtori te AMIK ne bashkëpunim me drejtorin e AKI-se fillon procedurat e bartjes se departamentit te verifikimit me dosjet përkatëse ne AMIK.2. Punonjësit aktual të ish-Departamentit te verifikimit te sigurisë ne kuadër te AKI kanë të drejtë që përmes një deklarimi vullnetarë të zgjedhin vazhdimin e punës në AMIK apo te mbesin në kuadër të strukturave të AKI3. Punonjësit e ish-Departamentit te verifikimit te sigurisë ne kuadër te AKI që do të vazhdojnë te punojnë ne AMIK, gëzojnë te drejtën e stazhit të fituar në AKI.4. Drejtori i AMIK dhe drejtori i AKI-se me marrveshje mund te shfrytezojn asetet e AKI deri ne kompletimin e stafit te AMIK5. Qeveria ofron objekt te përshtatshëm me standarde te sigurisë ne funksion te arritjes se mandatit të AMIK për mbrojtjen e informacioneve te klasifikuara te Republikës se Kosovës. 6. Ne ç’do dispozitë te ligjeve, akteve nënligjore , shprehja AKI e përdorur ne kuptimin e autoritetit verifikues, me hyrjen ne fuqi te këtij ligji zëvendësohet me AMIK.**Neni 73****Aktet nënligjore**Qeveria miraton aktet nënligjore për zbatimin e këtij ligji brenda një (1) viti nga hyrja e tij në fuqi.**Neni 74** **Shfuqizimi**Me hyrjen në fuqi të këtij ligji, shfuqizohet Ligji nr. 03/L-178 për klasifikimin e informacioneve dhe verifikimin e sigurisë (Gazeta Zyrtare e Republikës së Kosovës, nr. 76, 10 gusht 2010)**Neni 75** **Hyrja në fuqi**Ky ligj hyn në fuqi pesëmbëdhjetë (15) ditë pas publikimit në gazetën zyrtare të Republikës së Kosovës**Kadri Veseli****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Kryetar i Kuvendit të Republikës së Kosovës  | **The Assembly of the Republic of Kosovo,**Pursuant to Article 65 (1) of the Constitution of the Republic of Kosovo,Approves:**LAW ON PROTECTION OF CLASSIFIED INFORMATION****CHAPTER I** **GENERAL PROVISIONS****Article 1****Purpose**1. The purpose of this Law is to establish a unique system for protection of classified information related to the security interests of the Republic of Kosovo.2. This Law establishes the Agency for Protection of Classified Information (hereinafter referred to as APCI), whereby determining its mission, structure, functioning, duties and responsibilities.3.This Law is in line with the EU legislation, as follows:3.1 Council decision of 23 September 2013 on the security rules for protecting EU classified information3.2 Regulation (Eu) 2016/679 Of The European Parliament And Of The Council Of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**Article 2****Scope** This Law applies to all public institutions exercising executive, legislative and judicial competencies and natural and legal persons, which based on the need-to-know principle could, while discharging their duties, have access to classified information of the Republic of Kosovo, other states and international organizations.**Article 3****Definitions**1. Terms used in this Law shall have the following meanings:1.1. **Classified information** - any document or material, regardless of the form, nature or manner of its transmission, prepared or that is to be prepared, for which a certain level of classification has been set in the interest of security of the Republic of Kosovo and in compliance with the applicable legislation requiring protection against any violation, acquisition, distribution, loss or access of an unauthorized individual and any other type of security compromising;1.2. **Access –** ability or possibility to obtain knowledge of classified information;1.3. **Need-to-know –** the need of access to classified information in the light of a certain position and for the purpose of fulfilling a specific duty;1.4. **Classification** – the act or process of determining the level of classification and the time period for maintaining such classification;1.5. **Agency –** Agency for Protection of Classified Information (APCI);1.6. **National Security Authority** - the internal state authority responsible for controlling and implementing classified information security standards. APCI is the National Security Authority in the Republic of Kosovo. 1.7. **Vetting Authority** - the Agency for Protection of Classified Information, as a structural unit specialized for conducting security clearances for individuals who will obtain knowledge, produce, store, administer, transport and transmit classified information; 1.8. **Security Clearance Questionnaire** - the form completed by any individual requiring access to classified information, and serves as the base for security clearance and assessment of data for the issuance or rejection of “Personnel Security Clearance” certificate. 1.9. **Personnel Security Clearance (**PSC) - the official document of APCI, or competent security authority of another country, which confirms, in terms of security, that an individual meets the conditions set for obtaining knowledge, storing, administering and transferring classified information. 1.10. **“Briefing”/“Debriefing”** - a set of instructions and guidelines related to procedures for classified information security and individual responsibility for violation of security rules to which individuals requiring the opportunity for obtaining knowledge of classified information are subject to, or are equipped with PSC. 1.11 **Security breach** - an act or omission in contradiction with the applicable legislation that results, or may result in theft, loss, damage, compromise or unauthorized disclosure of classified information. 1.12 **Security Clearance** - the set of measures and procedures applied to a natural or legal person, and which serve as the basis for issuance, rejection, temporary suspension or withdrawal of “Personnel Security Clearance” certificate. 1.13 **Unacceptable Security Risk** - circumstances described in this Law, based on which APCI refuses the granting of PSC, or considers that the measure of its withdrawal or temporary suspension should be taken. 1.14 **Circumstances of Exceptional Urgency** – conditions of objective inability to follow normal procedures for issuing a PSC due to the exercise of a short-term official duty of participation in an unpredicted international activity, extending military missions in various countries, etc. 1.15 **Security Officer** (hereinafter SO) - the employee responsible for, or the structure charged by the head of the ministry, or state institution, for supervising and implementing requests for personnel security, and other disciplines of classified information;1.16 **Economic Operator** – any natural or legal person, or a group of such persons who supply goods, works and/or services;1.17 **Classification Authority** – President, President of Assembly, Prime Minister, President of the Supreme Court, Chief State Prosecutor, Director of KIA, Minister of Internal Affairs, Minister of MKSF, Commander of KSF, Police General Director, as well as any person authorized by them, who has original or delegated competence to classify information,1.18 **Classified Contract –** any contract concluded by a public institution and containing information classified under this law;1.19 **Declassification –** authorized change of the status of information from classified information into unclassified information;1.20 **Document -** any physical or electronic media upon which information is recorded.1.21 **Downgrading –** a decision that information classified and safeguarded at a set level is classified and safeguarded at a lower level of classification.1.22 **Foreign government information** means:1.22.1. information provided to the Republic of Kosovo from a foreign government, or international government organization; 1.22.2. information produced by the Republic of Kosovo in compliance with, or as a result of a common agreement with a foreign government or international governmental organizations, expecting or requiring that such information or agreement, or both, are kept secret.1.23. **Material –** documents and any machinery, equipment or armament produced or being produced.1.24. **Processing –** any operation, or set of operations, which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.1.25. **Public institution –** all institutions and bodies set in Article 2.1 of this Law.1.26. **Security interests -** refers to defence, intelligence and law enforcement activities, security or foreign relations of the Republic of Kosovo, including its territorial integrity, integrity of its institutions, the constitutional order and economic stability and development.1.27**. Spouse -** any relationship established under lawful marriage, and shall include, for the purposes of this Law, any extramarital relationship between two natural persons.1.28. **Head of public institution –** officers elected in elective positions in public institutions and officers appointed by elected officers.1.29. **Authorized holders of classified information –** a person in possession of classified information, valid PSC and meeting other conditions that allow access to classified information, except otherwise determined by law.1.30. “**Contracting Authority**” - any state entity assuming the classified procurement and entering contractual relationship. 1.31. “**Economic Operator**” - any natural or legal person, or a group of such persons, who supply goods, works and/or services. 1.32. “**Classified Contract**” – any contract and sub-contract, whose implementation requires access to classified information, or usage, storage, administration, circulation, transmission and transport of classified information or material. 1.33 “**Contracting Party**” – any natural or legal person with legal capacity to negotiate and conclude classified contracts.1.34 **Personnel Security Clearance –** official document of APCI, or a Competent Security Authority of another country, which confirms, in terms of security, that a natural person possess acceptable risk for access to classified information.1.35 “**Industrial Security Clearance**” certificate (hereinafter ISC), is an official document of APCI, or competent security authority of another country, whereby confirming, in terms of security, that an economic operator has organizational, technical, physical capacities and abilities and fulfils standards set for access, storage and administration of classified information in a project/program, or classified contract/sub-contract.**CHAPTER II – INFORMATION SECURITY** **Article 4****Classification Authority**1. The authority of classifying information shall be exercised by:* 1. President
	2. President of Assembly
	3. Prime Minister
	4. President of the Supreme Court
	5. Chief State Prosecutor
	6. Director of KIA
	7. Minister of Internal Affairs
	8. Minister of MKSF
	9. Commander of KSF
	10. Police General Director

2. Authorities responsible for information classification provided for in paragraph 1 of this article shall be entitled to transfer the classification competence to the heads of their subordinate institutions.3. The request for granting authorization by the Classification Authority shall be submitted to APCI, which after reviewing and assessing, recommends for granting authorization or not.4. Any authorization of the competency to classify information shall be done in writing and clearly identify the title holder by name and the title of the position. This authorization shall be valid only for the duration of the position as the head of relevant institution.5. Any head of the relevant institution cannot classify information of the institution and its relevant subordinate units without the authorization by the Classification Authority.6. Agency shall draft, maintain and regularly update a register with the names of heads with competence for classification.**Article 5****Categories of information to be classified**1. The information shall be classified only if necessary and if it falls within one or more of these categories: 1.1 projects, plans, systems or operations related to the protection and security of the constitutional order of the Republic of Kosovo;1.2 information of foreign governments, international relations or activities of the Republic of Kosovo, which will be protected against unauthorized exposure.1.3 activities, information sources and methods of intelligence institutions related to the security of the Republic of Kosovo.1.4 systems, installations, infrastructure, projects, plans or services of protection related to the security interests of the Republic of Kosovo; 1.5 scientific, technological, economic and financial activities related to the security interests of the Republic of Kosovo; 1.6. cryptologic systems; cryptologic issues/problems;1.7. plans on operation and use of the system of communication of classified information and cryptology;1.8. risk assessments/inspection reports related to the shortcomings in cryptology system;1.9. plans for identification, reduction and management of the risk that occurs in the electronic communication system.1.10. plans, projects and programs for securing systems of communication for classified information;1.11. information collected through specific operations and electronic interceptions.**Article 6****Prohibition of information classification**1. The classification of information is prohibited when done for the purpose of:1.1. hiding law violation, abuse of authority, lack of efficiency or administrative error, 1.2. depriving the right to recognize a person, organization or institution,1.3. hampering or delaying the provision of information that is not required to be protected in the interest of security of the Republic of Kosovo, and1.4. prohibiting competition,shall be prohibited. **Article 7****Classification levels**1. In terms of content, value and state interest, the information shall be classified in one of the following levels: 1.1. “TOP SECRET” - unauthorized dissemination and publication of which, under reasonable assessment, could result in exceptionally grave damage to the security interests of the Republic of Kosovo; 1.2. “SECRET” – unauthorized dissemination and publication of which would seriously damage security interests of the Republic of Kosovo; 1.3. “CONFIDENTIAL” – unauthorized dissemination and publication of which would damage security interests of the Republic of Kosovo; 1.4. “RESTRICTED” – unauthorized dissemination and publication of which would be unfavourable for security interests of the Republic of Kosovo. 2. The Classification Authority shall avoid over-classification of information and shall assign to them only a level of classification that is necessary to protect interests of the Republic of Kosovo.3. Information classification procedures, including classification of parts of documents, separate documents and markings that contain classified information, shall be determined with a bylaw proposed by APCI and adopted by the Government.**Article 8****Duration of classification**1. Information shall be classified insofar as it is in the interest of security of the Republic of Kosovo.2. Terms for classification of information shall be as follows:2.1. information classified as “RESTRICTED”, one (1) year; 2.2. information classified as “CONFIDENTIAL”, five (5) years; 2.3. information classified as “SECRET”, fifteen (15) years; and 2.4. information classified as “TOP SECRET”, fifty (50) years. 3. The calculation of the term for classification of information shall start from the date of production of classified information.4. If the Classification Authority considers that information should be protected for a period longer than provided for in paragraph 2, it shall issue a new decision for classification in accordance with Article 8 of this Law. Such a decision shall not be taken earlier than six (6) months before the date foreseen for declassification under paragraph 1 of this article.**Article 9****Conditions for production, usage and circulation of classified information**1. Production of classified information shall take place only based on the list of classified information approved by the Classification Authority, in compliance with the procedure determined by the applicable legislation.2. Production, usage, multiplication, transfer, physical transportation, archiving, storage and destruction of classified information shall take place in compliance with the following standards: 2.1. Personnel security;2.2. Physical security;2.3. Information security;2.4. Industrial security;2.5. Security of information communication systems.3. Procedures for implementation of this article shall be governed with a bylaw proposed by APCI and adopted by the Government.**Article 10****Declassification**1. Information shall be declassified when there is no longer a need for protection and when its publication no longer poses a risk to the security of the Republic of Kosovo.2. The Classification Authority, from which the classified information is originated, shall carry out the declassification. 3. Cases of declassification of classified information shall be:3.1. when its publication is dictated by state interests that are more important than the need to keep it classified;3.2. when an event or a particular date occurs as determined by the classification authority.4. Unauthorized disclosure and publication of classified Information shall not constitute a cause for declassification.5. The Classification Authority which has declassified information shall be obliged to notify all institutions that possess the classified information.6. The procedures for the implementation of this Article shall be regulated by a sub-legal act, proposed by APCI and approved by the Government.**Article 11****Disposal and Destruction of Classified Information**1. In any state institution, the head of the institution or its authorized representative shall establish the commissions for disposal and destruction of classified information.2. The commission for disposal shall review and decide on the disposal of classified information, in cases when this information is of no value for further retention and shall not be declassified.3. Commission for destruction, based on the Decision of the Commission for Disposal, shall carry out all procedures regarding the destruction of classified information and prepare the final report.4. Information that shall be submitted to the archive network should not be disposed and destroyed but declassified.5. Procedures for implementation of this Article shall be regulated by a sub-legal act proposed by APCI and approved by the Government.**Article 12****Downgrading and Upgrading of Classification Level**1. The Classification Authority, which has originated classified information, shall be responsible for the downgrading of the classification level of such information.2. The competent classification authority shall downgrade or upgrade the classification level if it becomes aware of facts that clearly indicate that the classified information does not require the level of protection associated with the existing level of classification. **Article 13****Citizens Proposals** 1. When a citizen or employee of the Republic of Kosovo, who has no classification authority, considers that particular information under the state’s control has the necessary values to be classified, he or she shall propose the classification of this information to the relevant institution. This institution shall decide within 10 days whether the information will be classified or not and shall notify the citizen or the employee of the decision taken.2. From the moment of the proposal on the classification of relevant information, its possessor shall be obliged to protect the information from unauthorized access.**CHAPTER III – PERSONNEL SECURITY****Article 14****Personnel Security**1. Personnel security shall mean the set of measures and procedures based on which is assessed on whether a person, while maintaining his loyalty, reliability and security, can be authorized to access classified information without jeopardizing the security of said information.2. Issuance, refusal, temporary suspension or revocation of the “Personnel Security Clearance” (hereinafter: PSC) shall be made in accordance with paragraph 1 of this Article.3. Procedures for implementation of this Article shall be regulated by a sub-legal act approved by the Government.**Article 15****Personnel Security Clearance** 1. The Verifying Authority shall issue the PSC only to the person who, after carrying out a security clearance procedure in accordance with the applicable law, is designated as an acceptable security risk.2. PSC shall clearly show the level of classified information, in which the person who has passed the security clearance procedure, can access. The PSC, for a certain level of classification, shall give the title holder access to information with the lowest classification level.3. Each head of the public institution shall be obliged, within 15 days, to implement the decision of the Verifying Authority and shall not provide access to classified information to a person who has been denied a PSC.**Article 16****Criteria for Knowing the Classified Information**1. The right to know, retain, manage and transfer classified information have only persons who: 1.1 obtain the right of knowing by the head of the institution or the Contractor's Industrial Security Officer due to the duty they perform; * 1. have full capacity to act;

1.3 are previously informed about the classified information security procedures and individual responsibilities for security breaches and have signed the non-disclosure statement; 1.4 are provided with PSC, with the exception of cases for knowing information classified as “restricted”. 2. Only the President of the Republic of Kosovo, the President of the Assembly of Kosovo and the Prime Minister shall be authorized to access classified information for the purpose of discharging their official duties without fulfilling the requirements set out in paragraph 1 of this Article provided they have a need to know this information.**Article 17****Lists of functions/positions for knowing the classified information**1. State institutions which, because of their activity, produce classified information or, while cooperating with other institutions benefit this category of information, have the duty to approve and send in writing to APCI a list of functions/positions that due to official duties can be acquainted with classified information and relevant PSC level.2. The review of these lists shall be done periodically and in accordance with the changes in the organizational structure of the respective institution. For any eventual change, the head of the institution shall be obliged to notify APCI.**Article 18****Conditions for initiating the Security Clearance** 1. Security Clearance procedure shall commence only after the applicant has accepted and has given written consent to collect data and perform security clearance procedures, as per the security questionnaire requirements.2. The handling of personal data and information collected in the Security Clearance process shall be carried out in accordance with the requirements of the applicable Law on the Protection of Personal Data.**Article 19****General Security Assessment Requirements****1.** APCI, as the only Verifying Authority in the Republic of Kosovo responsible for conducting the Security Clearance Procedure, shall comply with the General Security Assessment Requirements, which include, but are not limited to the following: 1.1. The accurate verification of identity, generality and status of citizenship in the past and the present, for each person.1.2. The data control, in function of the security of the Republic of Kosovo. 1.3. The applicant's financial status, in order to verify whether he may be under pressure due to instability, serious financial difficulties or the possession of any unjustified property. 1.4. The information on the education of a person after the age of 18 or for the period considered as appropriate by the verifying authority. 1.5. The information on the employment of the individual taking into consideration the references from previous jobs, based on employer reports. 1.6. The information on participation in military operations or the duration of service in the military. 1.7. The overall assessment of whether a person may be pressured by an unfriendly foreign force. **Article 20****Essential Security Assessment Criteria**1. The essential criteria, used to assess existence or non-existence of an unacceptable security risk for classified information, which serve as the grounds for issuing, suspending or rejecting the equipment or holding of a PSC, are the cases where an individual results to: 1.1. have been, is or is trying to secretly engage, alone, in collaboration or as part composition of an illegal organization, in espionage, terrorism, betrayal, rebellion or armed violence against the constitutional order or has actively encouraged someone to engage in espionage, terrorism, betrayal, rebellion or armed violence against the constitutional order; 1.2. has been or is a collaborator of espionage, terrorism, betrayal, rebellion or armed violence against the constitutional order, there are suspicions that he/she has been a collaborator of representatives of organizations, foreign states, including intelligence services, which may violate the security of our country and/or NATO and EU Member States, unless such collaborations are authorized due to the duty; 1.3. has been or is a member of an organization that, by violent, hostile, illegal means, intends to overthrow the government or change the constitutional order; 1.4. has been or is a supporter of an organization as described in point 1.3 of this Article, or has been or is closely associated with any member of such an organization; 1.5. has intentionally concealed, misrepresented or falsified information of major importance, of a particular security nature or intentionally lied during the completion of a security questionnaire or a security interview; 1.6. has been convicted for one or more intentionally committed criminal offenses. 1.7. has a background of addiction to alcohol, use of illegal drugs, or abuse of legal drugs; 1.8. has bad ethics, criminal tendencies, and involvement in organized crime, which bears risk of weakness toward blackmail or can be seriously influenced under different pressures; 1.9. through concrete actions has expressed a lack of loyalty, trustworthiness, and security; 1.10. has committed a security breach or has repeatedly violated classified information security rules or has attempted and managed to perform an unauthorized activity in the classified information communication systems; 1.11. suffers from chronic mental illness. **Article 21** **Security Interview**1. APCI may conduct interviews with persons who have applied to be equipped with a PSC and security clearance procedures have been undertaken in this regard. 2. APCI may conduct interviews with third impartial parties, who know the past and the activities of the person who has been subject to Security clearance.**Article 22****Validity of PSC**1. The TOP SECRET PSC shall be valid for a 5 year period.2. The SECRET PSC shall be valid for a 7 year period.3. The CONFIDENTIAL PSC shall be valid for a 10 year period.**Article 23****Extending the PSC validity period in extraordinary emergent situations**1. Under exceptional emergency circumstances, the APCI has the right to extend an individual's PSC validity period only one time, for up to 60 calendar days during its validity cycle under the following conditions: 1.1 The individual, which requires the extension of the validity period, must have a valid PSC, issued in full procedure. The extensions of the validity period for a PSC issued under circumstances of extraordinary emergency are exempted. 1.2 There is an official request clarifying the circumstances of extraordinary emergency and proves that circumstances do not allow applying under normal procedures for re-equipped with a new PSC, when: 1.3 an individual is exercising a short-term official duty, for which it was impossible to follow the procedures according to foreseen time limits;1.4 an individual needs to participate in an unpredicted international activity, which has rendered impossible to follow the procedures according to foreseen time limits;1.5 an individual, who was equipped with a PSC, is in the circumstance that requires extending the time limits for participating in military missions abroad and it is impossible to apply according to normal procedures for re-obtaining a new PSC. The extension of the PSC validity period under the aforementioned conditions is allowed for the PSCs of “Confidential”, “Secret” and “Highly Secret” levels.2. All individuals to whom the PSC has been extended under extraordinary circumstances and conditions are obliged to state, in the writing, that they have understood all their obligations to protect the classified information.**Article 24****Repetition of Security Clearance** 1. The persons to whom a PSC has been issued are subject to new security clearances during the following regular intervals: 1.1. every ten (10) years for persons with PSC of security that allows them access to classified information at “CONFIDENTIAL” level; 1.2. every seven (7) years for persons with PSC of security that allows them access to classified information at “SECRET” level; 1.3 every five (5) years for persons with PSC of security that allows them access to classified information at “HIGHLY SECRET” level 2. The Verifying Authority or the head of the public institution, where the verified person is employed, may require that person to undergo a new Security clearance procedure even before the PSC validity expires, if there are indications that events have taken place or there are circumstances that raise doubts whether the verified person still constitutes an acceptable security risk.**Article 25****Refusal, Revocation, and temporary Suspension of PSC****1.** APCI shall take a decision on refusal, revocation or suspension of PSC in cases where they have received information inferring that the equipment or possession of PSC by a specific person constitutes an unacceptable security risk in referral to the general and fundamental criteria of security assessment. 2. The notification of the decision taken by APCI to refuse, revoke or suspend the PSC is communicated in writing to the head of the concerned public institution which has initiated the request for performing the Security clearance procedure.**Article 26****The Right to Appeal**1. The person, to whom the Personnel Security Clearance was refused, has the right to lodge a complaint before the APCI within 15 days from the date of receipt of the notice; 2. Complaints are reviewed by the Complaints Commission;**Article 27****Complaints Commission** 1. The Complaints Commission consists of 5 members with one representative of the following institutions:* 1. Ministry of KSF
	2. Ministry of Internal Affairs
	3. Kosovo Prosecutorial Council
	4. Kosovo Judicial Council;
	5. Kosovo Intelligence Agency

2. Upon the proposal by the heads of relevant institutions, the Government shall establish the Complaints Commission by virtue of a decision3. A person authorized by APCI presents the case before the members of the Complaints Commission  4. The mandate of the members of the commission is 3 years, with the possibility of extension5. The members of the Complaints Commission shall be professional, have high integrity and possess a PSC of adequate level compared to information that will be reviewed during the complaint procedure6. After reviewing the appeal, the Complaints Commission recommends the APCI Director to make a decision.7. The work rules and procedures of the Appeals Commission and other issues related to the review of complaints are regulated by a sub-legal act proposed by APCI and approved by the Government**Article 28****Deadlines and duration covering Security clearance** 1. The overall deadline for carrying out the procedures for verifying and issuing the PSC by APCI is up to 120 calendar days. 2. This period may be longer when verifications are conditional on the performance of proceedings in cooperation with other countries’ national security authorities.3. The security vetting covers a period of not less than the last 10 years. In cases when such a period is deemed insufficient, the verification shall extend from the age of 18 to the current age. 4. If the Vetting Authority is unable to collect and compile all required information to conduct Security clearance within the time limits specified in paragraph 1 of this Article, the Vetting Authority may, by means of a decision, extend the time limit up to 60 calendar days. The director of the respective institution shall be notified with the decision.**Article 29****Obligation of natural persons to protect classified information**1. Every person is obliged to protect classified information according to this law, regardless of how they have been granted access, received, or in any other form has managed to possess classified information. 2. When leaving a public institution, termination of employment relationship or any other contractual relationship, the official or the contracted person is prohibited from disclosing or removing classified information, in any way, from the control of the public institution. **Article 30****Inter-institutional cooperation** 1. While performing the Security clearance procedure, the Vetting Authority cooperates with other public institutions of the Republic of Kosovo, as appropriate. Other public institutions are obliged to provide information upon request.2. Cooperation between APCI and the Kosovo Intelligence Agency, the Ministry of Internal Affairs, the Ministry for the Kosovo Security Force and other public security institutions will be of primary importance. 3. While conducting the security clearance procedure, the Verifying Authority shall cooperate with other States’ counterpart institutions, as appropriate.**Article 31****Security clearance for KIA employees**1. The Security clearance for KIA employees is performed by KIA in accordance with the KIA law and by applying the criteria and standards established by this law regarding the security of personnel.2. APCI provides KIA employees with PSC at KIA's request.**Article 32****Security File**1. The Security Certificate, the completed security questionnaire and all other relevant documents and materials related to Security clearance are kept by the Vetting Authority in the security file.2. In addition to data specified under paragraph 1 of this article, the security file also contain information on subsequent changes regarding the information presented in the security questionnaire. 3. The head of the public institution and the verified person are obliged to immediately inform the Vetting Authority of any new development, events or circumstances that may result in the change of information provided in the security questionnaire or which in some other way may adversely affect the Security clearance of the concerned person.4. The Vetting Authority classifies and maintains the security file in a way that gives the security file the level of classification and protection it deems necessary to protect the security interests of Kosovo. **Article 33****Data processing**1. The Verifying Authority may process the personal data of the verified person contained in the security file only for the purpose of exercising his/her functions and responsibilities as defined by this Law. 2. The Vetting Authority does not transfer personal data contained in the security file to other public institutions, unless there is a priority public interest, without prejudice to security interests of the Republic of Kosovo, and only for the needs of: 2.1. activities related to law enforcement; 2.2. activities related to disclosure; 2.3. parliamentary investigations. 3. The public institution receiving such data may use and process them only if absolutely necessary and for the purposes specified under paragraph 2 of this Article and shall provide protection against unauthorized publication required for relevant classification level. 4. Law Enforcement agencies may use and process data specified in paragraph 2 of this Article for the purposes of criminal prosecution only as the last resort, when such data cannot be collected in other forms or if the criminal prosecution would be seriously hindered due to the lack of access to such data.**CHAPTER IV****INDUSTRIAL SECURITY****Article 34****Protection of classified information in the industrial field**1. Protection of classified information in the industrial field is done by determining measures and prevention procedures from unauthorized disclosure, loss, or violation of classified information security, which is dealt with under the terms of a classified project/program/contract/subcontract.2. Definition of standards when a natural or legal person has the ability to have access to classified information and possesses the necessary capabilities to administer this information before submitting an offer, negotiating, or participating in a classified contract, or work for a classified project, which includes access to classified information, is done in accordance with the requirements of the applicable legislation.**Article 35****The conditions for concluding a classified contract**1. Economic Operators interested in participating in procurement classified as ''TOP SECRET'', ''SECRET'' and ''CONFIDENTIAL'', should be previously equipped with the required ISC level. The personnel representing the Economic Operator in classified procurement and other individuals who will have access to classified information must be appropriately certified in accordance with the requirements of the applicable legislation.2. Economic Operators interested to participate in a classified procurement at the "LIMITED" level, are not equipped with ISC. 3. The personnel representing the Economic Operator in this procurement, and all persons who shall have access to Classified Information, are briefed and sign the non-disclosure statement with regard to classified Information prior to the commencement of classified procurement procedures.**Article 36****Obtaining an Industrial Security Clearance** 1. The ISC shall be issued by APCI, based on applicable legislation’s requirements 2. For Economic Operators of other countries, the ISC shall be issued by the National Security Authorities or any Competent Security Authority of the country where the Economic Operator is registered. This certificate is considered valid for the purpose of participating in a classified procurement, only after written confirmation by the APCI, addressed to the Contracting Authority. Prior to confirming the ISC, APCI cooperates with Counterpart Authorities to carry out the relevant verifications. 3. Only after receiving the confirmation by APCI, the Contracting Authority shall grant the Economic Operator the right of access to classified information.4. An economic operator providing security services may initiate procedures for provision with ISC before having a classified contract with public institutions, making a request to APCI with appropriate justifications for the needs of ISC.5. Procedures for protection of classified information in the industrial field are defined by a sub-legal act proposed by the APCI and approved by the Government.**Article 37****Basic criteria for assessment of industrial security**1. The verification procedures for issuance of ISC are carried out in accordance with the requirements of the applicable legislation and include aspects related to: 1.1 The Economic Operator's ownership structure, its financial viability, commercial reputation, technical capabilities and ability, as well as security aspects. 1.2 Owners/shareholders and managerial staff who, due to their functions, will have access to classified information; 1.3 The person proposed in the position of SO, his deputy and employee, who will have access to classified information.2. APCI has the right to request information that it deems necessary from state institutions to verify the potential security risk of the Economic Operator and the categories of persons involved in classified procurements or pursuant to a classified contract.**Article 38****Conditions for concluding classified sub-contracts**1. The Contractor shall, prior to commencing the negotiations for concluding classified sub-contracts, at any case, first obtain the written approval of the Contracting Authority. 2. The Contracting Authority is not allowed to authorize a Contractor with whom it has concluded a contract classified as ''TOP SECRET'', to enter into contractual relations under the terms of a classified sub-contract.3. All criteria for concluding/executing a classified contract are suitably applied with the subcontractor.**Article 39****Transportation and international visits**1. Transportation of classified material during implementation of the classified contract is carried out on land, sea, air and rail wayswayting se, first obtain the written approval of the Contracting Authority. , subject to the safety rules as required by applicable legislation.2. Classified Information security standards in the field of industrial security apply also during international visits.**CHAPTER I****SECURITY OF COMMUNICATION AND INFORMATION SYSTEMS****Article 40****Understanding the Security of Information Communication Systems**1. The security of classified information communication system is the set of standards for the protection of classified information, system services and resources in the means of communication that process, store or transmit classified information.2. APCI is a national security accreditation authority of the electronic communication system that processes, stores, or transmits classified information.**Article 41****Guaranteeing information security**1. Guaranteeing Information Security is the practice of guaranteeing information security and risk management related to the use, processing and transmission of information or data in systems or other processing used for this purpose.2. Guaranteeing information security is the protection of Communication and Information Systems in balance with the principles of Confidentiality, Integrity, Availability, Authentication and Non-Denial.**Article 42****Communication and Information Systems**1.Security management mechanisms and procedures are established to avoid, prevent, detect, resist, and recover from the impacts of incidents affecting classified information security objectives, including reporting security incidents. These measures include:1.1 Ensuring sufficient information to allow for investigation of intentional or accidental compromising of security objectives in accordance with the damage that may be caused;1.2 Reliable identification and authentication of persons, equipment and services authorized for access. The information controlling the access to the Communication and Information Systems shall be controlled and protected in compliance with the information classification level to which the system grants access. 1.3 Controls access to classified information in accordance with the "need to know" principle1.4 Management of integrity, origin and availability of classified information 1.5 Controlling of Communication and Information System connections that handle Classified Information;1.6 Determining the Communication and Information System’s security mechanisms reliability level;1.7 Assesses and verifies the proper functioning of the Information and Communication System’s security protection mechanisms, throughout their lifespan;1.8 Investigation of users and communication and information systems activities;1.9. Ensuring that the receiver of the message provides the sender with the acknowledgement of the message (non-deniability of message acknowledgement) and that the receiver is provided with the sender’s identity confirmation. **CHAPTER II - PHYSICAL SECURITY** **Article 43****Physical Security**1. Physical security shall mean the set of physical, technical, electronic and procedural measures undertaken for the purpose of safeguarding areas, buildings, offices, rooms, spaces and equipment where the Classified Information is produced, recorded, used, transmitted, stored, archived and destroyed.2. State institutions are obliged to take measures for physical security of areas, buildings, offices, rooms, spaces and equipment where classified information is produced, recorded, used, transmitted, stored, archived and destroyed, in accordance with the standards and procedures established by sub-legal acts, which are in compliance with relevant standards determined by the North Atlantic Treaty Organization and the European Union.3. The head of the institution shall approve the division of security areas by means of an Order, which shall be accompanied by the physical security plan and scheme of the building where classified information is stored and managed.4. State institutions where classified information is processed, shall establish security structures/security officers, depending on the volume of classified information.5. In cooperation with state institutions, APCI shall periodically conduct electronic disinfection of buildings, offices, rooms, and premises where the Classified Information is produced, recorded, used, transmitted, stored, archived and destroyed.6. The rules for the physical transport of classified information shall be defined by a sub-legal act.**Article 44****Classified Information Unit**1. Any public institution that produces and manages classified information must, within its own structure, appoint an officer or unit and provide the appropriate offices or premises where classified information is maintained and administered.2. Public institutions shall maintain Registers for classified information according to the model established by the Agency.3. The model for marking classified information shall be unique and determined by APCI and all public institutions shall be obliged to implement it. 4. The process of establishing, maintaining and managing the unit or concerned officer, offices or respective premises, including the maintenance of Registers for Classified Information, shall be determined by a sub-legal act approved by the Government, upon proposal of the Agency. **Article 45****Registers**Any head of a public institution that generates and manages classified information should establish minimum security standards for protection of classified information and appoint persons responsible for managing such information.**Article 46****Foreign** **information**1 State institutions shall safeguard classified information of foreign states or international organizations pursuant to standards that provide a degree of protection that is equivalent to that required by the state or international organization.2. Any institution shall, prior to the signing of an agreement or technical protocol involving the exchange of Classified Information, consider the opinion of APCI. 1. The signing of a technical agreement or protocol involving the exchange of classified information shall be preceded by the signature of a general agreement on the provision of classified information between the national security authorities of the States Parties.

**Article 47****NATO and EU classified information**1. The NATO and EU’s classified information Registry System shall consist of the Central Registry Office in APCI, the Sub-register Office of NATO and EU classified information, and control points established in the Ministry and state institutions. 2. NATO and EU classified information shall be exchanged and managed only through this System. 3. NATO and EU classified information Register System shall be responsible for the registration, distribution and administration of classified information exchanged in the framework of cooperation with NATO and the EU.4. State institutions shall be obliged to protect NATO and EU classified information according to standards that provide a level of protection equivalent to that required by NATO and the EU respectively.5. The Central Registry Office of NATO and EU classified information in APCI shall be the structure responsible for managing the exchange, oversight and control of the security aspects of NATO and EU classified information within the Register System.**Article 48****Unclassified information of NATO, the EU, other states and international organizations**Unclassified information of NATO, the EU, other states and international organizations shall be the information that does not contain any of the classification levels but is used only for official reasons by state institutions and is accessible to the public.**Article 49****Inspection of Public Institutions and Economic Operators** 1. APCI shall conduct inspections related to the implementation of security measures for the protection of classified information to public institutions and economic operators that have classified information.2. Inspection shall be carried out on a regular basis and with prior notice of public institution.3. Only those institutions or economic operators who have reliable information that there are security breaches regarding the management of classified information shall be subject to inspection without a prior notice. 4. The following disciplines shall be subject to inspection:4.1 Personnel security 4.2Industrial security 4.3 Security of communication systems and information4.4Physical security * 1. Administration of classified information

5. Upon completion of security measures inspection, the APCI shall compile a detailed report on the findings and propose to take appropriate measures for increasing the degree of classified information security.6. The report shall be addressed to the head of the respective public institution. 7. In coordination with the head of the public institution, a plan for the implementation of the recommendations resulting from the inspection report shall be drafted.8. The APCI shall monitor the implementation of recommendations in public institutions and in case they are not implemented within the foreseen deadlines, it shall notify in writing the direct supervisor of the relevant institution that was subject to inspection.**CHAPTER VI** **AGENCY FOR PROTECTION OF CLASSIFIED INFORMATION (APCI)****Article 50****Establishment of the Agency**1. Agency for Protection of Classified Information (APCI) shall be established as a national security agency in the field of protection of classified information for all public institutions of the Republic of Kosovo and their contractors who in any form may have classified information under administration.  2. The Agency for Protection of Classified Information and all employees and personnel engaged therein shall be politically impartial, professional, without prejudices in their judgments, and act only in accordance with the law and shall not take instructions from any person or institution.3. APCI shall be a central authority seated in Prishtina.**Article 51** **APCI responsibilities in the field of protection of classified information**1. APCI is an independent central institution in the field of protection of classified information with a mandate to organize, run and control the measures for storing, classifying and administering classified information and security verification for all RKS institutions as well as their contractors, which is responsible for:* 1. policy making
	2. monitoring of procedures
	3. oversight of institutions and contractors in classified contracts
	4. security education,
	5. providing staff
	6. physical security
	7. providing information
	8. industrial security
	9. providing communication and information systems

1.10 negotiating the conclusion of security arrangements with respective states 1.11 monitoring the implementation of treaties or international instruments on the protection of classified information and proposing the undertaking of measures related to it;2. The APCI shall be the competent security authority of the Republic of Kosovo regarding the protection of foreign countries and international organizations’ classified information3. APCI shall cooperate with public institutions, economic operators concerned and counterpart authorities of states and international organizations for carrying out the tasks provided under the legislation in force.4. APCI's strategic work plan shall contain general and specific objectives for achieving security standards for protection of classified information, which after being reviewed by the KSC, are proposed to the government for approval. 5. The internal organization and functioning of APCI shall be regulated by a sub-legal act proposed by APCI and approved by the Government.**Article 52****Agency for Protection of Classified Information** 1. APCI shall act based on this law in accordance with the Constitution and all other applicable laws in Kosovo.
2. APCI shall be a legal person.
3. APCI shall be a national security authority

**Article 53****Budget preparation and provision**1. The Director of APCI shall prepare and submit to the Prime Minister the draft annual budget for APCI.2. APCI shall be an autonomous budget organization with its own budget code.3. The Assembly of Kosovo shall provide APCI with an annual budget that is sufficient for performing duties and responsibilities aimed at protecting classified information in accordance with the applicable law.**Article 54****Appointment of the Agency’s Director** 1. The Prime Minister shall, after consultation with the President, appoint the Director of the Agency within twenty (20) working days from the day when the position remains vacant.2. The Director of the Agency shall be dismissed through the same process by which he/she was appointed.3. The Director of the Agency shall be appointed for a term of five (5) years, which may be renewed.4. The Director of the Agency, in accordance with this Law, the Rule on Internal Organization and other applicable laws, shall be responsible for all aspects of the management of the Agency. 1. In the execution of his/her responsibilities, the Director of the Agency shall be assisted by the Deputy Director, the Heads of Organizational Units and appropriately qualified personnel, as needed, in accordance with the rules and procedures set forth in this Law and the Regulation on Internal Organization.

**Article 55****Deputy Director of the Agency**1. The Deputy Director of the Agency shall assist the Director of the Agency and govern the activities of organizational units of the Agency under the supervision of the Agency’s director.2. The Deputy Director of the Agency must have a university degree and shall be appointed based on the proven professionalism, experience and regardless of political affiliation, for a five (5) year renewable term which shall run independently of the term of the Director of the Agency.3. Three (3) candidates for Deputy Director of the Agency shall be proposed by the Director of APCI to the Prime Minister for appointment.4. The Prime Minister of the Republic of Kosovo shall appoint the Deputy Director of the Agency within twenty (20) working days from the day the position becomes vacant.5. The Deputy Director of the Agency shall be dismissed through the same process by which he/she was appointed.6. The Deputy Director of the Agency shall temporarily act and exercise the powers of the Director of the Agency when the Director is absent or incapacitated. In the event of permanent incapacity, the Deputy Director of the Agency shall act and exercise the powers of the Director of the Agency until the replacement of the Director of the Agency is formally appointed.Article 56**Criteria for appointing the Director General**1. The criteria for appointing the General Director of APCI are as follows: * 1. to be a citizen of the Republic of Kosovo;
	2. to have a university degree;
	3. have at least 8 years of professional experience in security institutions, out of which at least (5) years of leadership experience;
	4. has not been convicted of a criminal offense by a final decision;
	5. has not been convicted for serious disciplinary violations, within the last five-year (5) period, during which he/she worked in public institutions
	6. does not have a conflict of interest with the position or as foreseen in the Law on Prevention of Conflict of Interest in Exercise of Public Function;

**Article 57****Director of the Agency**1. The Director of the Agency shall respond directly to the Prime Minister.2. The Director of the Agency shall:* 1. advise the Prime Minister of the Republic of Kosovo on matters related to the protection of classified information.
	2. report and notify the Prime Minister of the Republic of Kosovo on the activities of the Agency;
	3. provide information to the Prime Minister of the Republic of Kosovo regarding the classification of information and security vetting;
	4. protect and assist in the protection of classified information from unauthorized disclosure;
	5. establish and coordinate relations with foreign counterpart agencies;
	6. ensure that the Agency does not take any action that may give rise to reasonable doubt that the Agency is engaged in advancing, protecting or impairing the interests of any community or any political party or organization;
	7. ensure that the Agency does not take any action aimed at influencing political processes, public opinion and media in Kosovo;
	8. prepare the annual work report and propose the undertaking of necessary measures to increase the degree of classified information security;
	9. initiate and sign Memorandums of Understanding and Cooperation with other institutions and bodies;
	10. report to the relevant parliamentary committee at least once a year;

 **Article 58****Specific Requirements for Agency’s Employees**1. Individuals selected for employment with the Agency shall meet the strict security standards which are determined in accordance with the applicable law and in accordance with the procedures set out in the regulations promulgated by the Agency's Director and approved by the Government. The candidate must be stable, trustworthy, have an excellent character, judgment, and exercise discretion. Any doubt related to any of the above-mentioned factors is in favour of Kosovo's security. 2. The Agency shall not hire the candidates who fail to meet the security requirement.3. In addition to the general employment requirements applicable to other government employees, special conditions may apply to the employees of the Agency with regard to expertise, health, work duties and security requirements which are consistent with Kosovo's security interests.4. The Regulation on Agency's Internal Organization shall set out the requirements for each position in the Agency and shall set out the specific requirements for employment in the Agency.5. In accordance with the internal rules, the Agency may contract third parties for ancillary services, where appropriate.**Article 59****Qualifications for Employment at the Agency**1. The Agency shall not recruit candidates who fail to meet the following requirements:* 1. be a citizen of Kosovo;
	2. have appropriate academic and professional qualifications as set out in the Regulation on Internal Organization;
	3. carry out the medical examination required for the position;
	4. be exempt from military service, if applicable; and
	5. be able to meet the security requirements to be determined by this law and bylaws.

2. Rules and procedures on general requirements and recruitment procedures, employment relationships, training, career advancement and appointments of positions are set out in the Regulation on Employment Relationship in APIC, approved by the Government.**Article 60****Status of APIC employees**AMIK employees shall have special status under this law. For issues not regulated by this law or the sub-legal acts deriving from this law, the legislation regulating civil service matters shall be appropriately applied. **Article 61****Rights of Agency's Employees**1. The employees of the Agency shall be entitled to:* 1. permanent employment until retirement, with the exception of individuals who have fixed-term employment contracts as well as those who are dismissed on reasonable grounds, in accordance with the legislation in force;
	2. leave in accordance with the legislation in force and resume the same or similar work when the leave ends;
	3. remuneration for duties and performance of duties as defined by this law;
	4. salary and payments in accordance with the legislation in force;
	5. career advancement and professional development through training and other means;

**Article 62****Prohibited Employees’ Behaviours** 1. The Agency’s employees cannot be members of political entities or receive instructions from them or individuals outside the Agency, and may not publicly express their political beliefs and preferences.2. The employees may not perform any other paid public or professional activities or duties, which are inconsistent with the work of the Agency, or create conflicts of interest.3. The Agency's employees cannot be employed elsewhere as long as they have employment relations with the Agency. 4. The Agency's employees are not entitled to actions aimed to stop the working activity or other forms aimed to collectively stop the work activity.5. The Agency’s employees, without prior consent of the Director of the Agency, may not make public statements or otherwise comment on the work of the Agency, or provide information to unauthorized persons on the data, documents, contacts, intentions, knowledge or staff of the Agency. 6. If an employee is running in the elections for the Assembly of the Republic of Kosovo or for local government bodies, the same shall seek release from duty and may no longer be readmitted to the Agency.**Article 63****Employee’s Personal Legal Obligations** 1. Each employee of the Agency shall perform the duties assigned in accordance with this Law and other relevant laws, and shall be personally responsible for the lawful implementation of Agency's duties as defined by this Law and which are within the duties given to certain employees.2. If an employee believes he/she received an unlawful order, he/she shall inform the issuer of the order about his/her concern.3. In case the instructor reiterates the order, the employee shall request a written confirmation of such order. If the employee still hesitates to execute the order, he or she shall convey the order to the principal supervisor of the issuer of the order and report the case to the Director.4. The employee shall protect and shall not disclose, unless authorized, classified information that he or she has become aware on or off duty. This is an obligation that continues even after termination of employment relationship with the Agency; 5. The employee shall not use the information obtained while on duty for purposes other than those set forth by law; 6. The employee shall protect and shall not disclose personal data and data related to the professional activity of people, which is protected by law and for which he/she has become aware while on duty. **Article 64** **Salaries and Remuneration for the Agency's Employees**  1. Salaries and additional remuneration for the Agency's staff shall be set out in the sub-legal act proposed by the Director and approved by the Government;2. In addition to the basic salary, the APCI employees may be entitled to other forms of allowances, such as wages and benefits, based on factors that include work-related difficulties, overtime or special skills;  3. In case of death on duty or due to exercising the duties within APCI, the Government shall pay to the late employee's family or legal heir(s) the monthly salary of APCI's employee for a period of one (3) year from his/her death;**Article 65****Termination of Employment**1. Employment of the Agency's employees may be terminated as follows:* 1. voluntary resignation from the Agency;
	2. termination of contract;
	3. retirement age;
	4. permanent disability to perform official duties due to health conditions, provided that the employee cannot be transferred to another appropriate position within the Agency;
	5. loss of Kosovo citizenship;
	6. final conviction for a criminal offense.
	7. dismissal from the Agency due to disciplinary proceedings.

**Article 66****Identity Cards**The Agency's employees shall be provided with identity cards. The type, form and content of this identity card shall be determined upon a decision issued by the Director of APCI.**Article 67****Regulation on Internal Organization**The internal organization of the Agency shall be defined by the Regulation on Internal Organization, which is approved by the Government.**Article 68****Implementation of EU and NATO standards**1. APCI is the Security Authority of the Republic of Kosovo responsible for fulfilling security standards on protection of classified information in accordance with the requirements deriving from the NATO and EU security directives.2. The Agency exchanges classified information with all NATO and EU member states as well as other states. 3. According to NATO and EU directives, the Agency recognizes the personnel security clearance and industrial security clearance certificates of the states with which have signed security agreements.**CHAPTER III****SECURITY BREACHES AND COMPROMISE OF CLASSIFIED INFORMATION****Article 69**1. A security breach shall occur as a result of an act or omission by an individual which constitutes a violation of the security rules set forth in this Law and other sub-legal acts.2. The compromising of classified information shall occur when information is completely or partially disclosed to an unauthorized person as a result of a security breach.3. Any security breach or suspicion thereof shall be reported immediately to the APCI's security authority.4. When known, or when there are sufficient reasons to allege that classified information has been compromised or lost, the security authority shall take measures in accordance with the law and sub-legal acts, by: * 1. informing the originating authority
	2. ensuring that the case is being investigated by a neutral person to the matter
	3. determining the potential damage caused to the interests of the Republic of Kosovo or other states and organizations
	4. shall take appropriate measures to prevent recurrence
	5. shall notify the relevant authorities of the action taken

5. Any individual who violates the security rules set forth in this Law and sub-legal act shall be liable to disciplinary penalties in accordance with the legislation in force.6. Any individual who compromises or losses classified information shall be liable to disciplinary penalties or legal actions in accordance with the applicable laws and sub-legal acts. **CHAPTER VII****PROTECTION OF FILES AND DATA****Article 70****Loss of Classified Information**1. For any type of loss, alleged loss, breach or alleged breach of classified information security or in case of an unauthorized actual or alleged access to classified information, all authorized holders of classified information shall immediately report to their respective public institution, State Prosecutor's office and the Agency. 2. The Agency shall, upon its own initiative or following the request of the appropriate authority, in cases of violations referred to in this Law, shall immediately take all necessary measures to:2.1 investigate the case,2.2 identify the cause of loss,  2.3 track any access by unauthorized individuals to such information, 2.4 remove any harmful effects and prevent further loss of classified information,3. If the alleged violation is suspected of constituting a criminal offense, it shall notify the State’s Prosecutor Office. **CHAPTER VIII****Article 71****Criminal Sanctions**1. A person who, without authorization, publishes information classified as “CONFIDENTIAL” under this Law, and any authorized holders of such classified information who fails to protect classified information as required by this Law, shall be considered to have committed a criminal offense and shall be punished by imprisonment of one (1) to five (5) years.2. A person who, without authorization, publishes information classified as “SECRET” under this Law and any authorized holder of such classified information who fails to protect classified information as required by this Law shall be considered to commit a criminal offense and shall be punished by imprisonment of three (3) to ten (10) years. 3. A person who, without authorization, publishes information classified as “TOP SECRET” under this Law, and any authorized holder of such classified information who fails to protect classified information as required by this Law shall be considered to have committed a criminal offense and shall be punished by imprisonment of five (5) to twelve (12) years.**ARTICLE 72****TRANSITIONAL AND FINAL PROVISIONS**1. Upon appointment, the Director of APCI, in cooperation with the Director of KIA, shall commence the procedures of relocating the Verification Department, together with respective files, to APCI.2. Current employees of the former Security Verification Department within KIA shall have the right to choose, through a voluntary declaration, if they want to work in APCI or remain within the KIA structures.3. Employees of the former Security Audit Department within KIA, who are to start work in APCI, shall have the right of having their experience at KIA recognized.4. The Director of APCI, upon an agreement with the Director of KIA, may use KIA assets until the completion of APCI staff. 5. The Government shall provide an appropriate facility with security standards in view of achieving the APCI’s mandate to protect the classified information of the Republic of Kosovo. 6. Upon entry into force of this Law, the term KIA, used in the sense of the Vetting Authority, shall be replaced by APCI in any provisions of the laws and sub-legal acts.**Article 73****Sub-Legal Acts** The Government shall adopt sub-legal acts for implementation of this law within one (1) year from its entry into force.**Article 74** **Repeal**Entry into force of this law shall repeal the Law No. 03/L-178 on Classification of Information and Security Clearances (Official Gazette of the Republic of Kosovo, No. 76, 10 August 2010)**Article 75****Entry into force**This law shall enter into force fifteen (15) days after its publication in the Official Gazette of the Republic of Kosovo.**Kadri Veseli****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Assembly President of the Republic of Kosovo  | **Skupština Republike Kosovo,**Na osnovu člana 65 (1) Ustava Republike Kosova, Usvaja:**ZAKON O ZAŠTITI KLASIFIKOVANIH INFORMACIJA****POGLAVLJE I****OPŠTE ODREDBE****Član 1****Cilj**1. Cilj ovog zakona je uspostavljanje jedinstvenog sistema za zaštitu klasifikovanih informacija koje se odnose na interese bezbednosti Republike Kosovo.2. Ovim zakonom se osniva Agencija za zaštitu klasifikovanih informacija (u daljem tekstu: AZKI) gde se utvrđuje njena misija, organizacija, funkcionisanje, dužnosti i odgovornosti3. Ovaj zakon je u saglasnosti sa EU legislaciju, kao sto sledi:3.1 Odluka Vijeća od 23. rujna 2013 o sigurnosnim propisima za zaštitu lasificiranih podataka EU-a (2013/488/EU)3.2 Uredba (Eu) 2016/679 Europskog Parlamenta I Vijeća od 27. travnja 2016. o zaštiti ojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)**Član 2****Delokrug**Ovaj zakon se odnosi na sve javne institucije koje obavljaju izvršne, zakonodavne i sudske nadležnosti, na fizička i pravna lica, koja na osnovu principa “nužnost pristupa informacijama”, u vršenju dužnosti mogu imati pristup klasifikovanim informacijama Republike Kosovo, država i drugih međunarodnih organizacija.**Član 3****Definicije**1. Izrazi upotrebljeni u ovom zakonu imaju sledeće značenje:1.1. **Klasifikovana informacija,** je svaki dokument ili materijal, bez obzira na formu, prirodu ili način njenog prenošenja, pripremljena ili koja se priprema, za koju je postavljen određeni stepen klasifikacije u interesu Republike Kosovo i u skladu sa važećim zakonodavstvom koje zahteva zaštitu od bilo koje povrede, prisvajanja, širenja, gubitka ili pristupa bilo kog neovlašćenog lica i bilo koje druge vrste kompromitovanja bezbednosti;1.2. **Pristup -** sposobnost ili mogućnost za sticanje saznanja o klasifikovanoj informaciji;1.3. **Nužnost pristupa informacijama -** je nužnost za pristupom klasifikovanim informacijama, u okviru određene pozicije i u cilju ispunjavanja specifične dužnosti;1.4. **Klasifikacija** - akt ili proces putem kojeg se informaciji određuje stepen klasifikacije i rok čuvanja ove klasifikacije;1.5. **Agencija -** Agencija za zaštitu klasifikovanih informacija (AZKI);1.6. **Organ za nacionalnu bezbednost**, je unutrašnji državni organ jedne države odgovoran za kontrolu i sprovođenje standarda bezbednosti klasifikovanih informacija. AZKI je Organ za nacionalnu bezbednost u Republici Kosovo.1.7. **Organ za proveru**, je Agencija za zaštitu klasifikovanih informacija, kao specijalizovana strukturna jedinica za vršenje bezbednosnih provera lica koja će saznati, proizvoditi, čuvati, upravljati, transportovati i prenositi klasifikovane informacije;1.8. **Bezbednosni upitnik**, je obrazac koji popunjava svako lice koje zahteva da se upozna sa klasifikovanim informacijama i na osnovu kojeg se vrši bezbednosna provera i ocenjuju podaci za izdavanje ili neizdavanje "Bezbednosne dozvole za osoblje".1.9. **Bezbednosna dozvola za osoblje (**BDO), je službeni dokument AZKI-a ili nadležnog organa bezbednosti druge zemlje, koji potvrđuje sa stanovišta bezbednosti da lice ispunjava uslove utvrđene za saznanje, čuvanje, upravljanje i prenos klasifikovanih informacija.1.10. “**Brifiranje”/“Debrifiranje**”, su skup instrukcija i bezbednosnih uputstava u vezi sa procedurama bezbednosti klasifikovanih informacija i individualne odgovornosti za kršenja pravila bezbednosti, kojima se podvrgavaju lica koja traže da imaju mogućnost saznanja klasifikovanih informacija ili su opremljeni sa BDO.1.11 **Povreda bezbednosti**, je radnja ili propust u suprotnosti sa važećim zakonodavstvom koje dovodi ili može dovesti do krađe, gubitka, oštećenja, kompromitovanja ili neovlašćenog širenja klasifikovanih informacija.1.12 **Bezbednosna provera**, predstavlja skup mera i procedura koje se primenjuju prema fizičkom ili pravnom licu, na osnovu kojih će biti procenjeno izdavanje, odbijanje, privremeno obustavljanje ili ukidanje "Bezbednosne dozvole za osoblje".1.13 **Neprihvatljiv bezbednosni rizik**, smatraju se okolnosti opisane u ovom zakonu, na osnovu kojih AZKI odbija izdavanje BDO ili procenjuje da mora preduzeti meru njenog privremenog ukidanja ili obustavljanja.1.14 **Okolnosti vanredne situacije**, se smatraju uslovi objektivne nemogućnosti za praćenje normalnih procedura za dobijanje BDO, zbog vršenja kratkoročne službene dužnosti za učešće u nepredviđenim međunarodnim aktivnostima, produženje rokova vojnih misija u različitim zemljama itd.1.15 **Službenik za bezbednost**, u nastavku SB, je odgovorno zaposleno lice ili struktura koja je postavljen od strane rukovodioca ministarstva ili državne institucije za nadzor i sprovođenje zahteva za bezbednost osoblja i drugih disciplina klasifikovanih informacija;1.16 **Ekonomski operater** - podrazumeva bilo koje fizičko ili pravno lice ili bilo koju grupu takvih lica, koja obezbeđuju isporuku robe, radova i/ili usluga na tržištu;1.17 **Autoritet za klasifikaciju** – predsednik, predsednik Skupštine, premijer, predsednik Vrhovnog suda i glavni državni tužilac, direktor OAK, ministar unutrašnjih poslova, ministar MKSB-a, komandant KSB-a, generalni direktor policije kao i bilo koja osoba ovlašćena od strane njih koja ima originalno ili povereno ovlašćenje da klasifikuje informacije,1.18 **Klasifikovani ugovor -** bilo koji ugovor zaključen od strane javne institucije koji sadrži klasifikovane informacije prema ovom zakonu;1.19 **Deklasifikacija -** ovlašćena izmena statusa informacija iz klasifikovanih informacija u neklasifikovane informacije;1.20 **Dokument -** bilo koje fizičko ili elektronsko sredstvo na kome je zapisana informacija.1.21 **Degradacija -** odluka da se klasifikovane i sačuvane informacije na određenom stepenu klasifikuju i čuvaju na nižem stepenu klasifikacije.1.22 **Informacije strane Vlade** podrazumeva:1.22.1. informacije koje je Republici Kosovo dostavila strana vlada ili međunarodna vladina organizacija;1.22.2. informacije koje su proizvedene od strane Republike Kosovo u skladu sa ili kao rezultat zajedničkog sporazuma sa stranom vladom ili međunarodnom vladinom organizacijom sa očekivanjem ili zahtevom da se takve informacije, sporazum ili oboje zadrže u tajnosti.1.23. **Materijal -** dokumenta kao i svaka mašina, oprema ili naoružanje koje je proizvedeno ili se proizvodi.1.24. **Obrada -** svaka radnja ili niz radnji koje se obavljaju na ličnim podacima, sa ili bez automatskih sredstava, kao što su prikupljanje, snimanje, organizovanje, čuvanje, prilagođavanje ili ispravka, traženje, konsultovanje, korišćenje, objavljivanje prenosom, širenje ili bilo koji drugi oblik stavljanja na raspolaganje, usklađivanje ili kombinovanje, blokiranje, brisanje ili uništavanje.1.25. **Javna institucija -** sve institucije i organi utvrđeni u članu 2.1 ovog zakona.1.26. **Bezbednosni interesi -** odnosi se na odbranu, aktivnosti sprovođenja zakona i obaveštajne aktivnosti, spoljne ili bezbednosne odnose Republike Kosovo, uključujući njen teritorijalni integritet, integritet njenih institucija, ustavni poredak kao i stabilnost i ekonomski razvoj.1.27**. Supružnik -** svaki odnos stvoren putem zakonskog braka a za potrebe ovog zakona uključuje i bilo koji vanbračni odnos između dva fizička lica.1.28. **Rukovodilac javne institucije -** izabrani zvaničnici na izbornim pozicijama u javnim institucijama i službenici imenovani od strane izabranih zvaničnika.1.29. **Ovlašćeni nosioci klasifikovanih informacija -** osoba koja poseduje klasifikovane informacije, ima validan BDO i ispunjava druge uslove koji dozvoljavaju pristup klasifikovanim informacijama, osim ako zakonom nije drugačije utvrđeno.1.30 "**Ugovorni organ**", podrazumeva bilo koji državni subjekat koji se obavezuje da izvrši klasifikovanu nabavku i stupi u ugovorni odnos.1.31 "**Ekonomski operater**", podrazumeva bilo koje fizičko ili pravno lice ili bilo koju grupu takvih lica, koja obezbeđuju isporuku robe, radova i/ili usluga na tržištu.1.32 "**Klasifikovani ugovor**", podrazumeva bilo koji ugovor, podugovor, čije sprovođenje zahteva pristup klasifikovanim informacijama ili korišćenje, čuvanje, upravljanje, promet, prenos i transport klasifikovanih informacija ili materijala.1.33 "**Ugovorna strana**" podrazumeva svako fizičko ili pravno lice koje ima pravnu sposobnost da pregovara i zaključuje klasifikovane ugovore.1.34 **Bezbednosna dozvola za osoblje –** je službeni dokument AZKI-a, odnosno nadležnog organa bezbednosti druge zemlje, kojim se potvrđuje, sa bezbednosne tačke gledišta, da fizičko lice predstavlja prihvatljiv rizik za pristup klasifikovanim informacijama1.35 "**Sertifikat industrijske bezbednosti**", dalje: SIB je službeni dokument AZKI-a, odnosno nadležnog organa bezbednosti druge zemlje, kojim se potvrđuje, sa bezbednosne tačke gledišta, da ekonomski operator, ima kapacitet i organizacione, tehničke, fizičke sposobnosti i da zadovoljava standarde utvrđene za saznanje, čuvanje i upravljanje klasifikovanim informacijama u projektu/programu ili klasifikovanom ugovoru/podugovoru.**POGLAVLJE II - BEZBEDNOST INFORMACIJA****Član 4****Autoritet za klasifikaciju**1. Autoritet za klasifikaciju informacija vrši:* 1. Predsednik
	2. Predsednik Skupštine
	3. Premijer
	4. Predsednik Vrhovnog suda
	5. Glavni državni tužilac
	6. Direktor OAK-a
	7. Ministar unutrašnjih poslova
	8. Ministar MKSB-a
	9. Komandant KSB-a
	10. Generalni direktor Policije

2. Autoriteti za klasifikaciju informacija propisani u stavu 1. ovog člana, imaju pravo da prenose nadležnost klasifikacije rukovodiocima institucija pod njihovim nadzorom.3. Zahtev za davanje ovlašćenja od strane Autoriteta za klasifikaciju dostavlja se AZKI, koja nakon razmatranja i procenjivanja, preporučuje davanje ili nedavanje ovlašćenja.4. Svako ovlašćenje nadležnosti za klasifikaciju vrši se pismeno i jasno identifikuje rukovodioca po imenu i nazivu položaja, a ovo ovlašćenje važi samo za vreme dok je rukovodilac odgovarajuće institucije.5. Svaki rukovodilac odgovarajuće institucije ne može izvršiti klasifikaciju informacija institucije i odgovarajućih jedinica pod njegovim nadzorom, bez ovlašćenja od strane Autoriteta za klasifikaciju.6. Agencija izrađuje, održava i redovno ažurira registar sa imenima rukovodilaca koji imaju nadležnost za klasifikaciju.**Član 5****Kategorije klasifikovanih informacija** 1. Informacije se klasifikuju samo ako je potrebno i spadaju u jednu ili više od ovih kategorija:1.1 projekti, planovi, sistemi ili operacije koje se odnose na zaštitu i bezbednost ustavnog poretka Republike Kosovo;1.2 informacije stranih vlada, odnosi ili međunarodne aktivnosti Republike Kosovo, koje će biti zaštićeni od neovlašćenog izlaganja.1.3 aktivnosti, izvori informacija i metode obaveštajnih institucija vezanih za bezbednost Republike Kosovo.1.4 sistemi, instalacije, infrastruktura, projekti, planovi ili usluge odbrane vezane za bezbednosne interese Republike Kosovo;1.5 naučne, tehnološke, ekonomske, finansijske aktivnosti vezane za bezbednosne interese Republike Kosovo; 1.6. kriptološki sistemi; kriptološka pitanja/problemi1.7. operativni planovi i korišćenje sistema klasifikovanih informacija i kriptologije;1.8. procene rizika/izveštaji o inspekciji vezani za nedostatke sistema kriptologije;1.9. planovi za identifikaciju, smanjenje i upravljanje rizikom koji se javlja u sistemu elektronske komunikacije.1.10. planovi, projekti, programi za obezbeđivanje komunikacionih sistema klasifikovanih informacija;1.11. informacije prikupljene putem specifičnih operacija i elektronskog presretanja.**Član 6****Zabrana klasifikacije informacija**1. Klasifikacija informacija je zabranjena kada se to radi sa ciljem:1.1. skrivanja kršenje zakona, zloupotrebu ovlašćenja, neefikasnost ili administrativnu grešku;1.2. lišavanja prava saznanja licu, organizaciji ili instituciji;1.3. sprečavanja ili odlaganja pružanja informacija koje ne zahtevaju zaštitu u interesu bezbednosti Republike Kosovo.1.4. zaustavljanja konkurencije.**Član 7****Stepeni klasifikacije**1. Informacije na osnovu sadržaja, vrednosti i državnog interesa klasifikuju se na jedan od sledećih stepena:1.1. "STROGA TAJNA", čije širenje i neovlašćeno otkrivanje prema razumnoj proceni bi izazvalo izuzetno tešku štetu bezbednosnim interesima Republike Kosovo;1.2. "TAJNA", čije širenje i neovlašćeno otkrivanje bi ozbiljno ugrozilo bezbednosne interese Republike Kosovo;1.3. "POVERLJIVO", čije širenje i neovlašćeno otkrivanje bi mogli ugroziti bezbednosne interese Republike Kosovo;1.4. "OGRANIČENO", čije širenje i neovlašćeno otkrivanje bi bilo nepovoljno za bezbednosne interese Republike Kosovo.2. Autoritet za klasifikaciju izbegava prekomernu klasifikaciju informacija i dodeljuje im samo takav stepen klasifikacije koji je potreban da bi se zaštitili interesi Republike Kosovo.3. Procedure klasifikacije informacija, uključujući klasifikaciju delova dokumenata, odvojenih dokumenata i oznake koje nose klasifikovane informacije utvrđuju se podzakonskim aktom koji predlaže AZKI i odobrava Vlada.**Član 8****Trajanje klasifikacije**1. Informacije se klasifikuju sve dok to zahteva bezbednosni interes Republike Kosovo.2. Vremenski rokovi čuvanja klasifikacije su:2.1. klasifikovane informacije: "OGRANIČENO" jednu (1) godinu;2.2. klasifikovane informacije: "POVERLJIVO" pet (5) godina;2.3. klasifikovane informacije: "TAJNA" petnaest (15) godina; i2.4. klasifikovane informacije: "STROGA TAJNA" pedeset (50) godina.3. Izračunavanje vremenskog roka čuvanja klasifikacije počinje od dana proizvodnje klasifikovane informacije.4. Ako Autoritet za klasifikaciju smatra da informacije treba zaštititi duže nego što je propisano u stavu 2, on izdaje novu odluku o klasifikaciji u skladu sa članom 8. ovog zakona. Takva odluka ne sme se doneti ranije od šest (6) meseci pre datuma predviđenog za deklasifikaciju iz stava 1. ovog člana.**Član 9****Uslovi za proizvodnju, upotrebu i promet klasifikovanih informacija**1. Proizvodnja klasifikovanih informacija se vrši samo na osnovu spiska klasifikovanih informacija koje je odobrio Autoritet za klasifikaciju, u skladu sa postupkom utvrđenim važećim zakonodavstvom2. Proizvodnja, upotreba, umnožavanje, prenos, fizički transport, arhiviranje, čuvanje i uništenje klasifikovanih informacija vrši se u skladu sa sledećim standardima:2.1. Bezbednosna provera osoblja;2.2. Fizička bezbednost;2.3. Bezbednost informacija;2.4. Industrijska bezbednost;2.5. Bezbednost informacionih i komunikacionih sistema.3. Postupci za sprovođenje ovog člana regulišu se podzakonskim aktom koji predlaže AZKI i odobrava Vlada.**Član 10****Deklasifikacija**1. Informacije se deklasifikuju kada više nema potrebe za zaštitom i kada njihovo objavljivanje više ne predstavlja pretnju za bezbednost Republike Kosovo2. Autoritet za klasifikaciju, od kojeg klasifikovane informacije potiču, vrši njihovu deklasifikaciju.3. Slučajevi deklasifikacije klasifikovanih informacija su:3.1 kada je njihovo objavljivanje diktirano državnim interesima koji su važniji od potrebe da se one klasifikuju;3.2. pojava događaja ili određenog datuma kako je utvrđeno od strane Autoriteta za klasifikaciju.4. Neovlašćeno širenje i otkrivanje klasifikovanih informacija ne predstavlja razlog za njihovu deklasifikaciju.5. Autoritet za klasifikaciju koji je izvršio deklasifikaciju informacija dužan je da obavesti sve institucije koje poseduju klasifikovane informacije;6. Procedure za sprovođenje ovog člana regulišu se podzakonskim aktom koji predlaže AZKI i odobrava Vlada.**Član 11****Uništavanje klasifikovanih informacija**1. U svakoj državnoj instituciji rukovodilac institucije ili njegov ovlašćeni predstavnik uspostavlja komisije za uništavanje klasifikovanih informacija.2. Komisija za uništavanje razmatra i odlučuje o uništavanju klasifikovanih informacija kada ove informacije nemaju vrednost za dalje čuvanje i ne moraju biti deklasifikovane.3. Komisija za uništavanje na osnovu svojih odluka, vrši sve postupke za uništavanje klasifikovanih informacija i priprema završni izveštaj. 4. Informacije koje se moraju dostaviti arhivskoj mreži ne smeju se uništavati, već se deklasifikuju.5. Procedure za sprovođenje ovog člana regulišu se podzakonskim aktom koji predlaže AZKI i odobrava Vlada.**Član 12****Degradiranje i povećanje stepena klasifikacije**1. Autoritet za klasifikaciju, od kojeg potiču klasifikovane informacije, odgovoran je za degradiranje ili povećanje stepena klasifikacije takvih informacija.2. Nadležni Autoritet za klasifikaciju degradira ili podiže stepen klasifikacije ako je upoznat sa činjenicama koje jasno ukazuju da klasifikovane informacije ne zahtevaju stepen zaštite koji se dodeljuje prema postojećem stepenu klasifikacije.**Član 13****Predlog građana**1. Kada građanin ili službenik Republike Kosovo, koji nema ovlašćenje za klasifikaciju, procenjuje da određene informacije pod kontrolom države imaju potrebne vrednosti da budu klasifikovane, predlaže odgovarajućoj instituciji klasifikaciju ovih informacija. Ova institucija odlučuje u roku od 10 dana da li će se informacije klasifikovati ili ne i obaveštava građanina ili službenika o donetoj odluci.2. Od trenutka predloga za klasifikaciju odgovarajućih informacija, njihov posednik je obavezan da štiti informacije od neovlašćenog pristupa**POGLAVLJE III – BEZBEDNOSNA PROVERA OSOBLJA****Član 14****Bezbednosna provera osoblja**1. Bezbednosna provera osoblja je skup mera i postupaka na osnovu kojih se procenjuje da li lice, pridržavajući se lojalnosti, pouzdanosti i bezbednosti, može biti ovlašćeno za pristup klasifikovanim informacijama, bez ugrožavanja bezbednosti ovih informacija.2. Izdavanje, odbijanje, privremeno obustavljanje ili ukidanje "Bezbednosne dozvole osoblja" (u daljem tekstu: BDO), vrši se u skladu sa stavom 1. ovog člana.3. Procedure za sprovođenje ovog člana regulišu se podzakonskim aktom koji usvaja Vlada.**Član 15****Bezbednosna dozvola za osoblje**1. Autoritet za verifikaciju izdaje BDO samo licu koje je, nakon obavljanja postupka bezbednosne provere u skladu sa važećim zakonodavstvom, utvrđeno kao prihvatljivi rizik za bezbednost.2. BDO jasno ukazuje na stepen klasifikovanih informacija, kojem lice koje je prošlo proceduru bezbednosne provere može imati pristup. BDO za određeni stepen klasifikacije daje nosiocu pristup i informacijama sa nižim stepenom klasifikacije3. Svaki rukovodilac javne institucije je dužan da u roku od 15 dana sprovede odluku Organa za proveru i neće obezbediti pristup klasifikovanim informacijama licu kojem je uskraćen BDO.**Član 16****Kriterijumi za saznanje klasifikovanih informacija**1. Pravo na saznanje, čuvanje, upravljanje i prenos klasifikovanih informacija imaju samo lica, koja:1.1 obezbede pravo saznanja od strane rukovodioca institucije ili službenika za industrijsku bezbednost izvođača radova zbog dužnosti koju obavljaju;* 1. imaju potpunu poslovnu sposobnost;

1.3 su prethodno obaveštena o saznanju postupaka bezbednosti klasifikovanih informacija i individualnih odgovornosti za kršenja bezbednosti i koji su potpisali izjavu o čuvanju informacija;1.4 su dobila BDO, osim za slučajeve saznanja o klasifikovanim informacijama na nivou "Ograničeno".2. Samo predsednik Republike Kosovo, predsednik Skupštine i premijer imaju ovlašćenje da imaju pristup klasifikovanim informacijama radi obavljanja svoje službene dužnosti bez ispunjavanja uslova utvrđenih u stavu 1. ovog člana, pod uslovom da imaju potrebu da budu upoznati sa ovim informacijama.**Član 17****Spisak funkcija/pozicija za saznanje klasifikovanih informacija**1. Državne institucije koje, zbog svoje delatnosti koju izvršavaju, proizvode klasifikovane informacije ili, u toku saradnje sa drugim institucijama dobijaju ovu kategoriju informacija, dužne su da odobre i pošalju u pisanoj formi AZKI-u spisak funkcija/pozicija koje zbog službenih dužnosti mogu biti upoznate sa klasifikovanim informacijama i odgovarajućim nivoom BDO-a.2. Pregled ovih spiskova vrši se periodično i u skladu sa promenama organizacione strukture odgovarajuće institucije. O svakoj eventualnoj promeni, rukovodilac institucije je dužan da obavesti AZKI.**Član 18****Uslovi za početak bezbednosne provere**1. Bezbednosna provera počinje tek nakon što je podnosilac zahteva prihvatio i dao pismenu saglasnost za prikupljanje podataka i izvršenje procedura bezbednosne provere, u skladu sa zahtevima bezbednosnog upitnika. 2. Tretiranje ličnih podataka i informacija prikupljenih u procesu bezbednosne provere vrši se u skladu sa zahtevima važećeg zakona o zaštiti ličnih podataka.**Član 19****Opšti zahtevi za bezbednosnu procenu**1. AZKI, kao jedini organ za verifikaciju u Republici Kosovo odgovoran za sprovođenje procedure bezbednosne provere treba da se pridržava opštih zahteva za bezbednosnu procenu, koji su dati u nastavku, ali ne ograničavaju se na sledeće:  1.1. Tačna provera identiteta, generalija i statusa državljanstva u prošlosti i sadašnjosti, za svaku osobu;1.2. Kontrola podataka, u funkciji bezbednosti Republike Kosovo. 1.3. Finansijski status podnosioca zahteva, kako bi se utvrdilo da li može biti pod pritiskom zbog nestabilnosti, ozbiljnih finansijskih poteškoća ili posedovanja bilo koje neopravdane imovine. 1.4. Informacije o obrazovanju osobe nakon 18 godina starosti ili za period koji se smatra odgovarajućim od strane organa za verifikaciju.1.5. Informacije o zapošljavanju pojedinca uzimajući u obzir reference ranijih radnih mesta, na osnovu izveštaja poslodavaca.  1.6. Informacije o učešću u vojnim operacijama ili trajanje službe u oružanim snagama. 1.7. Sveukupna procena o tome da li osoba može biti stavljena pod pritiskom neprijateljske strane. **Član 20****Osnovni kriterijumi za bezbednosnu procenu** 1. Osnovni kriterijumi na osnovu kojih se procenjuje postojanje ili nepostojanje neprihvatljivog bezbednosnog rizika za klasifikovane informacije koje služe kao osnova za izdavanje, obustavljanje ili odbijanje pružanja ili daljeg zadržavanja BDO-a, su slučajevi u kojima pojedinac rezultira da:  1.1. je bio, jeste ili pokušava da se tajno angažuje, sam ili u saradnji ili u sastavu ilegalne organizacije u aktivnostima špijunaže, terorizma, izdaje, pobune ili oružanog nasilja protiv ustavnog poretka ili aktivno podstiče nekoga da izvrši dela špijunaže, terorizma, izdaje, pobune ili oružanog nasilja protiv ustavnog poretka; 1.2. jeste ili je bio saučesnik u špijunaži, terorizmu, izdaji, pobuni ili oružanom nasilju protiv ustavnog poretka, postoje sumnje da je bio takav ili saradnik predstavnika organizacija, stranih država, uključujući obaveštajne službe koje mogu ugroziti bezbednost naše zemlje i/ili država članica NATO-a, EU-a, osim ako je takva saradnja odobrena zbog dužnosti; 1.3. jeste ili je bio član organizacije koja nasilnim, neprijateljskim i nezakonitim sredstvima namerava srušiti Vladu ili promeniti ustavni poredak; 1.4. jeste ili je podržavao organizaciju kako je opisano u tački 1.3 ovog člana, ili jeste ili je bilo blisko povezan sa bilo kojim članom takve organizacije; 1.5. namerno je sakrivao, pogrešno predstavio ili je falsifikovao informacije od velikog značaja, određene bezbednosne prirode ili je namerno slagao prilikom popunjavanja bezbednosnog upitnika ili tokom bezbednosnog intervjua; 1.6. rezultira osuđenim za jedno ili više namerno izvršenih krivičnih dela. 1.7. ima istoriju zavisnosti od alkohola, upotrebe ilegalnih droga ili zloupotrebe legitimnih droga; 1.8. ima loše ponašanje, kriminalne tendencije i učešće u organizovanom kriminalu, što dovodi do rizika od slabosti naspram ucene ili može da bude pod ozbiljnim uticajem različitih pritisaka; 1.9. konkretnim radnjama izrazio je nedostatak lojalnosti, pouzdanosti i sigurnosti; 1.10. izvršio je povredu bezbednosti ili je u više navrata prekršio pravila bezbednosti klasifikovanih informacija ili je pokušao i uspeo da izvrši neovlašćene aktivnosti u sistemima komunikacije klasifikovanih informacija; 1.11. pati od hroničnih mentalnih poremećaja.**Član 21** **Bezbednosni intervju**1. AZKI može obaviti intervjue sa licima koja su podnela zahtev za dobijanje BDO-a i prema njima su preduzete procedure za bezbednosnu proveru. 2. AZKI može obaviti intervjue sa trećim nepristrasnim licima, kojima je poznata prošlost i aktivnosti lica koje podleže bezbednosnoj proveri.**Član 22****Validnost BDO-a**1. BDO stepena STROGA TAJNA važi za petogodišnji period;2. BDO stepena TAJNA važi za sedmogodišnji period;3. BDO stepena POVERLJIVO važi za desetogodišnji period.**Član 23****Produženje roka BDO-a u okolnostima vanrednog stanja**1. U okolnostima vanrednog stanja, AZKI ima pravo da produži rok važenja DBO-a samo jednom, do 60 kalendarskih dana tokom ciklusa njegovog važenja pod sledećim uslovima: 1.1 Lice, za koga se traži produženje roka, treba da poseduje važeći DBO, koji je izdat odgovarajućom procedurom. Isključeni su slučajevi produženja roka za jedan DBO koji je izdat u okolnostima vanrednog stanja; 1.2 Postoji zvaničan zahtev koji objašnjava okolnosti vanrednog stanja i dokazuje okolnosti nemogućnosti primene u skladu sa normalnim procedurama za ponovno dobijanje novog BDO-a, kada je: 1.3 lice je u uslovima izvršenja kratkoročnog službenog zadatka, o kojem je bilo nemoguće pratiti procedure, u skladu sa predviđenim vremenskim rokovima;1.4 lice treba da učestvuje u nepredviđenim međunarodnim aktivnostima za koje je bilo nemoguće pratiti procedure prema predviđenim vremenskim rokovima;1.5 lice, koje je dobilo DBO, se nalazi u uslovima produženja roka za učešće u vojnim misijama van zemlje i nemogućnosti primene u skladu sa normalnim procedurama za dobijanje novog DBO-a. Produženje rokova DBO-a pod gore navedenim uslovima je dozvoljeno za DBO-e stepena “Poverljivo”, “Tajna” i “Stroga tajna”.2. Sva lica kojima je DBO produžen u vanrednim okolnostima i uslovima dužna su da se u pisanoj formi izjasne da su shvatila sve svoje obaveze o čuvanju klasifikovanih informacija.**Član 24****Ponavljanje bezbednosne provere**1. Lica kojima je izdat DBO podležu novoj bezbednosnoj proveri u sledećim redovnim intervalima: 1.1. svakih deset (10) godina za lica sa DBO-om bezbednosti koja im omogućuje pristup klasifikovanim informacijama stepena “POVERLJIVO”; 1.2. svakih sedam (7) godina za lica sa DBO-om koja im omogućuje pristup klasifikovanim informacijama stepena “TAJNA” 1.3 svakih pet (5) godina za lica sa DBO-om koje im omogućuje pristup klasifikovanim informacijama stepena “STROGA TAJNA”. 2. Organ za proveru ili rukovodilac javne institucije u kojoj je zaposleno provereno lice može zatražiti od tog lica da se podvrgne novoj proceduri bezbednosne provere čak i pre isteka važenja DBO-a ako postoje indikacije događaja koji su se desili ili okolnosti koje izazivaju sumnju o tome da li proverena osoba i dalje predstavlja prihvatljiv bezbednosni rizik.**Član 25****Privremeno odbijanje, opoziv i obustavljanje DBO-a****1.** AZKI donosi odluku o odbijanju, otkazivanju ili privremenoj obustavi DBO-a u slučajevima kada je dobila informaciju kojom se smatra da izdavanje ili dalje držanje DBO-a od strane određenog lica predstavlja neprihvatljiv bezbednosni rizik, pozivajući se na opšte i osnovne kriterijume bezbednosne procene. 2. Obaveštenje o odluci koju je doneo AZKI o odbijanju, opozivu ili privremenom obustavljanju SBO-a pismeno se dostavlja rukovodiocu odgovarajuće javne institucije koja je podnela zahtev za vođenje postupka bezbednosne provere.**Član 26****Pravo na žalbu**1. Lice kojem je odbijena Bezbednosna dozvola za osoblje ima pravo da podnese žalbu pri AZKI-u u roku od 15 dana od dana prijema obaveštenja; 2. Žalbu razmatra Žalbena komisija;**Član 27****Žalbena komisija**1. Žalbena komisija sastoji se od 5 članova sa po jednim predstavnikom sledećih institucija:* 1. Ministarstvo KSB-a;
	2. Ministarstvo unutrašnjih poslova;
	3. Tužilački savet Kosova;
	4. Sudski savet Kosova;
	5. Obaveštajna agencija Kosova.

2. Predlogom rukovodilaca relevantnih institucija, Vlada svojom odlukom osniva Žalbenu komisiju;3. Lice koje je ovlastila AZKI predstavlja slučaj pred članovima Žalbene komisije;  4. Mandat članova komisije je 3 godine uz mogućnost produženja;5. Članovi žalbene komisije moraju biti profesionalni, sa visokim integritetom i posedovati BDO adekvatnog stepena sa informacijama koje treba pregledati u postupku žalbe;6. Žalbena komisija nakon razmatranja žalbe preporučuje direktoru AZKI-a da donese odluku;7. Pravila i procedure Žalbene komisije i druga pitanja koja se odnose na razmatranje žalbi regulisana su podzakonskim aktom koji predlaže AZKI a odobrava Vlada.**Član 28****Rokovi i trajanje koje pokriva bezbednosnu proveru**1. Ukupni rok za sprovođenje procedura za proveru i izdavanje BDO-a od strane AZKI-a je do 120 kalendarskih dana. 2. Ovaj rok može biti duži kada su provere uslovljene obavljanjem procedura u saradnji sa organima državne bezbednosti drugih zemalja.3. Bezbednosna provera pokriva period koji nije kraći od zadnjih 10 godina. Kada ovaj period nije dovoljan, provera se proteže od 18 godina do trenutnog doba. 4. U slučaju da Organ za proveru ne može prikupiti i obraditi sve potrebne informacije za obavljanje bezbednosne provere u rokovima navedenim u stavu 1. ovog člana, Organ za proveru može svojom odlukom produžiti rok do 60 kalendarskih dana. Rukovodilac relevantne institucije se obaveštava u vezi donete odluke.**Član 29****Obaveza fizičkih lica za zaštitu klasifikovanih informacija**1. Svako lice je dužno da zaštiti klasifikovane informacije prema ovom zakonu, bez obzira na to na koji način im je omogućen ili kako su dobili pristup, ili u bilo kojem drugom obliku je uspeo posedovati klasifikovane informacije. 2. Prilikom napuštanja javne institucija, prekidanja radnog odnosa ili bilo kog drugog ugovornog odnosa, službenom ili ugovornom licu je zabranjeno uklanjanje ili otkrivanje u bilo kom obliku klasifikovanih informacija iz kontrole javne institucije. **Član 30****Međuinstitucionalna saradnja**1. Tokom sprovođenja postupka bezbednosne provere, Organ za proveru sarađuje sa drugim javnim institucijama Republike Kosovo, po potrebi. Druge javne institucije su dužne da pružaju informacije na zahtev.2. Saradnja između AZKI-a i Obaveštajne agencije Kosova, Ministarstva unutrašnjih poslova, Ministarstva kosovskih snaga bezbednosti i drugih institucija javne bezbednosti biće od primarnog značaja. 3. Tokom odvijanja postupka bezbednosne provere, Organ za verifikaciju po potrebi sarađuje sa srodnim institucijama drugih država. **Član 31****Bezbednosna provera zaposlenih u OAK-u**1. Bezbednosnu proveru zaposlenih u OAK-u vrši OAK u skladu sa zakonom OAK-a i primenom kriterijuma i standarda utvrđenih ovim zakonom u pogledu bezbednosne provere osoblja.2. AZKI izdaje zaposlenim u OAK-u BDO na zahtev OAK-a.**Član 32****Bezbednosni dosije**1. Bezbednosna dozvola, popunjeni bezbednosni upitnik i svi ostali relevantni dokumenti i materijali koji se odnose na bezbednosnu proveru, čuvaju se od strane organa za proveru u bezbednosnom dosijeu.2. Pored podataka iz stava 1. ovog člana, bezbednosni dosije sadrži i podatke o naknadnim promenama u vezi sa informacijama predstavljenim u bezbednosnom upitniku. 3. Rukovodilac javne institucije i provereno lice dužni su odmah obavestiti organ za proveru o svim novim dešavanjima, događajima ili okolnostima koji mogu dovesti do promene informacija datih u bezbednosnom upitniku ili koji na neki drugi način mogu negativno uticati na bezbednosnu proveru dotične osobe.4. Organ za proveru klasifikuje i održava bezbednosni dosije na način koji daje bezbednosnom dosijeu stepen klasifikacije i zaštite koji smatra neophodnim radi zaštite interesa bezbednosti Kosova. **Član 33****Obrada podataka**1. Organ za proveru može obraditi lične podatke proverene osobe koji se nalaze u bezbednosnom dosijeu samo u cilju obavljanja svojih funkcija i odgovornosti utvrđenih ovim zakonom. 2. Organ za proveru ne prenosi drugim javnim institucijama lične podatke koji se nalaze u bezbednosnom dosijeu, osim ako ne postoji prioritetni javni interes bez ugrožavanja bezbednosnih interesa Republike Kosovo i samo za potrebe: 2.1. aktivnosti vezanih za sprovođenje zakona; 2.2. aktivnosti vezanih za otkrivanje; 2.3. parlamentarnih istraga. 3. Javna institucija koja prima takve podatke može ih koristiti i obraditi samo ako je to apsolutno neophodno i za ciljeve navedene u stavu 2. ovog člana i treba obezbediti zaštitu od neovlašćenog objavljivanja koje se zahteva za odgovarajući stepen klasifikacije. 4. Agencije za sprovođenje zakona mogu koristiti i obrađivati podatke iz stava 2. ovog člana u cilju krivičnog gonjenja samo kao poslednju sredstvo kada se takvi podaci ne mogu prikupiti u drugim oblicima ili ako bi se ozbiljno sprečilo krivično gonjenje u odsustvu pristupa takvim podacima.**POGLAVLJE IV****INDUSTRIJSKA BEZBEDNOST****Član 34****Zaštita klasifikovanih informacija u industrijskoj oblasti**1. Zaštita klasifikovanih informacija u industrijskoj oblasti vrši se utvrđivanjem preventivnih mera i postupaka od neovlašćenog širenja, gubitka ili kršenja bezbednosti klasifikovanih informacija, koja se obrađuju pod uslovima realizacije klasifikovanog projekta/programa/ ugovora/podugovora.2. Utvrđivanje standarda kada fizičko ili pravno lice ima mogućnost pristupa klasifikovanoj informaciji i poseduje sposobnosti potrebne za upravljanje ovim informacijama pre podnošenja ponude, da pregovara ili učestvuje u klasifikovanom ugovoru ili da radi za klasifikovani projekat, koji uključuje pristup klasifikovanim informacijama, vrši se u skladu sa zahtevima važećeg zakonodavstva.**Član 35****Uslovi za zaključivanje klasifikovanog ugovora**1. Ekonomski operateri koji su zainteresovani za učešće u klasifikovanoj nabavci na stepenu “STROGA TAJNA”, “TAJNA” i “POVERLJIVO”, prethodno treba da dobiju potreban stepen SIB-a. Osoblje koje zastupa ekonomskog operatera u klasifikovanoj nabavci i druge pojedince, koji će imati pristup klasifikacionim informacijama, treba da budu propisno sertifikovani u skladu sa zahtevima važećeg zakonodavstva.2. Ekonomski operateri koji su zainteresovani za učešće u klasifikovanoj nabavci na nivou „OGRANIČENO”, neće morati da dobiju SIB. 3. Osoblje koje zastupa Ekonomskog operatera u ovoj nabavci i sva lica koja će imati pristup klasifikovanim informacijama, brifiraju se i potpisuju izjavu o čuvanju klasifikovanih informacija pre pokretanja procedura klasifikovane nabavke.**Član 36****Dobijanje sertifikata industrijske bezbednosti** 1. SIB se izdaje od strane AZKI-a, u skladu sa zahtevima važećeg zakonodavstva.2. Za ekonomske operatere drugih zemalja, SIB se izdaje od strane organa nacionalne bezbednosti, ili od strane nadležnog organa bezbednosti zemlje, u kojoj je registrovan ekonomski operater. Ovaj sertifikat se smatra važećim u cilju učešća u klasifikovanoj nabavci, tek nakon pismene potvrde od strane AZKI-a, upućenoj ugovornom organu. AZKI, pre potvrđivanja SIB-a, sarađuje sa srodnim organima za izvršenje odgovarajućih provera. 3. Tek nakon primanja potvrde AZKI-a, ugovorni organ daje ekonomskom operateru pravo na pristup klasifikovanim informacijama.4. Ekonomski operater koji pruža usluge u oblasti bezbednosti može pokrenuti procedure za dobijanje SIB-a pre zaključivanja klasifikovanog ugovora sa javnim institucijama, podnoseći zahtev AZKI-u uz odgovarajuća obrazloženja za potrebu SIB-a.5. Procedure za zaštitu klasifikovanih informacija u industrijskoj oblasti utvrđuju se podzakonskim aktom koji predlaže AZKI i odobrava Vlada.**Član 37****Osnovni kriterijumi za procenu industrijske bezbednosti**1. Postupci provere za izdavanje SIB-a sprovode se u skladu sa zahtevima važećeg zakonodavstva i obuhvataju aspekte koji se odnose na: 1.1 Vlasničku strukturu Ekonomskog operatera, njegovu finansijsku stabilnost, trgovinsku reputaciju, sposobnost i tehničke kapacitete, kao i bezbednosne aspekte. 1.2 Vlasnici/akcionari i menadžersko osoblje koji će zbog svojih funkcija imati pristup klasifikovanim informacijama; 1.3 Predloženo lice za poziciju SB-a, njegovog zamenika i zaposlenih, koji će imati pristup klasifikovanim informacijama.2. AZKI ima pravo da zatraži informacije od državnih institucija ako to smatra neophodnim za proveru mogućeg bezbednosnog rizika Ekonomskog operatera i kategorija lica uključenih u klasifikovanim nabavkama ili u sprovođenju klasifikovanog ugovora.**Član 38****Uslovi za zaključivanje klasifikovanih podugovora**  1. Izvođač radova, u bilo kom slučaju, pre početka pregovora za zaključivanje klasifikovanog podugovora, mora prvo da dobije pismenu saglasnost od Ugovornog organa. 2. Nije dozvoljeno da Ugovorni organ ovlasti Izvođača radova sa kojim je zaključio klasifikovani ugovor na stepenu “STROGA TAJNA”, kako bi stupio u ugovorne odnose u uslovima klasifikovanog podugovora.3. Svi kriterijumi za zaključivanje/sprovođenje klasifikovanog ugovora primenjuju se na odgovarajući način i sa podizvođačem radova.**Član 39****Prevoz i međunarodne posete** 1. Prevoz klasifikovanog materijala tokom sprovođenja klasifikovanog ugovora vrši se kopnenim, morskim, železničkim i vazdušnim putem, pridržavajući se bezbednosnim pravilima u skladu sa zahtevima važećeg zakonodavstva.2. Bezbednosni standardi klasifikovanih informacija u oblasti industrijske bezbednosti primenjuju se i tokom međunarodnih poseta.**POGLAVLJE I****BEZBEDNOST KOMUNIKACIONIH I INFORMACIONIH SISTEMA** **Član 40****Razumevanje bezbednosti komunikacionih i informacionih sistema** 1. Bezbednost klasifikovanog komunikacionog i informacionog sistema predstavlja skup standarda za zaštitu klasifikovanih informacija, izvora i sistemskih usluga u komunikacionim sredstvima koja obrađuju, čuvaju ili prenose klasifikovane informacije.2. AZKI je nacionalni autoritet za akreditaciju bezbednosti sistema elektronske komunikacije koji obrađuje, čuva ili prenosi klasifikovane informacije.**Član 41****Garantovanje bezbednosti informacija**1. Garantovanje bezbednosti informacija predstavlja praksu garantovanja bezbednosti informacija i upravljanja rizikom koji se odnosi na upotrebu, obradu i prenos informacija ili podataka u sistemima ili drugim obradama koje se koriste u tu svrhu.2. Garantovanje bezbednosti informacija predstavlja održavanje komunikacionih i informacionih sistema u ravnoteži sa principima poverljivosti, integriteta, dostupnosti, autentifikacije i neporicanja.**Član 42****Komunikacioni i informacioni sistemi** 1.Mehanizmi i procedure upravljanja bezbednošću su uspostavljeni u cilju ometanja, sprečavanja, otkrivanja, odupiranja i oporavljanja od napada incidenata koji pogađaju bezbednosne ciljeve klasifikovanih informacija, uključujući izveštavanje bezbednosnih incidenata. Ove mere uključuju:1.1 Obezbeđivanje dovoljnih informacija kako bi se omogućila istraga o namernoj ili slučajnoj kompromitaciji bezbednosnih ciljeva u skladu sa štetom koja može biti prouzrokovana;1.2 Pouzdanu identifikaciji i autentifikaciju lica, uređaja i usluga ovlašćenih za pristup. Informacija koja kontroliše pristup u komunikacionim i informacionim sistemima je kontrolisana i zaštićena u skladu sa stepenom poverljivosti informacije za koju odobrava pristup.1.3 Kontrolisanje pristupa klasifikovanim informacijama u skladu sa principom “nužnost pristupa informacijama”1.4 Upravljanje integritetom, poreklom i dostupnošću klasifikovanih informacija; 1.5 Kontrolu povezivanja komunikacionih i informacionih sistema koji tretiraju klasifikovane informacije;1.6 Utvrđivanje stepena pouzdanosti zaštitnih mehanizama bezbednosti komunikacionih i informacionih sistema;1.7 Procenu i proveru tačnog funkcionisanja zaštitnih mehanizama bezbednosti komunikacionih i informacionih sistema tokom njihovog celokupnog životnog veka;1.8 Istraživanje aktivnosti korisnika i komunikacionih i informacionih sistema;1.9 Garantovanje neporicanja kako bi pošiljalac informacija dobio potvrdu o preuzimanju poruke od strane primaoca i da primalac dobije potvrdu o identitetu pošiljaoca;**POGLAVLJE II – FIZIČKA BEZBEDNOST** **Član 43****Fizička bezbednost** 1. Fizička bezbednost predstavlja skup fizičkih, tehničkih, elektronskih i proceduralnih mera za očuvanje područja, zgrada, kancelarija, soba, prostorija i uređaja u kojima se proizvodi, snima, koristi, prenosi, čuva, arhivira ili uništava klasifikovana informacija.2. Državne institucije su obavezne da preduzimaju mere za fizičku bezbednost područja, zgrada, kancelarija, soba, prostorija i uređaja u kojima se proizvodi, snima, koristi, prenosi, čuva, arhivira ili uništava klasifikovana informacija, u skladu sa standardima i procedurama utvrđenim podzakonskim aktima, koji su u skladu sa relevantnim standardima koji su utvrđeni od strane Organizacije severnoatlantskog ugovora i Evropske unije.3. Rukovodilac institucije nalogom odobrava podelu bezbednosnih zona koji je propraćen planom i šemom fizičke bezbednosti objekta u kom se čuvaju i upravljaju klasifikovane informacije.4. U državnim institucijama u kojima se radi sa klasifikovanim informacijama, u zavisnosti od obima klasifikovanih informacija, uspostavlja se bezbednosna struktura/službenik za bezbednost.5. AZKI, u saradnji sa državnim institucijama, periodično vrši elektronsku dezinfekciju zgrada, kancelarija, soba, prostorija u kojima se proizvodi, snima, koristi, prenosi, čuva, arhivira ili uništava klasifikovana informacija.6. Pravila fizičkog prevoza klasifikovanih informacija utvrđuju se podzakonskim aktom.**Član 44****Jedinica za klasifikovane informacije** 1. Svaka javna institucija koja proizvodi i upravlja klasifikovanim informacijama mora da u okviru strukture svoje organizacije odredi odgovarajućeg službenika ili jedinicu, kao i da obezbedi odgovarajuće kancelarije ili prostorije koje služe za održavanje i upravljanje klasifikovanim informacijama.2. Javne institucije vode Registre za klasifikovane informacije prema modelu koji je utvrdila Agencija.3. Model za obeležavanje klasifikovanih informacija je jedinstven i isti utvrđuje AZKI, a sve javne institucije su obavezne da ga primenjuju. 4. Proces uspostavljanja, održavanja i upravljanja odgovarajućom jedinicom ili službenikom, odgovarajućim kancelarijama ili prostorijama, uključujući i vođenje Registara za klasifikovane informacije, utvrđuje se podzakonskim aktom koji usvaja Vlada na predlog Agencije. **Član 45****Registri**Svaki rukovodilac javne institucije, koja proizvodi i upravlja klasifikovanim informacijama, mora da stvori minimalne bezbednosne standarde za zaštitu klasifikovanih informacija, kao i da odredi odgovorna lica za upravljanje ovim informacijama.**Član 46****Strane informacije**1. Državne institucije čuvaju klasifikovane informacije stranih država ili međunarodnih organizacija prema standardima koji obezbeđuju stepen zaštite koji je isti sa stepenom zaštite koji zahteva država ili međunarodna organizacija.2. Svaka institucija, pre potpisivanja sporazuma ili tehničkog protokola koji obuhvata razmenu klasifikovanih informacija, mora najpre da dobije mišljenje AZKI-a. 1. Potpisivanju sporazuma ili tehničkog protokola, koji obuhvata razmenu klasifikovanih informacija, mora da prethodi potpisivanje opšteg sporazuma za bezbednost klasifikovanih informacija između organa nacionalne bezbednosti država ugovornica.

**Član 47****Klasifikovane informacije NATO-a i EU-a** 1. Sistem Registra klasifikovanih informacija NATO-a i EU-a sastoji se od Kancelarije centralnog registra u AZKI-u, Kancelarija podregistra klasifikovanih informacija NATO-a i EU-a i kontrolnih tačaka koje se uspostavljaju u ministarstvima i državnim institucijama. 2. Klasifikovane informacije NATO-a i EU-a se razmenjuju i upravljaju samo preko ovog Sistema. 3. Sistem Registra klasifikovanih informacija NATO-a i EU-a je odgovoran za registraciju, širenje i upravljanje klasifikovanim informacijama razmenjenih u okviru saradnje NATO-a i EU-a.4. Državne institucije su obavezne da štite klasifikovane informacije NATO-a i EU-a u skladu sa standardima koji obezbeđuju isti stepen zaštite sa onim koji se zahteva od strane NATO-a i EU-a.5. Kancelarija centralnog registra klasifikovanih informacija NATO-a i EU-a u AZKI-u je odgovorna struktura za vođenje razmene, nadzora i kontrolu nad aspektima bezbednosti klasifikovanih informacija NATO-a i EU-a unutar sistema Registra.**Član 48****Neklasifikovane informacije NATO-a, EU-a, država i drugih međunarodnih organizacija**Neklasifikovane informacije NATO-a, EU-a, država i drugih međunarodnih organizacija predstavljaju informacije koje nisu kategorizovane ni u jednom stepenu klasifikovanih informacija, ali se koriste isključivo iz službenih razloga od strane državnih institucija i nisu otvorene za javnost.**Član 49****Inspekcija javnih institucija i ekonomskih operatera** 1. AZKI vrši inspekcije u vezi sa sprovođenjem mera bezbednosti za zaštitu klasifikovanih informacija kod javnih institucija i ekonomskih operatera koji upravljaju klasifikovanim informacijama.2. Inspekcija se vrši redovno i uz prethodno obaveštavanje javnih institucija.3. Predmet inspekcija bez prethodnog obaveštavanja su samo one institucije ili ekonomski operateri za koje postoje pouzdane informacija da ima kršenja bezbednosti u smislu upravljanja klasifikovanim informacijama. 4. Predmet inspekcija su sledeće discipline:1. Bezbednost osoblja
2. Industrijska bezbednost
3. Bezbednost komunikacionih i informacionih sistema
4. Fizička bezbednost
5. Upravljanje klasifikovanim informacijama

5. Po završetku inspekcije mera bezbednosti, AZKI izrađuje detaljan izveštaj o nalazima i predlaže preduzimanje odgovarajućih mera za povećanje stepena bezbednosti klasifikovanih informacija.6. Izveštaj se upućuje rukovodiocu odgovarajuće javne institucije. 7. U koordinaciji sa rukovodiocem javne institucije izrađuje se plan za sprovođenje preporuka koje proizilaze iz izveštaja o inspekciji.8. AZKI nadgleda sprovođenje preporuka kod javnih institucija i ako se iste ne sprovode u okviru unapred predviđenih rokova, pismenim putem obaveštava direktnog nadzornika rukovodioca odgovarajuće institucije koja je bila predmet inspekcije.**POGLAVLJE VI** **AGENCIJA ZA ZAŠTITU KLASIFIKOVANIH INFORMACIJA (AZKI)****Član 50****Osnivanje Agencije** 1. Agencija za zaštitu klasifikovanih informacija (AZKI) se osniva kao agencija za nacionalnu bezbednost u oblasti zaštite klasifikovanih informacija za sve javne institucije Republike Kosovo i njihovih izvođača radova koji u bilo kom obliku mogu upravljati klasifikovanim informacijama.  2. Agencija za zaštitu klasifikovanih informacija, kao i svi zaposleni i osoblje angažovano za rad u agenciji, moraju da budu politički nepristrasni, profesionalni, bez predrasuda u svojoj proceni i da deluju isključivo u skladu sa zakonom i da ne primaju uputstva od bilo koje osobe ili institucije.3. AZKI je centralni organ sa sedištem u Prištini.**Član 51** **Odgovornosti AZKI-a u oblasti zaštite klasifikovanih informacija** 1. AZKI je nezavisna centralna institucija u oblasti zaštite klasifikovanih informacija sa mandatom za organizovanje, vođenje i kontrolisanje mera za čuvanje, klasifikaciju i upravljanje klasifikovanim informacijama i bezbednosnu proveru za sve institucije RKS-a kao i njihovih izvođača radova, i odgovorna je za:* 1. izradu politika
	2. praćenje procedura
	3. nadgledanje institucija i izvođača radova u klasifikovanim ugovorima
	4. bezbednosnu edukaciju,
	5. bezbednost osoblja
	6. fizičku bezbednost
	7. bezbednost informacija
	8. industrijsku bezbednost
	9. bezbednost komunikacionih i informacionih sistema

1.10 vođenje pregovora za zaključivanje bezbednosnih sporazuma sa odgovarajućim državama 1.11 nadgledanje sprovođenja međunarodnih ugovora ili instrumenata o zaštiti klasifikovanih informacija i predlaže preduzimanje mera u vezi s tim;2. AZKI je nadležni bezbednosni organ za Republiku Kosovo u vezi sa zaštitom klasifikovanih informacija stranih država i međunarodnih organizacija3. AZKI sarađuje sa javnim institucijama, zainteresovanim ekonomskim operaterima i srodnim organima država i međunarodnih organizacija za obavljanje zadataka predviđenih važećim zakonodavstvom.4. Strateški plan rada AZKI-a sadrži opšte i specifične ciljeve za postizanje bezbednosnih standarda za zaštitu klasifikovanih informacija, koji nakon razmatranja od strane SBK-a, predlaže se vladi na usvajanje. 5. Unutrašnja organizacija i funkcionisanje AZKI-a je regulisana podzakonskim aktom koji predlaže AZKI a odobrava Vlada.**Član 52****Agencija za zaštitu klasifikovanih informacija** **1.** AZKI deluje na osnovu ovog zakona u skladu sa Ustavom i svim drugim važećim zakonima na Kosovu.2. AZKI je pravno lice.3. AZKI je organ nacionalne bezbednosti **Član 53****Pripremanje i obezbeđivanje budžeta** 1. Direktor AZKI-a priprema i podnosi premijeru nacrt godišnjeg budžeta za AZKI2. AZKI je autonomna budžetska organizacija sa sopstvenim budžetskim kodom.3. Skupština Kosova stavlja na raspolaganje AZKI-u zadovoljavajući godišnji budžet za obavljanje zadataka i odgovornosti za zaštitu klasifikovanih informacija u skladu sa važećim zakonodavstvom.**Član 54****Imenovanje direktora Agencije** **1.** Premijer, nakon konsultacija sa predsednikom, imenuje direktora Agencije u roku od dvadeset (20) radnih dana od dana kada je radno mesto ostaje upražnjeno.2. Postupak za razrešenje direktora Agencije je isti kao i postupak za njegovo imenovanje.3. Direktor Agencije se imenuje na mandat od pet (5) godina, koji se može produžiti.4. Direktor Agencije, u skladu sa ovim Zakonom, Uredbom o unutrašnjoj organizaciji i drugim važećim zakonima, odgovoran je za sve aspekte upravljanja Agencijom. 5. U izvršavanju njegovih odgovornosti, direktoru Agencije pomažu zamenik direktora, rukovodioci organizacionih jedinica i osoblje sa odgovarajućom kvalifikacijom po potrebi, u skladu sa pravilima i procedurama utvrđenim ovim Zakonom i Uredbom o unutrašnjoj organizaciji.**Član 55****Zamenik direktora Agencije**1. Zamenik direktora Agencije pomaže direktoru Agencije i upravlja aktivnostima organizacionih jedinica Agencije pod nadzorom direktora Agencije.2. Zamenik direktora Agencije mora imati univerzitetsko obrazovanje i imenuje se na osnovu dokazanog profesionalizma i iskustva i ne uzimajući u obzir političku pripadnost, za mandat od pet (5) godina, koji se može obnoviti i teći će nezavisno od mandata direktora Agencije.3. Direktor AZKI-a predlaže premijeru za imenovanje tri (3) kandidata za zamenika direktora Agencije.4. Premijer Republike Kosovo, imenuje zamenika direktora Agencije u roku od dvadeset (20) radnih dana od dana kada je radno mesto ostaje upražnjeno.5. Zamenik direktora Agencije se razrešava dužnosti istim postupkom kojim je imenovan.6. Zamenik direktora Agencije privremeno obavlja i vrši odgovornosti direktora Agencije za vreme odsustva ili nemogućnosti direktora. U slučaju trajne nemogućnosti, zamenik direktora Agencije obavlja i vrši odgovornosti direktora Agencije, sve dok se zamena za direktora formalno ne imenuje.Član 56**Kriterijumi za imenovanje generalnog direktora**1. Kriterijumi za imenovanje generalnog direktora AZKI-a su:
	1. da bude samo državljanin Republike Kosovo;
	2. da ima univerzitetsku diplomu;
	3. da ima najmanje 8 godina profesionalnog iskustva u bezbednosnim institucijama, od kojih najmanje (5) godina radnog iskustva na rukovodećoj poziciji;
	4. da nije bio osuđen pravosnažnom odlukom za krivično delo;
	5. da, u poslednjih pet (5) godina tokom kojih je radio u javnim institucijama, nije bio kažnjen zbog teških disciplinskih prekršaja;
	6. da nema sukoba interesa sa dužnošću ili kao što je predviđeno Zakonom o sprečavanju sukoba interesa u vršenju javnih funkcija;

**Član 57****Direktor Agencije**1. Direktor Agencije će direktno odgovarati premijeru.2. Direktor Agencije:* 1. savetuje premijera Republike Kosovo o pitanjima zaštite klasifikovanih informacija;
	2. izveštava i obaveštava premijera Republike Kosovo o aktivnostima Agencije;
	3. daje podatke premijeru Republike Kosovo što se tiče klasifikacije informacija i bezbednosne provere;
	4. štiti i pomaže u zaštiti klasifikovanih informacija od neovlašćenog objavljivanja;
	5. uspostavlja i koordinira odnose sa stranim srodnim agencijama;
	6. obezbeđuje da Agencija ne preduzima nikakvu radnju koja može dovesti do opravdane sumnje da je Agencija posvećena unapređenju, zaštiti ili oštećenju interesa bilo koje zajednice ili bilo koje političke partije ili organizacije;
	7. obezbeđuje da Agencija ne preduzima nikakvu radnju kako bi uticala na političke procese, javno mišljenje i medije na Kosovu;
	8. priprema godišnji izveštaj o radu i predlaže preduzimanje neophodnih mera za povećanje nivoa bezbednosti klasifikovanih informacija;
	9. inicira i potpisuje Memorandume o razumevanju i saradnji sa drugim institucijama i organima;
	10. najmanje jednom godišnje izveštava nadležnoj parlamentarnoj komisiji;

**Član 58****Specifični uslovi za zaposlene u Agenciji**1. Lica izabrana za rad u Agenciji treba da ispunjavaju stroge bezbednosne standarde, koji su utvrđeni u skladu sa važećim zakonom i u skladu sa procedurama navedenim u uredbama koje je doneo direktor Agencije i usvojila Vlada. Kandidat mora da bude procenjen kao stabilan, pouzdan i sa karakterom, odličnom procenom i diskrecijom. Bilo kakva sumnja u vezi sa bilo kojim od gore pomenutih faktora se rešava u korist bezbednosti Kosova. 2. Kandidati se ne zapošljavaju u Agenciji, ukoliko ne prođu bezbednosni uslov.3. Pored opštih zahteva za zapošljavanje koji se sprovode za druge zaposlene u vladi, mogu se primeniti posebni uslovi za zaposlene u Agenciji u vezi sa uslovima stručnosti, zdravlja, radnih zadataka i bezbednosnih uslova koji su u skladu sa interesima bezbednosti Kosova.4. Uredba o unutrašnjoj organizaciji Agencije, utvrđuje uslove za svaku poziciju u Agenciji, kao i da će podneti specifične uslove za zapošljavanje u Agenciji.5. U skladu sa internim pravilima i, kada je to neophodno, Agencija može angažovati treća lica za pomoćne usluge.**Član 59****Kvalifikacije za zapošljavanje u Agenciji**1. Agencija ne može zaposliti kandidate, ukoliko ne ispunjavaju sledeće uslove:* 1. da su državljani Kosova;
	2. da imaju odgovarajuće obrazovne i profesionalne kvalifikacije, kao što je to utvrđeno Uredbom o unutrašnjoj organizaciji;
	3. da izvrše lekarski pregled koji je zahtevan za tu poziciju;
	4. da budu oslobođeni od vojne službe, ako je primenjivo; i
	5. da budu u mogućnosti da ispune bezbednosne uslove koje će biti određene ovim Zakonom i podzakonskim aktima.

2. Pravila i procedure za opšte uslove i procedure zapošljavanja, radne odnose, obuku, napredovanje u karijeri i imenovanje pozicija su utvrđena Uredbom o radnom odnosu u AZKI-u koju je usvojila Vlada.**Član 60****Status zaposlenih AZKI-a**Zaposleni AZKI-a prema ovom zakonu imaju poseban status. Za pitanja koja nisu uređena ovim zakonom ili podzakonskim aktima koji proizilaze iz ovog zakona, odgovarajuće će se primenjivati zakonodavstvo koje uređuje pitanja civilne službe.**Član 61****Prava zaposlenih u Agenciji**1. Zaposleni u Agenciji imaju pravo:* 1. na trajno zaposlenje do ispunjenja uslova za penziju, izuzev lica koja su zaposlena na osnovu ugovora o pružanju usluga za određeni period, kao i onih koji su sa razlogom razrešeni dužnosti, na osnovu važećeg zakonodavstva;
	2. da uzmu odmor u skladu sa važećim zakonodavstvom i mogućnost da nastave sa istim ili sličnim radom, kada se odmor završi;
	3. na nadoknadu za dužnosti i obavljanje dužnosti, kao što je utvrđeno ovim zakonom;
	4. da primaju plate i naknade u skladu sa važećim zakonodavstvom;
	5. na napredovanje karijere i profesionalnog razvoja putem obuka i drugih sredstava;

**Član 62****Zabranjeno ponašanje zaposlenih**1. Zaposleni u Agenciji ne smeju da budu članovi političkih subjekata ili da dobijaju uputstva od njih ili pojedinaca van Agencije, kao i ne smeju da javno izražavaju svoja politička uverenja i preferencije.2. Zaposleni ne mogu vršiti bilo koje druge javne ili stručne plaćene aktivnosti ili dužnosti, koji nisu u skladu sa radom Agencije ili stvaraju sukob interesa.3. Zaposleni u Agenciji ne mogu da imaju drugo zaposlenje dok su zaposleni u Agenciji.4. Zaposleni u Agenciji nemaju pravo na delatnosti koje imaju za cilj prestanak aktivnosti ili bilo kog drugog oblika kolektivne obustave rada.5. Zaposleni u Agenciji, bez prethodne saglasnosti direktora Agencije, ne mogu davati izjave za javnost ili da na drugi način daju komentare o radu Agencije ili daju informacije neovlašćenim licima, o podacima, dokumentima, kontaktima, ciljevima, saznanjima ili osoblju Agencije. 6. Ukoliko se kandiduje na izborima za Skupštinu Kosova ili za organe lokalne samouprave, obavezuju se da zahtevaju oslobađanje od dužnosti i ne mogu da ponovo budu primljeni u Agenciji.**Član 63****Lične zakonske obaveze zaposlenog**1. Svaki zaposleni u Agenciji obavlja funkcije koje su mu dodeljene u skladu sa ovim Zakonom i drugim odgovarajućim zakonima i lično je odgovoran za zakonito sprovođenje zadataka Agencije, kao što je definisano ovim Zakonom i koji su u okviru zadataka dodeljenih određenom zaposlenom.2. Ukoliko zaposleni veruje da je on ili ona dobio nezakonitu naredbu, on ili ona treba da obavesti naredbodavca u vezi sa svojim zabrinutostima.3. U slučajevima kada naredbodavac ponovi naredbu, radnik će zatražiti pismenu potvrdu o takvoj naredbi. Ukoliko zaposleni i dalje ima sumnje, on ili ona će proslediti naredbu direktnom nadređenom naredbodavca i po tom pitanju će izvestiti direktora.4. Obezbeđivanje zaštite i neovlašćenog otkrivanja klasifikovanih informacija, o kojima je dobio saznanje tokom ili van vršenja dužnosti, obaveza je koja nastavlja čak i nakon što prestane radni odnos sa Agencijom; 5. Da ne upotrebljava informacije prikupljene tokom vršenja dužnosti u druge svrhe osim onih utvrđenih Zakonom; 6. Da obezbedi zaštitu i otkrivanje ličnih podataka i onih koji se odnose na profesionalne delatnosti lica, zaštićenih u skladu sa zakonom, sa kojima se upoznaje tokom vršenja dužnosti. **Član 64****Plate i naknade za zaposlene u Agenciji**1. Dodatna plaćanja i naknade za osoblje Agencije je utvrđeno podzakonskim aktom koji predlaže direktor a odobrava Vlada;2. Pored osnovne plate, zaposleni AZKI-a mogu zakonski primiti i druge vrste dodataka na plate, dnevnice i beneficije, na osnovu faktora koji uključuju poteškoće u radu, prekovremeni rad ili specijalne sposobnosti;3. U slučaju smrti na dužnosti ili zbog obavljanja njegovih dužnosti u okviru AZKI-a, Vlada će porodici ili pravnom(im) nasledniku(cima) pokojnika plaćati mesečnu platu zaposlenog AZKI -a u periodu od jedne (3) godine od smrti zaposlenog;**Član 65****Prekid zaposlenja**1. Zaposlenje zaposlenih u Agenciji se prekida u ovim slučajevima:* 1. dobrovoljno podnošenje ostavke Agenciji;
	2. završetak ugovora;
	3. dostizanje starosti za penzionisanje;
	4. trajna nemogućnost za obavljanje službene dužnosti zbog zdravstvenog stanja, pod uslovom da zaposleni nema pravo da bude prebačen na drugu odgovarajuću poziciju u Agenciji;
	5. gubitak državljanstva Kosova;
	6. pravosnažna osuda za krivično delo.
	7. isključenje iz agencije kao rezultat disciplinskog postupka.

**Član 66****Identifikacione kartice** Zaposlenima u Agenciji se izdaju identifikacione kartice. Vrsta, oblik i sadržaj identifikacione kartice zaposlenog u Agenciji se utvrđuje Odlukom izdatom od strane direktora AZKI-a.**Član 67****Uredba i unutrašnja organizacija**Unutrašnju organizaciju Agencije se utvrđuje Uredbom o unutrašnjoj organizaciji koja se usvaja u Vladi.**Član 68****Sprovođenje standarda EU-a i NATO-a**1. AZKI je Organ bezbednosti Republike Kosovo koji se stara o postizanju bezbednosnih standarda za zaštitu klasifikovanih informacija u skladu sa zahtevima koji proizilaze iz bezbednosnih direktiva NATO-a i EU-a.2. Agencija razmenjuje klasifikovane informacije sa svim državama članicama NATO-a i EU-a, kao i drugim državama.3. U skladu sa direktivama NATO-a i EU-a, Agencija priznaje bezbednosne dozvole za osoblje i sertifikate industrijske bezbednosti država sa kojima je potpisala bezbednosne sporazume.**POGLAVLJE III****POVREDA BEZBEDNOSTI I KOMPROMITOVANJE KLASIFIKOVANIH INFORMACIJA****Član 69**1. Povreda bezbednosti nastupa kao posledica dela ili propusta od strane pojedinca koji postupa u suprotnosti sa pravilima bezbednosti predviđenim ovim zakonom i drugim podzakonskim aktima.2. Kompromitovanje klasifikovanih informacija se javlja kada je, kao rezultat povrede bezbednosti, došlo do potpunog ili delimičnog otkrivanja informacija neovlašćenom licu.3. Svako kršenje ili sumnja na kršenje bezbednosti se odmah izveštava nadležnom organu bezbednosti AZKI-a.4. Kada je poznato ili kada postoji dovoljan razlog da se tvrdi da je klasifikovana informacija kompromitovana ili izgubljena, organ bezbednosti preduzima mere u skladu sa zakonom i podzakonskim aktima: * 1. obaveštavajući organ porekla
	2. obezbeđujući da se slučaj istražuje od strane neutralne osobe u vezi sa ovim pitanjem
	3. utvrđujući potencijalnu štetu prouzrokovanu interesima Republike Kosovo ili drugih država i organizacija
	4. Preduzima odgovarajuće mere za sprečavanje ponavljanja
	5. Obaveštava organe o preduzetim radnjama

5. Svaki pojedinac odgovoran za povredu pravila bezbednosti utvrđenih ovim zakonom i podzakonskim aktima podleže disciplinskim kaznama u skladu sa važećim zakonodavstvom.6. Svaki pojedinac odgovoran za kompromitovanje ili gubitak klasifikovanih informacija podleže disciplinskim kaznama ili pravnim postupcima u skladu sa važećim zakonima i primenjenim podzakonskim aktima.**POGLAVLJE VII** **ZAŠTITA DOSIJEA I PODATAKA****Član 70****Gubitak klasifikovanih informacija**1. Za bilo koji gubitak, sumnju na gubitak, povredu ili sumnju na povredu bezbednosti klasifikovane informacije, kao i bilo koji neovlašćeni trenutni ili sumnjivi pristup klasifikovanim informacijama, svi ovlašćeni nosioci klasifikovanih informacija odmah izveštavaju njihovoj javnoj instituciji, državnom tužilaštvu i Agenciji. 2. Agencija, na svoju inicijativu ili na zahtev odgovarajućeg organa u slučajevima navodnih kršenja u ovom zakonu, odmah preduzima sve potrebne mere da:* 1. istraži slučaj,
	2. identifikuje uzrok gubitka,

 2.3 prati bilo koje otvaranje od strane neovlašćenih lica za pristup takvim informacijama, 2.4 ukloni štetne efekte i da spreči dalje gubitke klasifikovanih informacija,3. U slučaju da se sumnja da navodno kršenje predstavlja krivično delo, obaveštava državnog tužioca. **POGLAVLJE VIII****Član 71****Krivične Sankcije**1. Lice koje bez ovlašćenja objavi informaciju koja je prema ovom zakonu klasifikovana kao ”POVERLJIVA” i bilo koji ovlašćeni nosilac takve klasifikovane informacije koji ne štiti klasifikovane informacije kao što se traži ovim zakonom, vrši krivično delo i kažnjava se kaznom zatvora od godinu dana do pet (5) godina.2. Lice koje bez ovlašćenja objavi informaciju koja je prema ovom zakonu klasifikovana kao ”TAJNA” i bilo koji ovlašćeni nosilac takve klasifikovane informacije koji ne štiti klasifikovane informacije kao što se traži ovim zakonom, vrši krivično delo i kažnjava se kaznom zatvora od tri do deset godina. 3. Lice koje bez ovlašćenja objavi informaciju koja je prema ovom zakonu klasifikovana kao ”STROGA TAJNA” i bilo koji ovlašćeni nosilac takve klasifikovane informacije koji ne štiti klasifikovane informacije kao što se traži ovim zakonom, vrši krivično delo i kažnjava se kaznom zatvora od pet (5) do dvanaest (12) godina.**ČLAN 72****PRELAZNE I ZAVRŠNE ODREDBE** 1. Nakon imenovanja, direktor AZKI-a u saradnji sa direktorom OAK-a, započinje postupak prenošenje odeljenja za proveru sa odgovarajućim dosijeima u AZKI.2. Sadašnji zaposleni u bivšem Odeljenju za bezbednosnu proveru u okviru OAK-a imaju pravo da putem dobrovoljne izjave izaberu nastavak rada u AZKI-u ili da ostanu u okviru struktura OAK-a 3. Zaposleni bivšeg Odeljenja za bezbednosnu proveru u okviru OAK-a koji će nastaviti da rade u AZKI-u, imaju pravo na staž stečen u OAK-u. 4. Direktor AZKI-a i direktor OAK-a po dogovoru mogu koristiti sredstva OAK-a do kompletiranja osoblja AZKI-a. 5. Vlada će osigurati odgovarajući objekat sa bezbednosnim standardima u funkciji postizanja mandata AZKI-a za zaštitu klasifikovanih informacija Republike Kosovo. 6. U svakoj odredbi zakona, podzakonskih akata, izraz OAK korišćen u smislu organa za proveru, stupanjem na snagu ovog zakona zamenjuje se izrazom AZKI. **Član 73****Podzakonski akti** Vlada usvaja podzakonske akte za sprovođenje ovog zakona u roku od jedne (1) godine od njegovog stupanja na snagu. **Član 74****Ukidanje** Stupanjem na snagu ovog zakona, ukida se Zakon br. 03/L-178 o klasifikaciji informacija i verifikaciji bezbednosti (Službeni list Republike Kosovo, br. 76, 10. avgust 2010)**Član 75****Stupanje na snagu**Ovaj zakon stupa na snagu petnaest (15) dana nakon objavljivanja u službenom listu Republike Kosovo**Kadri Veseli****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Predsednik Skupštine Republike Kosovo |