

ZAKON BR.08/L-175**O ZAŠTITI KLASIFIKOVANIH INFORMACIJA**

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 utvrđivanje osnovnih načela minimalnih standarda bezbednosti kao i 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) u kojem se utvrđuje njena misija, organizacija, funkcionisanje, dužnosti i odgovornosti.
3. Ovaj zakon je u skladu sa zakonodavstvom EU, i to:

3.1. Odluka Saveta od 23. septembra 2013. o bezbednosnim pravilima za zaštitu klasifikovanih informacija EU-a.

**Član 2.
Delokrug primene**

Ovaj zakon primenjuju sve javne institucije koje vrše izvršnu, zakonodavnu i sudsku nadležnost, zatim sva fizička i pravna lica, koja bi po principu potreba za saznanjem mogla, u vršenju svojih dužnosti, imati pristup klasifikovanim informacijama Republike Kosovo, drugih država i međunarodnih organizacija.

**Član 3.
Zaštita klasifikovanih informacija**

1. Klasifikovane informacije su zaštićene u skladu sa ovim zakonom.
2. Svako lice kome je poverena klasifikovana informacija ili je upoznato sa njenim sadržajem, odgovorno je za njenu zaštitu u skladu sa ovim zakonom.
3. Celokupnost klasifikovanih informacija zaštićene je najvišim nivoom klasifikacije koju poseduje njegova komponenta.

**Član 4.
Definicije**

1. Izrazi upotrebljeni u ovom zakonu imaju sledeće značenje:

1.1. **Klasifikovana informacija** – svaka informacija ili materijal, za koju je postavljen određeni nivo klasifikacije čije bi neovlašćeno otkrivanje ugrozilo u različitim stepenima bezbednosne interese Republike Kosovo;

1.2. **Potreba da se zna** – je potreba da se ima pristup klasifikovanoj informaciji, u kontekstu određene funkcije i kako bi se ispunio određeni zadatak;

1.3. **Klasifikacija** – akt ili proces utvrđivanja nivoa klasifikacije;

1.4. **Agencija za zaštitu klasifikovanih informacija** (u daljem tekstu **AZKI**) – Nacionalni bezbednosni organ odgovoran za zaštitu klasifikovanih informacija u Republici Kosovo;

1.5. **Organ za proveru** – je Agencija za zaštitu klasifikovanih informacija, specijalizovana za obavljanje bezbednosnih provera lica koja će saznati, proizvoditi, čuvati, upravljati, transportovati i prenositi klasifikovane informacije;

1.6. **Bezbednosni upitnik** – obrazac koji popunjava svako lice koje želi 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“;

1.7. **Sertifikat o bezbednosti osoblja** (u daljem tekstu: SBO) – službeni dokument AZKI-a ili nadležnog organa bezbednosti druge zemlje, koji potvrđuje sa stanovišta bezbednosti da neko lice ispunjava uslove utvrđene za saznanje, čuvanje, upravljanje i prenos klasifikovanih informacija za koje važi određeno vreme i određeni nivo pristupa;

1.8. **Povreda bezbednosti** – radnja ili propust u suprotnosti sa važećim zakonodavstvom, koje dovodi ili može dovesti do krađe, gubitka, oštećenja, kompromitovanja ili neovlašćenog otkrivanje klasifikovanih informacija;

1.9. **Bezbednosna provera** – skup mera i postupaka, koje se primenjuju na fizičko ili pravno lice, a koje služe kao osnov za izdavanje, odbijanje, privremenu suspenziju ili povlačenje „Sertifikata o bezbednosti osoblja“;

1.10. **Neprihvatljiv bezbednosni rizik** – okolnosti opisane u ovom zakonu, na osnovu kojih AZKI odbija izdavanje SBO-a ili procenjuje da mora preduzeti meru njenog povlačenja ili privremene suspenzije;

1.11. **Okolnosti vanredne situacije** – uslovi objektivne nemogućnosti praćenja uobičajenih procedura za dobijanje SBO-a, zbog vršenja kratkoročne službene dužnosti učešća u nepredviđenoj međunarodnoj aktivnosti, produženje rokova vojnih misija u različitim zemljama;

1.12. **Službenik za bezbednost** – odgovorno zaposleno lice ili struktura koje je postavljeno od strane rukovodioca ministarstva ili državne institucije za nadzor i sprovođenje zahteva za bezbednost osoblja i drugih disciplina klasifikovanih informacija;

1.13. **Klasifikovani ugovor** – svaki ugovor koji je javna institucija zaključila sa ugovaračem za snabdevanje robom, izvođenje radova ili pružanje usluga, čije izvođenje zahteva ili uključuje pristup ili stvaranje klasifikovanih informacija ili materijala klasifikovanih prema ovom zakonu;

1.14. **Klasifikovani podugovor** – svaki ugovor koji je ugovarač javne ustanove zaključio sa drugim ugovaračem (tj. podugovaračem) za snabdevanje robom, izvođenje radova ili pružanje usluga, čije izvođenje zahteva ili uključuje unošenje ili stvaranje klasifikovanih informacija;

1.15. **Deklasifikacija** – uklanjanje bilo kojeg nivoa klasifikacije;

1.16. **Dokument** – svaka informacija koja se evidentira bez obzira na njen fizički oblik ili karakteristike;

1.17. **Degradacija** – odluka da se klasifikovane i sačuvane informacije na određenom stepenu klasifikuju i čuvaju na nižem stepenu klasifikacije;

1.18. **Materijal** – svaki dokument, nosilac podataka, deo mašina, opreme koji su proizvedeni ili u procesu proizvodnje;

1.19. **Ovlašćeni nosilac klasifikovanih podataka** – fizičko ili pravno lice koje poseduje klasifikovanu informaciju ima važeći SBO i ispunjava druge uslove koji omogućavaju pristup klasifikovanim podacima, ako zakonom nije drugačije određeno;

1.20. **Sertifikat o industrijskoj bezbednosti** (u daljem tekstu: SIB) – zvanični dokument AZKI-a ili nadležnog bezbednosnog organa druge zemlje, kojim se potvrđuje da, u pogledu bezbednosni, neki ekonomski operater ima organizacione, tehničke i fizičke kapacitete i sposobnosti i da zadovoljava standarde utvrđene za priznavanje, čuvanje i administriranje klasifikovane informacije u nekom projektu/programu ili klasifikovanom ugovoru/podugovoru;

1.21. **Organ za klasifikaciju** – svako lice iz stava 5. ovog zakona, koje ima prvobitnu ili delegiranu nadležnost da klasifikuje informacije.

POGLAVLJE VI.

BEZBEDNOST INFORMACIJA

Član 3.

Organ za klasifikaciju

1. Nadležni organi za klasifikaciju informacija su:

1.1 Predsednik;

1.2 Predsednik Skupštine i članovi Predsedništva Skupštine;

1.3 Predsednik Vlade i ostali članovi Vlade;

1.4 Predsednik Vrhovnog suda;

1.5 Glavni državni tužilac;

1.6 Direktor OAK-a;

1.7 Komandant KBS-a;

1.8 Generalni direktor Policije;

1.9 Rukovodioci nezavisnih institucija.

2. Organi za klasifikaciju informacija propisani u stavu 1. ovog člana, imaju pravo da prenesu nadležnost za klasifikaciju na rukovodiocima njihovih podređenih institucija, nakon što rukovodioci budu informisani o bezbednosnim pravilima i procedurama zaštite klasifikovane informacije i koji su pojedinačno prihvatili svoje odgovornosti u pogledu zaštite takvih informacija.

3. Zahtev za ovlašćenje Organ za klasifikaciju dostavlja AZKI-u, koji nakon razmatranja i procenjivanja, preporučuje davanje ili ne ovlašćenja.

4. Ovlašćenje nadležnosti za klasifikaciju se sačinjava u pisanom obliku i jasno identifikuje rukovodioca po imenu i nazivu položaja, a ovo ovlašćenje važi samo za vreme dok je rukovodilac odgovarajuće institucije.

5. AZKI izrađuje, održava i redovno ažurira registar sa imenima lica koja su nadležna za klasifikaciju.

Član 6.

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 država i međunarodnih organizacija, međunarodni odnosi ili 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/problemi;

1.7. 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 i programi za obezbeđivanje komunikacionih sistema klasifikovanih informacija;

1.11. informacije prikupljene putem specifičnih operacija i elektronskog presretanja koje se odnose na zaštitu Ustavne bezbednosti i reda Republike Kosovo.

Član 7.

Zabrana klasifikacije informacija

1. Klasifikacija informacija je zabranjena kada se vrši u cilju:

1.1. prikrivanja kršenja zakona, zloupotrebe ovlašćenja, neefikasnosti ili administrativne greške;

1.2. lišavanja prava saznanja licu, organizaciji ili instituciji;

1.3. ometanja ili odlaganja pružanja informacija, koje ne zahtevaju zaštitu u interesu bezbednosti Republike Kosovo.

1.4. ograničenja konkurencije.

Član 8.

Stepeni klasifikacije

1. Informacije na osnovu sadržaja, vrednosti i državnog interesa klasifikuju se na jedan od sledećih stepena:

1.1. „STROGA TAJNA“, čije bi neovlašćeno otkrivanje, po razumnoj proceni, nanelo izuzetno ozbiljnu štetu bezbednosnim interesima Republike Kosovo;

1.2. „TAJNA“, čije bi neovlašćeno otkrivanje ozbiljno ugrozilo bezbednosne interese Republike Kosovo;

1.3. „POVERLJIVO“, čije bi neovlašćeno otkrivanje moglo ugroziti bezbednosne interese Republike Kosovo;

1.4. „OGRANIČENO“, čije bi neovlašćeno otkrivanje bilo nepovoljno za bezbednosne interese Republike Kosovo.

2. Organ za klasifikaciju izbegava prekomernu klasifikaciju informacija i dodeljuje im samo onaj nivo klasifikacije koji je neophodan za očuvanje interesa Republike Kosovo.

Član 9.

Trajanje klasifikacije

1. Informacije se klasifikuju sve dok to zahteva bezbednosni interes Republike Kosovo.

2. Vremenski rokovi čuvanja klasifikacije su:

2.1. informacija klasifikovana kao: „OGRANIČENO“ jednu (1) godinu;

2.2. informacija klasifikovana kao: „POVERLJIVO“ pet (5) godina;

2.3. informacija klasifikovana kao: „TAJNA“ petnaest (15) godina; i

2.4. informacija klasifikovana kao: „STROGA TAJNA“ pedeset (50) godina.

3. Obračun roka za čuvanje klasifikacije počinje od dana proizvodnje klasifikovane informacije.

4. Ako organ za klasifikaciju smatra da informaciju treba zaštititi duže nego što je propisano u stavu 2. ovog člana donosi 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 10.

Uslovi za upravljanje klasifikovanim informacijama

1. Proizvodnja klasifikovanih informacija se vrši samo na osnovu spiska klasifikovanih informacija koje je odobrio Organ za klasifikaciju, u skladu sa postupkom utvrđenim važećim zakonodavstvom.

2. Proizvodnja, upotreba, umnožavanje, prenos, fizički transport, arhiviranje, čuvanje i uništenje klasifikovanih informacija vrši se u skladu sa sledećim standardima:

2.1. Bezbednost osoblja – sastoji se od izbora fizičkih lica koja treba da imaju pristup tajnim podacima, verifikacija uslova za pristup klasifikovanim informacijama i njihovog obrazovanja u oblasti bezbednosti;

2.2. Fizička bezbednost – je sistem mera dizajniran da spreči ili ometa neovlašćeni pristup klasifikovanim informacijama ili da pruži dokaze o bilo kakvom pristupu ili pokušaju neovlašćenog pristupa;

2.3. Informaciona bezbednost – sistem mera za poreklo, prijem, registraciju, tretman, otpremu, transport, prenos, ručni transport, čuvanje, uklanjanje, arhiviranje ili neki drugi način rukovanja tajnim podacima, u zavisnosti od slučaja;

2.4. Industrijska bezbednost – sprovođenje mera za obezbeđenje i proveravanje uslova za pristup tajnim podacima sa objekta, i obezbeđenje tretmana poverljivih informacija od strane objekta u skladu sa ovim zakonom;

2.5. Bezbednost informaciono komunikacionih sistema – sistem mera za obezbeđivanje poverljivosti, integriteta i dostupnosti klasifikovanih informacija koje su obrađene od ovih sistema i odgovornost administracije i korisnika za njihovu implementaciju u informacionim ili komunikacionim sistemima koristeći kriptografske metode i materijale u obradi, prenosu ili skladištenju klasifikovanih informacija;

2.6. Rukovodioci javnih ustanova koji proizvode i administriraju klasifikovanim informacijama su dužni da preduzmu sve neophodne radnje za zabranu neovlašćenog pristupa klasifikovanim informacijama tokom životnog ciklusa takvih informacija od proizvodnje, množenja, distribucije, prenosa, obrade i arhiviranja, registracije u odgovarajućim knjigama za upravljanje klasifikovanim informacijama.

3. Postupci za sprovođenje ovog člana regulišu se podzakonskim aktom koji predlaže AZKI i odobrava Vlada.

Član 11. Deklasifikacija

1. Informacije se deklasifikuju kada više nema potrebe za zaštitom i kada njihovo objavljivanje više ne predstavlja pretnju za bezbednost Republike Kosovo.

2. Organ za klasifikaciju, od kojeg klasifikovane informacije potiču, vrši njihovu deklasifikaciju.

3. Slučajevi deklasifikacije klasifikovanih informacija su:

3.1. kada njihovo objavljivanje diktiraju državni interesi, koji su važniji od potrebe da se one klasifikuju;

3.2. nastanak događaja ili određenog datuma kako je odredio Organ za klasifikaciju.

4. Neovlašćeno otkrivanje klasifikovanih informacija ne predstavlja razlog za njihovu deklasifikaciju.

5. Organ za klasifikaciju koji je izvršio deklasifikaciju informacije dužan je da obavesti sve institucije koje poseduju klasifikovanu informaciju;

6. Procedure za sprovođenje ovog člana regulišu se podzakonskim aktom koji predlaže AZKI i odobrava Vlada.

Član 12. Uništavanje klasifikovanih informacija

1. U svakoj državnoj instituciji rukovodilac institucije ili njegov ovlašćeni predstavnik obrazuje 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. Na osnovu odluke Komisije za uništavanje Komisija za uništavanje sprovodi 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 13.

Degradacija i povećanje stepena klasifikacije

1. Organ za klasifikaciju, od kojeg potiču klasifikovane informacije, odgovoran je za degradiranje ili povećanje stepena klasifikacije takvih informacija.
2. Nadležni organ 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.
3. Procedure klasifikacije informacija, uključujući klasifikaciju delova dokumenata, posebnih dokumenata i oznaka koje nose klasifikovane informacije, deklasifikacija i revizija nivoa klasifikacije utvrđuju se podzakonskim aktom koji predlaže AZIK i odobrava Vlada.

Član 14.

Predlog građana

1. Kada građanin ili službenik Republike Kosovo, koji nema ovlašćenje za klasifikaciju, oceni da određene informacija pod kontrolom države ima potrebne vrednosti da bude klasifikovane, predlaže odgovarajućoj instituciji klasifikaciju ove informacije. Ova institucija odlučuje u roku od deset (10) dana da li će se informacija klasifikovati ili ne i obaveštava građanina ili službenika o donetoj odluci.
2. Od trenutka podnošenja predloga za klasifikaciju odgovarajuće informacije, njen vlasnik je obavezan da štiti informaciju od neovlašćenog pristupa.

POGLAVLJE III.

BEZBEDNOST OSOBLJA

Član 15.

Bezbednost osoblja

Bezbednost osoblja je skup mera i postupaka na osnovu kojih se procenjuje da li lice, pridržavajući se njegove lojalnosti, pouzdanosti i bezbednosti, može biti ovlašćeno za pristup klasifikovanoj informaciji, bez ugrožavanja bezbednosti ove informacije.

Član 16.

Sertifikat o bezbednosti osoblja

1. Organ za proveru izdaje SBO samo licu koje je, nakon sprovođenja postupka bezbednosne provere, u skladu sa važećim zakonodavstvom, označeno kao prihvatljivi rizik za bezbednost.
2. SBO jasno ukazuje na stepen klasifikovane informacije, kojem lice koje je prošlo proceduru

bezbednosne provere može imati pristup. SBO za određeni stepen klasifikacije daje nosiocu pristup i informacijama sa nižim stepenom klasifikacije

3. Svaki rukovodilac javne institucije je dužan da u roku od petnaest (15) dana sprovede odluku Organa za proveru i neće dozvoliti pristup klasifikovanim informacijama licu kojem je uskraćen SBO.

Član 17.

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;

1.2. su prethodno obaveštena o saznanju postupaka bezbednosti klasifikovanih informacija i individualnih odgovornosti za narušavanje bezbednosti i koji su potpisali izjavu o čuvanju informacija;

1.3. imaju SBO, osim u slučajevima priznavanja tajnih podataka na „ograničenom“ nivou.

2. Samo predsednik Republike, predsednik Skupštine i predsednik Vlade Republike Kosovo su ovlašćeni da imaju pristup klasifikovanim informacijama bez podvrgavanja proveri bezbednosti pod uslovom da:

2.1. treba da znaju takve informacije;

2.2. budu informisani o pravilima i sigurnosnim procedurama za zaštitu klasifikovanih informacija;

2.3. su potvrdili da su obavešteni o svojim odgovornostima za zaštitu klasifikovanih informacija i da su potpisali izjavu o čuvanju informacija.

Član 18.

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 SBO-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 19.

Uslovi za početak bezbednosne provere

1. Bezbednosna provera počinje tek nakon što je podnosilac zahteva prihvatio i dao pismenu saglasnost za prikupljanje podataka i sprovođenje postupaka 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 20.

Opšti zahtevi za bezbednosnu procenu

1. AZKI, kao jedini Organ za proveru u Republici Kosovo odgovoran za sprovođenje postupka 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, ličnih podataka i državnog statusa, 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 neke neopravdane imovine;
- 1.4. informacije o obrazovanju osobe nakon osamnaest (18) godina starosti ili za period koji se smatra odgovarajućim od strane Organa za proveru;
- 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, trajanju i razlogu prestanka službe u oružanim snagama;
- 1.7. ukupna procena o tome da li osoba može biti stavljena pod pritiskom spoljnog faktora.

Član 21.

Osnovni kriterijumi za procenu bezbednosti

1. Osnovni kriterijumi na osnovu kojih se procenjuje postojanje ili neprihvatljivog bezbednosnog rizika za klasifikovane informacije, koje služe kao osnov za izdavanje, suspendovanje, odbijanje izdavanja ili daljeg posedovanja SBO-a, su slučajevi u kojima pojedinac rezultira da:

- 1.1. je bio, jeste ili pokušava da se tajno angažuje, sam, u saradnji ili u sastavu neke ilegalne organizacije u aktivnostima špijunaže, terorizma, izdaje, pobune, sabotaže ili oružanog nasilja protiv ustavnog poretka ili aktivno podstiče druge da izvrše dela špijunaže, terorizma, izdaje, pobune ili oružanog nasilja protiv ustavnog poretka;
- 1.2. jeste ili je bio saučesnik u špijunaži, terorizmu, izdaji, pobuni, sabotaži ili oružanom nasilju protiv ustavnog poretka, postoji sumnja da je bio ili da je i dalje saradnik predstavnika organizacija, stranih država, uključujući obaveštajne službe, koje mogu ugroziti bezbednost naše zemlje i/ili država članica Severnoatlanskog pakta i Evropske unije, osim ako je takva saradnja odobrena zbog dužnosti;
- 1.3. jeste ili je bio član organizacije koja nasilnim, neprijateljskim i nezakonitim sredstvima ima za cilj rušenje vlade ili promenu ustavnog poretka;
- 1.4. jeste ili je bio pristalica organizacije iz podstava 1.3. ovog člana ili jeste ili je i dalje blisko povezan sa nekim članom takve organizacije;
- 1.5. je namerno prikrio, pogrešno predstavio ili je falsifikovao neku informaciju 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. da je bio zavisn od alkohola, upotrebe ilegalnih droga ili zloupotrebe legalnih droga;

1.8. ima loše ponašanje, sklonost za kriminalno učešće u organizovanom kriminalu, što nosi rizik slabosti pred ucenom ili može da bude pod ozbiljnim uticajem različitih pritisaka;

1.9. je konkretnim postupcima ispoljavao nedostatak lojalnosti, poverenja i sigurnosti;

1.10. je izvršio povredu bezbednosti ili je u više navrata prekršio pravila bezbednosti klasifikovanih informacija, da je pokušao i ili je uspeo da izvrši neovlašćene aktivnosti u sistemima komunikacije klasifikovanih informacija;

1.11. pati od mentalnih poremećaja.

2. Ponašanje i okolnosti bračnog i vanbračnog druga ili užeg člana porodice mogu se takođe smatrati relevantnim prilikom procene bezbednosti.

Član 22. Bezbednosni intervju

1. AZKI može obaviti intervju sa licima koja su podnela zahtev za SBO i prema njima su preduzete procedure za bezbednosnu proveru.

2. AZKI može obaviti intervju sa trećim nepristrasnim licima, kojima je poznata prošlost i aktivnosti lica koje podleže bezbednosnoj proveri.

Član 23. Validnost SBO-a

1. SBO stepena STROGA TAJNA važi za period od pet (5) godina od dana izdavanja;

2. SBO stepena TAJNA važi za period od sedam (7) godina od dana izdavanja;

3. SBO stepena POVERLJIVO važi za period od deset (10) godina od dana izdavanja.

Član 24. Produženje roka SBO-a u okolnostima vanrednog stanja

1. U okolnostima vanrednog stanja, AZKI ima pravo da produži rok važenja SBO-a pojedinca samo jednom i to do šezdeset (60) kalendarskih dana tokom ciklusa njegovog važenja pod sledećim uslovima:

1.1. lice, za koje se traži produženje roka važenja, treba da poseduje važeći SBO, koji je izdat odgovarajućom procedurom. Isključeni su slučajevi produženja roka važenja SBO-a koji je izdat u okolnostima vanrednog stanja;

1.2. postoji zvaničan zahtev koji objašnjava okolnosti vanrednog stanja i dokazuje okolnosti nemogućnosti prijave u skladu sa normalnim procedurama za ponovno dobijanje novog SBO-a, kada:

1.3. lice obavlja kratkoročnu službenu dužnost, za koju je bilo nemoguće poštovanje procedura, 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. je lice, koje ima SBO, u procesu produženja roka za učešće u vojnim misijama van zemlje i nemogućnosti prijave u skladu sa normalnim procedurama za dobijanje novog SBO -a;

1.6. produženje rokova SBO -a pod gore navedenim uslovima je dozvoljeno za SBO-e stepena „Poverljivo“, „Tajna“ i „Stroga tajna“.

2. Sva lica kojima je SBO produžen u vanrednim okolnostima i uslovima, dužna su da se u pisanom obliku izjasne o tome da su shvatila sve svoje obaveze o čuvanju klasifikovanih informacija.

Član 25.

Ponavljanje bezbednosne provere

1. Lica kojima je izdat SBO podležu novoj bezbednosnoj proveri u sledećim redovnim intervalima:

1.1. svakih deset (10) godina za lica koja već imaju SBO, što im omogućuje pristup klasifikovanim informacijama stepena „POVERLJIVO“;

1.2. svakih sedam (7) godina za lica koja već imaju SBO što im omogućuje pristup klasifikovanim informacijama stepena „TAJNA“;

1.3. svakih pet (5) godina za lica koja već imaju SBO što 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 i pre isteka roka važenja SBO-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 26.

Privremeno odbijanje, opoziv i suspenzija SBO-a

1. AZKI donosi odluku o odbijanju, opozivu ili privremenoj suspenziji SBO-a u slučajevima kada je dobila informaciju, kojom se smatra da izdavanje ili dalje držanje SBO-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 privremenom odbijanju, opozivu ili suspenziji SBO-a, pismeno se dostavlja rukovodiocu odgovarajuće javne institucije, koja je podnela zahtev za vođenje postupka bezbednosne provere.

3. Procedure za proveru bezbednosti osoblja definišu se podzakonskim aktom koji predlože od strane AZKI, a usvaja Vlada.

Član 27.

Pravo na žalbu

1. Lice kome je odbijena Sertifikat o bezbednosti osoblja ima pravo da podnese žalbu AZKI u roku od petnaest (15) dana od dana prijema obaveštenja;

2. Žalbu razmatra Komisija za žalbe.

Član 28.

Komisija za žalbe

1. Komisija za žalbe se sastoji od pet (5) članova sa po jednim (1) predstavnikom sledećih institucija:

- 1.1. Ministarstvo odbrane;
- 1.2. Policija Kosova;
- 1.3. Tužilački savet Kosova;
- 1.4. Sudski savet Kosova;
- 1.5. Obaveštajna Agencija Kosova.

2. Predlogom rukovodilaca relevantnih institucija, Vlada odlukom obrazuje Komisiju za žalbe.

3. Mandat članova komisije je tri (3) godine uz mogućnost produženja.

4. Članovi Komisije za žalbe moraju biti profesionalci, sa visokim integritetom i da imaju SBO najvišeg stepena, sa informacijama koje treba pregledati u postupku žalbe.

5. Lice ovlašćeno od AZKI-a vrši predstavljanje slučaja pred članovima Komisije za žalbe.

6. Nakon razmatranja žalbe, Komisija preporučuje direktoru AZKI-a da donese odluku.

7. Pravila i procedure Komisije za žalbe i druga pitanja, koja se odnose na razmatranje žalbi regulisana su podzakonskim aktom koji predlaže AZKI a odobrava Vlada.

Član 29.

Rokovi i trajanje koje pokriva bezbednosnu proveru

1. Ukupni rok za sprovođenje procedura za proveru i izdavanje SBO-a od strane AZKI-a je do sto dvadeset (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 deset (10) godina. Kada ovaj period nije dovoljan, provera se proteže od osamnaest (18) godina do trenutnog doba.

4. Ako Organ za proveru nije u mogućnosti da prikupi i obraditi sve potrebne informacije za obavljanje bezbednosne provere u rokovima navedenim u stavu 1. ovog člana, Organ za proveru može odlukom da produži rok do šezdeset (60) kalendarskih dana. Rukovodilac relevantne institucije se obaveštava o donetoj odluci.

Član 30.

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 kom drugom obliku je uspeo posedovati klasifikovane informacije.

2. Prilikom napuštanja javne institucija, raskida radnog odnosa ili nekog drugog ugovornog odnosa, službenom ili ugovornom licu je zabranjeno uklanjanje ili otkrivanje u bilo kom obliku klasifikovanih informacija iz kontrole javne institucije.

Član 31.

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, Ministarstvo odbrane i drugih institucija javne bezbednosti biće od primarnog značaja.
3. Tokom sprovođenja postupka bezbednosne provere, Organ za proveru po potrebi sarađuje sa srodnim institucijama drugih država.

Član 32.

Bezbednosna provera zaposlenih u Obaveštajnoj Agenciji Kosova

1. Bezbednosnu proveru zaposlenih u Obaveštajnoj Agenciji Kosova (u daljem tekstu: OAK) vrši OAK u skladu sa relevantnim zakonom Obaveštajnoj Agenciji Kosova i primenom kriterijuma i standarda utvrđenih ovim zakonom u pogledu bezbednosne provere osoblja.
2. AZKI izdaje zaposlenim u OAK-u SBO na zahtev OAK-a.

Član 33.

Bezbednosni dosije

1. Sertifikat o bezbednosti, popunjeni bezbednosni upitnik i sva ostala relevantna dokumenta i materijale, koji se odnose na bezbednosnu proveru, čuva Organ za proveru u bezbednosnom dosijeju.
2. Pored podataka iz stava 1. ovog člana, bezbednosni dosije sadrži i podatke o naknadnim promenama u vezi sa informacijama predstavljanim u bezbednosnom upitniku.
3. Rukovodilac javne institucije i provereno lice dužni su da odmah obaveste Organ za proveru o svakom novom razvoju događaja ili novim 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. Rukovodilac javne institucije je dužan da obavesti AZIK o svakoj promeni koja se odnosi na službenike koji imaju SBO za premeštaj, unapređenje ili otpuštanje.
5. Organ za proveru klasifikuje i održava bezbednosni dosije na način koji bezbednosnom dosijeju daje stepen klasifikacije i zaštite koji smatra neophodnim za očuvanje interesa bezbednosti Kosova.

Član 34.

Obrada podataka

1. Organ za proveru može obraditi lične podatke proverene osobe koji se nalaze u bezbednosnom dosijeju 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 dosijeju, 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 za potrebe krivičnog gonjenja samo kao poslednje sredstvo kada se takvi podaci ne mogu prikupiti na drugi način ili ako bi se ozbiljno sprečilo krivično gonjenje u odsustvu pristupa takvim podacima.

Član 35.

Informacije o ličnim podacima

1. Lice koje je bilo podvrgnuto ili je u toku provere bezbednosti ima pravo da bude obavešteno od strane Organa za proveru o svim ličnim podacima prikupljenim i sačuvanim tokom postupka bezbednosne provere. Informaciju o ličnim podacima daje Organ za proveru na osnovu pismenog zahteva koji je podnela verifikovana osoba.

2. Organ za proveru odbija zahtev ako:

2.1. bi otkrivanje traženih informacija ugrozilo javnu bezbednost ili bezbednosne interese Republike Kosovo; ili

2.2. treba da informacija bude poverljiva kako bi se zaštitila legitimna prava i interesi trećeg lica ili obaveštajnih izvora.

3. U slučaju odbijanja zahteva, osoba koja traži informacije može podneti žalbu Agenciji za informacije i privatnost u skladu sa relevantnim zakonom o zaštiti ličnih podataka.

POGLAVLJE IV.

INDUSTRIJSKA BEZBEDNOST

Član 36.

Zaštita klasifikovanih informacija u oblasti industrije

1. Zaštita klasifikovanih informacija u oblasti industrijskoj vrši se utvrđivanjem preventivnih mera i postupaka od neovlašćenog otkrivanja, gubitka ili narušavanja bezbednosti klasifikovane informacije, koja se obrađuje u skladu sa 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 37.

Uslovi za zaključivanje klasifikovanog ugovora

1. Ekonomski operateri koji su zainteresovani za učešće u nabavci klasifikovanoj kao „TAJNA“ i „POVERLJIVO“, potrebno je da imaju odgovarajući stepen provere bezbednosti. Osoblje koje zastupa ekonomskog operatera u klasifikovanoj nabavci i drugi pojedinci, koji će imati pristup klasifikacionim informacijama, treba da budu sertifikovani na odgovarajući način, u skladu sa zahtevima važećeg zakonodavstva.

2. Ekonomski operateri koji su zainteresovani za učešće u klasifikovanoj nabavci na nivou „OGRANIČENO“, ne dobijaju SIB.

3. Osoblje koje zastupa Ekonomskog operatera u ovoj nabavci i sva lica koja će imati pristup klasifikovanim informacijama, upoznaju se o bezbednosnim pravilima i procedurama zaštite poverljivih informacija i pojedinačno prihvataju svoje odgovornosti u pogledu zaštite takvih informacija, potpisuju izjavu o čuvanju klasifikovanih informacija pre pokretanja procedura klasifikovane nabavke.

Član 38.

Dobijanje Sertifikata industrijske bezbednosti

1. SIB izdaje AZKI, u skladu sa zahtevima važećeg zakonodavstva.
2. Za ekonomske operatere drugih zemalja, SIB izdaje Organ nacionalne bezbednosti ili bilo koji nadležni organ bezbednosti zemlje, u kojoj je registrovan ekonomski operater. Ovaj sertifikat se smatra važećim za učešće u klasifikovanoj nabavci, samo nakon pismene potvrde AZKI-a, upućenoj ugovornom organu. Pre potvrđivanja SIB-a, AZKI sarađuje sa srodnim organima za obavljanje odgovarajućih provera.
3. Tek nakon prijema 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, u skladu sa relevantnim standardima koje je uspostavila Organizacija Severnoatlantskog pakta i Evropska unija, a koje je predložio AZKI a odobrila Vlada.

Član 39.

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. vlasnike/akcionare i rukovodeće osoblje, koji će zbog svojih funkcija imati pristup klasifikovanim informacijama;
 - 1.3. lice predloženo na mestu službenika za obezbeđenje, njegovog zamenika i zaposlene, 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 40.

Uslovi za sklapanje klasifikovanih podugovora

1. U svakom slučaju, pre početka pregovora za sklapanje klasifikovanog podugovora, Ugovarač 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“, da stupi u ugovorne odnose pod uslovima klasifikovanog podugovora.

3. Svi kriterijumi za zaključivanje/sprovođenje klasifikovanog ugovora primenjuju se na odgovarajući način i sa podizvođačem radova.

Član 41.

Prevoz i međunarodne posete

1. Prevoz klasifikovanog materijala tokom sprovođenja klasifikovanog ugovora vrši se kopnenim, morskim, železničkim i vazdušnim putem, u skladu sa bezbednosnim pravilima i zahtevima važećeg zakonodavstva.

2. Bezbednosni standardi klasifikovanih informacija u oblasti industrijske bezbednosti primenjuju se i tokom međunarodnih poseta.

POGLAVLJE V.

BEZBEDNOST KOMUNIKACIONIH I INFORMACIONIH SISTEMA

Član 42.

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 43.

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 44.

Komunikacioni i informacioni sistemi

1. Mehanizmi i procedure upravljanja bezbednošću su uspostavljeni u cilju ometanja, sprečavanja, otkrivanja, odupiranja i oporavljanja od uticaja 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 namernom ili slučajnom ugrožavanju bezbednosnih ciljeva u skladu sa štetom koja može biti prouzrokovana;

1.2. pouzdanu identifikaciju i autentifikaciju lica, uređaja i usluga kojima je dozvoljen pristup. Informacija koja kontroliše pristup komunikacionim i informacionim sistemima

je kontrolisana i zaštićena u skladu sa stepenom klasifikacije informacije za koju odobrava pristup;

1.3. kontrolisanje pristupa klasifikovanim informacijama u skladu sa principom „potreba saznanja“;

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 nepobitnosti kako bi pošiljalac informacija dobio potvrdu o preuzimanju poruke od strane primaoca i da primalac dobije potvrdu o identitetu pošiljaoca;

1.10. obezbeđivanje da u slučaju narušavanja bezbednosti sva uključena pravna i fizička lica budu obaveštena da je informacija ugrožena.

POGLAVLJE VI. FIZIČKA BEZBEDNOST

Član 45. 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 i uništava klasifikovana informacija, uključujući i proces upravljanja rizikom za sprečavanje neovlašćenog pristupa sigurnosnim zonama.

2. Državne institucije su dužne da preduzmu mere za fizičko obezbeđenje 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, koje su odredili Organizacija Severnoatlantskog pakta i Evropska unija.

3. Rukovodilac institucije nalogom odobrava podelu bezbednosnih zona koji je praćen 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 46.

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 utvrdio AZKI.
3. Model za obeležavanje klasifikovanih informacija je jedinstven, određuje ga 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 AZKI-a.

Član 47.

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 48.

Strane informacije

1. Državne institucije čuvaju klasifikovane informacije stranih zemalja 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.
3. Potpisivanju sporazuma ili tehničkog protokola, koji obuhvata razmenu klasifikovanih informacija, mora da prethodi potpisivanje opšteg sporazuma o bezbednosti klasifikovanih informacija između organa nacionalne bezbednosti država ugovornica.

Član 49.

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 dužne 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 50.

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 51.

Implementacija standarda EU-a i NATO-a

1. AZKI je organ bezbednosti Republike Kosovo, koji se stara o dostizanju bezbednosnih standarda za zaštitu tajnih podataka u skladu sa zahtevima, koji proizilaze iz bezbednosnih direktiva NATO-a i EU-a.
2. AZKI razmenjuje klasifikovane informacije sa svim državama članicama NATO-a i EU-a, kao i drugim državama u skladu sa potpisanim sporazumima i relevantnim zakonodavstvom na snazi.
3. Prema direktivama NATO-a i EU-a, AZKI priznaje bezbednosne sertifikate osoblja i sertifikate o industrijskoj bezbednosti država sa kojima je potpisala sporazume o bezbednosti.

Član 52.

Narušavanje bezbednosti i kompromitovanje klasifikovanih informacija

1. Narušavanje bezbednosti nastaje kao rezultat činjenja ili nečinjenja lica koje postupa suprotno bezbednosnim pravilima utvrđenim ovim zakonom i drugim podzakonskim aktima.
2. Kompromitacija klasifikovanih informacija nastaje kada je, kao rezultat narušavanja bezbednosti, došlo do njihovog potpunog ili delimičnog otkrivanja neovlašćenom licu.
3. Svako narušavanje ili sumnju da je došlo do narušavanja bezbednosti odmah se prijavljuje organu bezbednosti AZKI-a.
4. Kada je poznato ili kada postoji dovoljan razlog da se tvrdi da su klasifikovane informacije kompromitovane ili izgubljene, u skladu sa zakonom i podzakonskim aktima, organ za bezbednost preduzima sledeće mere:
 - 4.1. informiše nadležni organ;
 - 4.2. obezbeđuje da slučaj istraži osoba koja je neutralna u vezi sa tim pitanjem;
 - 4.3. utvrđuje potencijalnu štetu, koja je prouzrokovana interesima Republike Kosovo ili drugim državama i organizacijama;
 - 4.4. poduzima odgovarajuće mere kako bi se sprečilo ponavljanje;
 - 4.5. o preduzetim merama obaveštava nadležne organe.
5. Svaka osoba koja je odgovorna za narušavanje bezbednosnih pravila utvrđenih ovim zakonom i podzakonskim aktima, podleže disciplinskim kaznama, u skladu sa važećim zakonodavstvom.

6. Svako lice odgovorno za kompromitovanje ili gubitak klasifikovanih informacija podleže disciplinskom/sudskom postupku u skladu sa relevantnim zakonodavstvom na snazi.

Član 53. **Gubitak klasifikovanih informacija**

1. Za svaki sumnjiv gubitak, navodno kršenje bezbednosti poverljivih informacija i svaki sumnjivi neovlašćeni pristup klasifikovanim informacijama, svi ovlašćeni nosioci klasifikovanih informacija odmah će to prijaviti svojoj relevantnoj javnoj instituciji, državnom tužilaštvu i AZKI-u.

2. AZKI, na sopstvenu inicijativu ili na zahtev nadležnog organa, u slučaju navodnih povreda ovog zakona, odmah preduzima sve dole navedene neophodne mere da:

- 2.1. obavesti državnog tužioca u slučaju sumnje da kršenje čini krivično delo;
- 2.2. ispita slučaj;
- 2.3. identifikuje uzrok gubitka,
- 2.4. istraži moguće otvaranje od strane neovlašćenih lica za pristup takvim informacijama;
- 2.5. ukloni štetne efekte i spreči dalji gubitak klasifikovanih informacija.

3. Ukoliko se sumnja da navodna povreda predstavlja krivično delo, obaveštava državnog tužioca.

POGLAVLJE VII. **KAZNENE ODREDBE**

Član 54. **Krivične sankcije**

1. Kogod otkrije ili ne čuva klasifikovanu informaciju kao „POVERLJIVO“, čini krivično delo i kažnjava se kaznom zatvora u trajanju od jedne (1) do pet (5) godine.

2. Kogod otkrije ili ne čuva klasifikovanu informaciju kao „TAJNA“, čini krivično delo i kažnjava se kaznom zatvora u trajanju od tri (3) do deset (10) godine.

3. Kogod otkrije ili ne čuva klasifikovanu informaciju kao „STROGA TAJNA“, čini krivično delo i kažnjava se zatvorom u trajanju od pet (5) do dvanaest (12) godine.

Član 55. **Inspekcijski nadzor javnih institucija i ekonomskih operatera**

1. AZKI vrši inspekcijski nadzor u vezi sa sprovođenjem mera bezbednosti za zaštitu klasifikovanih informacija kod javnih institucija i ekonomskih operatera koji upravljaju klasifikovanim informacijama.

2. Inspekcijski nadzor se redovno obavlja i uz prethodno obaveštavanje javne institucije.

3. Predmet inspekcijskog nadzora bez prethodnog obaveštavanja je samo ona institucija ili ekonomski operater za koji postoje pouzdane informacije da ima kršenja bezbednosti u smislu upravljanja klasifikovanim informacijama.

4. Predmet inspekcijskog nadzora su sledeće discipline:

- 4.1. bezbednost osoblja;
- 4.2. industrijska bezbednost;
- 4.3. bezbednost komunikacionih i informacionih sistema;
- 4.4. fizička bezbednost;
- 4.5. upravljanje klasifikovanim informacijama.

5. AZKI obezbeđuje standarde fizičke bezbednosti za zaštitu klasifikovanih informacija kojima upravlja i nadgleda njihovu primenu u skladu sa zahtevima utvrđenim važećim zakonodavstvom.

6. Po završetku inspekcijskog nadzora mera bezbednosti, AZKI izrađuje detaljan izveštaj o nalazima i predlaže preduzimanje odgovarajućih mera za povećanje stepena bezbednosti klasifikovanih informacija.

7. Izveštaj se upućuje rukovodiocu odgovarajuće javne institucije.

8. U koordinaciji sa rukovodiocem javne institucije izrađuje se plan za sprovođenje preporuka koje proizilaze iz izveštaja o inspekcijskom nadzoru.

9. 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 inspekcijskog nadzora.

POGLAVLJE VIII. AGENCIJA ZA ZAŠTITU KLASIFIKOVANIH INFORMACIJA

Član 56. Osnivanje i status AZKI

1. 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. Svi zaposleni i osoblje angažovano za rad u AZIK moraju da budu politički nepristrasni, profesionalni, bez predrasuda u svojoj proceni i da deluju isključivo u skladu sa zakonom.

3. AZKI je pravno lice sa sedištem u Prištini.

4. AZKI ima svoj logo.

Član 57. Odgovornosti AZKI-a u oblasti zaštite klasifikovanih informacija

1. AZKI je nezavisna centralna specijalizovana 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 Republike Kosovo kao i njihovih izvođača radova, i odgovorna je za:

- 1.1. izradu politika;

- 1.2. praćenje procedura;
- 1.3. nadgledanje institucija i izvođača radova u klasifikovanim ugovorima;
- 1.4. bezbednosnu edukaciju;
- 1.5. bezbednost osoblja;
- 1.6. fizičku bezbednost;
- 1.7. bezbednost informacija;
- 1.8. industrijsku bezbednost;
- 1.9. bezbednost sistema komunikacije i informacije;
- 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 organizacija

3. 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, predlaže se predsedniku Vlade na usvajanje.

5. Unutrašnja organizacija i funkcionisanje AZKI-a je regulisana podzakonskim aktom koji predlaže AZKI a odobrava predsednik Vlade.

Član 58.

Pripremanje i obezbeđivanje budžeta

1. Direktor AZKI-a priprema i podnosi predsedniku Vlade nacrt godišnjeg budžeta za AZKI.
2. AZKI je autonomna budžetska organizacija sa sopstvenim budžetskim kodom.
3. AZKI-u se stavlja na raspolaganje godišnji budžet neophodan za obavljanje zadataka i odgovornosti za zaštitu klasifikovanih informacija u skladu sa važećim zakonodavstvom.

Član 59.

Kriterijumi za imenovanje direktora

1. Kriterijumi za imenovanje generalnog direktora AZKI-a su:
 - 1.1. da je državljanin samo Republike Kosovo;
 - 1.2. da ima univerzitetsku diplomu;
 - 1.3. da ima najmanje osam (8) godina profesionalnog iskustva u bezbednosnim institucijama, od kojih najmanje pet (5) godina radnog iskustva na rukovodećem položaju;

- 1.4. da nije osuđen pravosnažnom odlukom za krivično delo;
- 1.5. da, u poslednjih pet (5) godina, nije bio kažnjen zbog teških disciplinskih prekršaja;
- 1.6. da nema sukoba interesa sa dužnošću ili kao što je predviđeno zakonom o sprečavanju sukoba interesa u vršenju javnih funkcija.

Član 60.

Imenovanje direktora AZKI-a

1. Direktora AZKI-a imenuje predsednik Vlade
2. U slučaju upražnjenog radnog mesta, predsednik Vlade imenuje direktora AZKI-a u roku od dvadeset (20) radnih dana.
3. Direktor AZKI-a se razrešava po istom postupku po kom je imenovan.
4. Direktor AZKI-a, u skladu sa ovim zakonom, Pravilnikom o unutrašnjoj organizaciji i drugim važećim zakonima, odgovoran je za sve aspekte upravljanja AZKI-om.
5. U izvršavanju svojih odgovornosti, direktoru AZKI-a pomaže zamenik direktora, rukovodioci organizacionih jedinica i osoblje sa odgovarajućim kvalifikacijama, u skladu sa pravilima i procedurama utvrđenim ovim zakonom i Pravilnikom o unutrašnjoj organizaciji.

Član 61.

Završetak mandata direktora

1. Mandat direktora prestaje kada:
 - 1.1. je osuđen za krivično delo;
 - 1.2. doseže doba za odlazak u penziju;
 - 1.3. podnese ostavku;
 - 1.4. zbog nemogućnosti vršenja dužnosti u periodu dužem od šest (6) meseci;
 - 1.5. po isteku mandata;
 - 1.6. zbog slabog dokumentovanog učinka.

Član 62.

Direktor AZKI-a

1. Direktor AZKI-a direktno odgovara predsedniku Vlade.
2. Direktor AZKI-a:
 - 2.1. savetuje predsednika Vlade o pitanjima zaštite klasifikovanih informacija;
 - 2.2. izveštava i obaveštava predsednika Vlade o aktivnostima AZKI-a;
 - 2.3. daje podatke predsedniku Vlade vezano za klasifikacijom informacija i bezbednosne provere;
 - 2.4. štiti i pomaže u zaštiti klasifikovanih informacija od neovlašćenog objavljivanja;

- 2.5. uspostavlja i koordinira odnose sa stranim srodnim agencijama;
- 2.6. obezbeđuje da AZKI obavlja posao na nepristrastan i apolitički način u vezi sa svim zajednicama i političkim subjektima;
- 2.7. obezbeđuje da AZKI ne preduzima nikakvu radnju kako bi uticala na političke procese, javno mišljenje i medije na Kosovu;
- 2.8. priprema godišnji izveštaj o radu i predlaže preduzimanje neophodnih mera za povećanje nivoa bezbednosti klasifikovanih informacija;
- 2.9. inicira i potpisuje Memorandume o razumevanju i saradnje sa drugim institucijama i organima;
- 2.10. najmanje jednom godišnje izveštava nadležnoj parlamentarnoj komisiji.

Član 63.

Zamenik direktora AZKI-a

- 1. Zamenika direktora imenuje predsednik Vlade, na predlog direktora iz redova osoblja AZKI-a.
- 2. Kriterijumi za imenovanje i prestanak mandata direktora odnose se i na zamenika direktora.
- 3. Zamenik direktora AZKI-a pomaže direktoru AZKI-a i upravlja aktivnostima organizacionih jedinica AZKI-a pod nadzorom direktora AZKI-a.
- 4. Zamenik direktora AZKI-a se razrešava dužnosti istim postupkom kojim je imenovan.
- 5. Zamenik direktora AZKI-a privremeno obavlja i vrši odgovornosti direktora AZKI-a za vreme odsustva ili nemogućnosti direktora. U slučaju trajne nemogućnosti, zamenik direktora AZKI-a obavlja i vrši odgovornosti direktora AZKI-a, sve do imenovanja novog direktora.

Član 64.

Specifični uslovi za zaposlene u AZKI-u

- 1. Lica izabrana za rad u AZKI-u treba da ispune stroge bezbednosne standarde, koji su utvrđeni u skladu sa važećim zakonom.
- 2. AZKI ne zapošljava kandidate koji ne ispune uslov bezbednosti.
- 3. Pored opštih zahteva za zapošljavanje, koji se sprovode za druge zaposlene u vladi, mogu se primeniti posebni uslovi za zaposlene u AZKI-u u vezi sa uslovima stručnosti, zdravlja, radnih zadataka i bezbednosnih uslova, koji su u skladu sa interesima bezbednosti Kosova.
- 4. Poslovník o unutrašnjoj organizaciji AZKI-a, utvrđuje uslove za svaku poziciju u AZKI-u, kao i postavlja specifične uslove za zapošljavanje u AZKI-u.
- 5. U skladu sa internim pravilima i kada je to neophodno, AZKI može angažovati treća lica za pomoćne usluge.

Član 65.

Kvalifikacije za zapošljavanje u AZKI-u

- 1. Kandidati za AZKI moraju ispuniti sledeće uslove:

- 1.1. da su državljani Kosova;
- 1.2. da imaju odgovarajuće obrazovne i profesionalne kvalifikacije, kao što je to utvrđeno Poslovnikom o unutrašnjoj organizaciji;
- 1.3. da obave lekarski pregled neophodan za tu poziciju;
- 1.4. da budu u mogućnosti da ispune bezbednosne uslove koji će biti određeni ovim zakonom i podzakonskim aktima.

2. Pravila i procedure za opšte uslove i procedure zapošljavanja, radne odnose, obuke, napredovanja u karijeri i imenovanja pozicija su utvrđeni Uredbom o radnom odnosu u AZKI-u koju je usvojila Vlada.

Član 66.

Status zaposlenih u AZKI-u

Zaposleni u AZKI-u imaju poseban status prema ovom zakonu. Za pitanja koja nisu uređena ovim zakonom ili podzakonskim aktima, koji proističu iz ovog zakona, primenjivaće se na odgovarajući način zakoni koji uređuju pitanja civilne službe.

Član 67.

Prava zaposlenih u AZKI-u

1. Zaposleni u AZKI-u imaju pravo:
 - 1.1. 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;
 - 1.2. da uzmu odmor u skladu sa važećim zakonodavstvom i mogućnost da nastave sa istim ili sličnim radom, kada se odmor završi;
 - 1.3. na nadoknadu za dužnosti i obavljanje dužnosti, kao što je utvrđeno ovim zakonom;
 - 1.4. da primaju plate, dodatke i ostale naknade;
 - 1.5. na napredovanje karijere i profesionalnog razvoja putem obuka i drugih sredstava.

Član 68.

Zabranjeno ponašanje zaposlenih

1. Zaposleni u AZKI-u ne mogu da budu članovi političkih subjekata ili da od njih ili pojedinaca dobijaju uputstva AZKI-a, kao i ne treba da javno izražavaju svoja politička uverenja i preferencije.
2. Zaposleni ne mogu obavljati ni jednu drugu plaćenu javnu ili profesionalnu delatnost ili zadatak, koji nisu u skladu sa radom AZKI-a ili stvaraju sukob interesa.
3. Zaposleni u AZKI-u ne mogu da imaju drugo zaposlenje dok su zaposleni u AZKI-u.
4. Zaposleni u AZKI-u nemaju pravo na delatnosti koje imaju za cilj prestanak aktivnosti ili bilo kog drugog oblika kolektivne obustave rada.
5. Zaposleni u AZKI-u, bez prethodne saglasnosti direktora AZKI-a, ne mogu davati izjave za javnost ili da na drugi način daju komentare o radu AZKI-a ili daju informacije neovlašćenim licima, o podacima, dokumentima, kontaktima, ciljevima, saznanjima ili osoblju AZKI-a.

6. Ukoliko se kandiduje na izborima za Skupštinu Kosova ili za organe lokalne samouprave, obavezuju se da traže oslobađanje od dužnosti i ne mogu da ponovo budu primljeni u AZKI.

Član 69.

Lične zakonske obaveze zaposlenog

1. Svaki zaposleni u AZKI-u obavlja funkcije koje su mu dodeljene u skladu sa ovim Zakonom i drugim odgovarajućim zakonima i lično je odgovoran za zakonito sprovođenje zadataka AZKI-a, kao što je definisano ovim zakonom i koji su u okviru zadataka dodeljenih određenom zaposlenom.
2. Ukoliko zaposleni smatra da je dobio nezakonitu naredbu, 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 neovlašćeno 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 AZKI-om;
5. Obezbeđuje da informacije prikupljene tokom vršenja dužnosti ne budu upotrebljene u druge svrhe osim onih utvrđenih ovim zakonom;
6. Obezbeđuje zaštitu i ne 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 70.

Plate i naknade za zaposlene u AZKI-u

1. Dodatna plaćanja i naknade osoblja AZKI-a određuje Vlada, u skladu sa specifičnostima posla i posebnim statusom AZKI-a.
2. Pored osnovne plate, zaposleni AZKI-a mogu zakonski primiti i druge vrste dodataka na platu, dnevnice i beneficije, na osnovu faktora koji uključuju poteškoće u radu, prekovremeni rad ili specijalne sposobnosti.

Član 71.

Prestanak radnog odnosa

1. Radni odnos zaposlenih u AZKI-u prestaje:
 - 1.1. dobrovoljnim podnošenjem ostavke AZKI-u;
 - 1.2. završetkom ugovora;
 - 1.3. dostizanjem starosti za penzionisanje;
 - 1.4. trajna nemogućnost za obavljanje službene dužnosti zbog zdravstvenog stanja, pod uslovom da zaposleni nema pravo da bude prebačen na drugu odgovarajuću poziciju u AZKI-u;
 - 1.5. gubitkom državljanstva Kosova;
 - 1.6. pravosnažnom presudom za krivično delo;
 - 1.7. isključenjem iz AZKI-a kao rezultat disciplinskog postupka.

Član 72.

Identifikacione kartice

Zaposlenima u AZKI-u se izdaju identifikacione kartice. Vrsta, oblik i sadržaj identifikacione kartice zaposlenog u AZKI-u se utvrđuje Odlukom donetom od strane direktora AZKI-a.

Član 73.

Pravilnik i unutrašnja organizacija

Unutrašnja organizacija AZKI-a se utvrđuje Pravilnikom o unutrašnjoj organizaciji koji usvaja predsednik Vlade.

POGLAVLJE IX.

PRELAZNE I ZAVRŠNE ODREDBE

Član 74.

Prelazne odredbe

1. Nakon imenovanja, direktor AZKI-a, u saradnji sa direktorom OAK-a, započinje postupak prenošenja 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 i osobljem OAK-a do funkcionalnosti AZKI.
5. Sve licence za bezbednost izdate od odeljenja za verifikaciju bezbednosti unutar OAK-a ostaju na snazi do isteka njihovog roka.
6. Postupci verifikacije bezbednosti koji su započeti pre stupanja na snagu ovog zakona završiće se u roku od tri (3) meseca u skladu sa odredbama Zakona br.03/L-178 o klasifikaciji informacija i verifikaciji bezbednosti.
7. Vlada obezbeđuje odgovarajući objekat sa bezbednosnim standardima u funkciji postizanja mandata AZKI-a za zaštitu klasifikovanih informacija Republike Kosovo.
8. U svakoj odredbi zakona, podzakonskih akata, izraz OAK korišćen u smislu organa za proveru, stupanjem na snagu ovog zakona zamenjuje se izrazom AZKI.

Član 75.

Podzakonski akti

1. Vlada usvaja podzakonske akte za sprovođenje ovog zakona u roku od šest (6) meseci od njegovog stupanja na snagu.
2. Pod uslovom da nisu u suprotnosti sa ovim zakonom i do donošenja podzakonskih akata predviđenih ovim zakonom, primenjuju se podzakonski akti koji su trenutno na snazi.

Član 76.
Stavljanje van snage

Stupanjem na snagu ovog zakona prestaje da važi Zakon br.03/L-178 o klasifikaciji informacija i verifikaciji bezbednosti.

Član 77.
Stupanje na snagu

Ovaj zakon stupa na snagu petnaest (15) dana nakon objavljivanja u Službenom listu Republike Kosovo.

Zakon br.08/L-175
9. februar 2023. godine

Proglaseno ukazom Br. DL-25/2023, dana 02.03.2023, od strane Predsednice Republike Kosova Vjosa Osmani-Sadriu