

**REPUBLIKA E SHQIPËRISË**

**K u v e n d i**

**P R O J E K T L I G J**

**Nr.\_\_\_\_/ 2021**

**PËR INFORMACIONIN E KLASIFIKUAR[[1]](#footnote-1)**

Në mbështetje të neneve 78 dhe 81, pika 1, të Kushtetutës, me propozimin e Këshillit të Ministrave, Kuvendi i Republikës së Shqipërisë,

**V E N D O S I:**

**KREU I**

**DISPOZITA TË PËRGJITHSHME**

**Neni 1**

**Objekti**

Objekti i këtij ligji është përcaktimi i parimeve bazë dhe i rregullave të përgjithshme për krijimin, administrimin dhe mbikëqyrjen e informacionit të klasifikuar gjatë gjithë ciklit jetësor të tij.

**Neni 2**

**Qëllimi**

Qëllimi i këtij ligji është mbrojtja e informacionit të klasifikuar nga humbja, dëmtimi, rrjedhja, kompromentimi dhe/ose ekspozimi i paautorizuar.

**Neni 3**

**Fusha e veprimit**

Ky ligj zbatohet për të gjitha institucionet publike, personat fizikë, juridikë, të cilët për ushtrimin e detyrave të tyre dhe bazuar në parimin “nevojë për njohje” kërkohet të kenë qasje në informacionin e klasifikuar.

**Neni 4**

**Përkufizime**

Në kuptim të këtij ligji, termat e mëposhtëm kanë këto kuptime:

1. **“Administrim** **i informacionit të klasifikuar”,** nënkupton regjistrimin, qarkullimin, shfrytëzimin, shumëfishimin, transportimin, transmetimin, arkivimin, asgjësimin dhe shkatërrimin e tij.
2. “**Akreditim i sigurisë**” është procesi i pranimit të riskut të mbetur, lidhur me vazhdimësinë e operimit të sistemit të komunikimit, informacionit dhe autorizimit të tij për të operuar për një kohë të përcaktuar.
3. **“Autoritet klasifikues”** në kuptim të këtij ligji, janë titullarët e institucioneve që në përmbushje të detyrave zyrtare, në mënyrë të drejtpërdrejtë apo me autorizim të Kryeministrit, fitojnë të drejtën për klasifikimin origjinal të informacionit.
4. **“Autoriteti Kombëtar për Sigurinë e Informacionit të Klasifikuar” (AKSIK)**, është autoriteti kompetent, përgjegjës për hartimin e politikave dhe standardeve të sigurisë për mbrojtjen e informacionit të klasifikuar dhe kontrollin e zbatimit të tyre.
5. **“Dokument i klasifikuar “sekret shtetëror”** është çdo dokument i regjistruar, pavarësisht formës fizike, ose karakteristikave, përfshirë dokumentin e shkruar të printuar, ose në formë elektronike, klasifikuar sipas legjislacionit në fuqi.
6. **“Drejtoria e Sigurisë të Informacionit të Klasifikuar”,** në vijim referuar DSIK, është Autoriteti Kombëtar për Sigurinë e Informacionit të Klasifikuar “sekret shtetëror” dhe në marrëdhënie me NATO, BE, shtete dhe organizata të tjera ndërkombëtare.
7. **“Certifikata e Sigurisë së Personelit** **(CSP)”** është dokumenti zyrtar i autoritetit përgjegjës për sigurinë e informacionit të klasifikuar ose i një autoriteti kompetent përgjegjës i sigurisë së një vendi tjetër, i cili vërteton nga pikëpamja e sigurisë se një individ i plotëson kushtet e përcaktuara për qasje në informacionin e klasifikuar.
8. **“Certifikata e Sigurisë Industriale (CSI)”** është dokumenti zyrtar i autoritetit kompetent për sigurinë e informacionit të klasifikuar, ose i një autoriteti kompetent përgjegjës i sigurisë së një vendi tjetër, i cili vërteton nga pikëpamja e sigurisë, se një operator ekonomik ka kapacitetet dhe aftësitë organizative, teknike e fizike dhe i plotëson standardet e përcaktuara për njohjen, ruajtjen dhe administrimin e informacionit të klasifikuar.
9. **“Deklasifikimi”** nënkupton ndryshimin e autorizuar të statusit të informacionit nga informacion i klasifikuar, në informacion të paklasifikuar.
10. **“Informacioni i klasifikuar “Sekret shtetëror”** është çdo dokument ose material, pavarësisht nga forma dhe natyra e tij, i përgatitur ose që përgatitet, të cilit i është vendosur një nivel i caktuar klasifikimi dhe afat ruajtjeje klasifikimi në pajtim me ligjislacionin në fuqi në interes të sigurisë kombëtare dhe mbrohet nga shkatërrimi, humbja, vjedhja, rrjedhja, përhapja e paautorizuar ose qasja nga çdo lloj tjetër kompromentimi sigurie.
11. **“Klasifikimi”** është procesi në përputhje me legjislacionin në fuqi përmes të cilit një informacion përcaktohet si i klasifikuar “sekret shtetëror”, duke i caktuar nivelin e klasifikimit dhe afatin e ruajtjes së këtij klasifikimi.
12. **“Material i klasifikuar “Sekret shtetëror””** përfshin dokumentet, makineritë, pajisjet, armatimet dhe komponentët e tyre të prodhuara, ose në proces prodhimi, klasifikuar sipas legjislacionit në fuqi.
13. **“Menaxhimi i riskut”**, nënkupton një qëndrim sistematik për të përcaktuar cilat masa të sigurisë janë të nevojshme për mbrojtjen e informacionit dhe mbështetjen e shërbimeve, burimeve, bazuar në vlerësimin e kërcënimit dhe dobësitë.
14. **“Nevojë për njohje”** është nevoja për të pasur qasje tek informacioni i klasifikuar gjatë ushtrimit të një funksioni të caktuar, me qëllim përmbushjen e një detyre zyrtare.
15. **"Siguria kombëtare"** do të thotë mbrojtja e pavarësisë, integritetit territorial, rendit kushtetues, jetës dhe mirëqenies së qytetarëve, pasurisë kombëtare dhe marrëdhënieve me jashtë të Republikës së Shqipërisë.
16. **“Shkelje e sigurisë”** së informacionit të klasifikuar është veprimi ose mosveprimi nga cilido që vepron në kundërshtim me rregullat e sigurisë së informacionit të klasifikuar.
17. **“Vlerësimi i rrezikut dhe kërcënimit të sigurisë”** nënkupton të gjithë procesin periodik të identifikimit, kontrollit dhe përcaktimit të masave për parandalimin, minimizimin apo eliminimin e rreziqeve apo kërcënimeve të sigurisë dhe ngjarjeve të paparashikuara, të pasigurta për informacionin e klasifikuar dhe identifikimin e zonave që kanë nevojë për mjete dhe masa mbrojtëse shtesë.
18. **“Zhvlerësim”** është procesi i ndryshimit të autorizuar të nivelit të klasifikimit të një informacioni të klasifikuar “Sekret shtetëror”, që për shkak të humbjes së disa vlerave fillestare të tij, i caktohet një nivel me i ulët klasifikimi dhe afat i ri i ruajtjes së klasifikimit.

**Neni 5**

**Objektivat e sigurisë**

1. Objektivat e sigurisë së informacionit të klasifikuar janë:
2. Konfidencialiteti, që nënkupton mbrojtjen e informacionit të klasifikuar nga aksesi i paautorizuar;
3. Integriteti, që nënkupton mbrojtjen e informacionit të klasifikuar nga modifikimi i paautorizuar;
4. Disponibiliteti, që nënkupton garantimin e aksesit të nevojshëm dhe përdorimit të informacionit të klasifikuar prej personave të autorizuar;

ç. Autenticiteti, që nënkupton garantimin që informacioni i klasifikuar është origjinal nga burim i besueshëm dhe i vërtetueshëm.

1. Pamohueshmëria duhet të sigurohet për entitetet që përpunojnë informacion të klasifikuar.

**Neni 6**

**Rregulla të përgjithshme**

1. Institucionet shtetërore dhe operatorët ekonomikë që kanë akses në informacionin e klasifikuar “Sekret shtetëror”, zbatojnë të gjitha masat për mbrojtjen e informacionit të klasifikuar, në përputhje me kërkesat e legjislacionit në fuqi.
2. E drejta e njohjes me informacionin e klasifikuar kufizohet vetëm tek ata persona që kanë nevojë për njohje dhe përmbushin kriteret e sigurisë.
3. Një institucion nuk ka të drejtë të zbulojë informacionin origjinal të klasifikuar nga një institucion tjetër pa autorizimin e këtij të fundit.
4. E drejta e informimit nuk refuzohet automatikisht kur informacioni i kërkuar është i klasifikuar.
5. Informacioni nuk publikohet kur është i klasifikuar “Sekret shtetëror”.
6. Çdo individ ka për detyrë që të mbrojë informacionin e klasifikuar sipas këtij ligji, pavarësisht nga mënyra se si ai ka arritur ta posedojë apo ta garantojë të drejtën e njohjes së këtij informacioni të klasifikuar.
7. Në çdo rast, kur një individ i ndërpret marrëdhëniet e punës apo çdo marrëdhënie tjetër kontraktuese, pavarësisht funksionit është i detyruar që të mos ekspozojë përmbajtjen e informacionit të klasifikuar që ai ka njohur gjatë ushtrimit të një detyre apo funksioni, në kuadrin e një institucioni shtetëror apo operatori ekonomik.

**Neni 7**

**Disiplinat për mbrojtjen e informacionit të klasifikuar**

1. Disiplinat për mbrojtjen e informacionit të klasifikuar janë:
2. Siguria e informacionit;
3. Siguria e personelit;
4. Siguria fizike;

ç. Siguria e sistemeve të komunikimit dhe informacionit;

1. Projekte të klasifikuara dhe siguria industriale.

**KREU II**

**SIGURIA E INFORMACIONIT**

**Neni 8**

**Kuptimi i sigurisë së informacionit të klasifikuar**

Me siguri të informacionit të klasifikuar kuptojmë tërësinë e procedurave dhe standardeve që garantojnë sigurinë e informacionit të klasifikuar gjatë procesit të krijimit, administrimit dhe mbikëqyrjes së tij.

**Neni 9**

**Nivelet e klasifikimit**

1. Informacion i klasifikuar “sekret shtetëror” në bazë të përmbajtjes, të vlerave dhe interesit shtetëror, klasifikohet në njërin nga katër nivelet e mëposhtme:
2. **"Tepër sekret",** kur ekspozimi i paautorizuar mund t'i shkaktojë dëme shumë të rënda sigurisë kombëtare;
3. **"Sekret"**, kur ekspozimi i paautorizuar mund t'i shkaktojë dëme serioze sigurisë kombëtare;
4. "**Konfidencial",** kur ekspozimi i paautorizuar mund t'i shkaktoje dëme sigurisë kombëtare;

ç. **“I kufizuar“,** kur ekspozimi i paautorizuar mund të dëmtojë veprimtarinë ose efektivitetin e institucioneve shtetërore në fushën e sigurisë kombëtare“.

1. Për përcaktimin e informacionit të klasifikuar nuk do të përdoret asnjë term tjetër.

**Neni 10**

**Kategoritë e klasifikimit**

1. Informacioni do t'i nënshtrohet procesit të klasifikimit sipas niveleve të përcaktuara në këtë ligj për kategoritë e mëposhtme, kur lidhet me sigurinë kombëtare:
2. Raporte, analiza, informacione, etj, të paraqitura në mbledhjet e Këshillit të Sigurimit Kombëtar dhe të Komisioneve të Kuvendit të Shqipërisë;
3. Raporte, analiza, informacione etj., në takimet dypalëshe ose shumëpalëshe me delegacionet e shteteve të huaja të strukturave shtetërore;
4. Veprimtaria e shërbimeve informative ku ekspozohen format dhe metodat e punës;

ç. Burimet e informacionit në shërbimet informative dhe në strukturat e tjera parandaluese, gjurmuese dhe zbuluese;

1. Dokumentacioni i krijuar nga strukturat shtetërore gjatë veprimtarisë informuese, parandaluese, gjurmuese dhe zbuluese;

dh. Plane ushtarake, programe, harta, planimetri dhe informacione të tjera ushtarake që përmbajnë të dhëna me rëndësi taktike, operative e strategjike;

1. Informacione për planet e mbrojtjes me rëndësi startegjike dhe kapacitetet e Forcave të Armatosura;

ë. Informacion që lidhet me ndërtimin, përbërjen, fortësinë, përdorimin e sistemeve, algoritmeve dhe materialeve kriptografike në të cilat trajtohet informacion i klasifikuar;

1. Vlerësimet strategjike të Forcave të Armatosura për kërcënimet, rreziqet dhe masat për përballimin e tyre;
2. Informacione për gatishmërinë luftarake, pajisjen, modernizimin, kompletimin me forca, mjete të Forcave të Armatosura;

gj. Çështjet kriptologjike, shkencore, teknologjike dhe ekonomike;

1. Informacionet lidhur me substancat e ndryshme kimike, biologjike, nukleare të rrezikshme për jetën dhe mjedisin;
2. Planimetritë, skemat dhe projektet për objektet e rëndësisë së veçantë;
3. Planet për sigurinë e personaliteteve të larta shtetërore të vendit dhe të huaja;
4. Programin për mbrojtjen e dëshmitarëve dhe të bashkëpunëtorëve të drejtësisë;
5. Veprimtarinë e përgjimit parandalues të telekomunikimeve;
6. Informacion që lidhet me gjendjen, kapacitetin, operimin, vlerësimin e sigurisë, kërcënimet, dobësitë, riskun, incidente sigurie të sistemeve/pajisjeve që trajtojnë informacion të klasifikuar.
7. Planet dhe skemat e sigurisë fizike të zonave të sigurisë për informacionin e klasifikuar;
8. Planet e evakuimit të informacionit të klasifikuar “Sekret shtetëror”, NATO, BE, shteteve dhe organizatave të tjera ndërkombëtare;

nj. Prokurimet në fushën e sigurisë dhe mbrojtjes që kanë lidhje me sigurinë e informacionit të klasifikuar “Sekret shtetëror”, NATO, BE, shteteve dhe organizatave të tjera ndërkombëtare, kontratat në funksion të tyre dhe dokumentacioni për kontratat e klasifikuara;

1. Regjistrat dhe librat për informacionin e klasifikuar “Sekret shtetëror” pas plotësimit të tyre.

**Neni 11**

**Ndalimi i klasifikimit**

1. Ndalohet klasifikimi i një informacioni kur ai bëhet me qëllim që:
2. të fshehë dhunimin e ligjeve, paefektshmërinë apo gabimet e administratës;
3. t’i privojë të drejtën e njohjes një personi, organizate apo instituconi;
4. të pengojë apo të vonojë dhënien e informacionit që nuk kërkon mbrojtje në interes të sigurisë kombëtare.

**Neni 12**

**Autoritete klasifikuese**

1. Autoritete klasifikuese të drejtpërdrejta në Republikën e Shqipërisë janë:
2. Presidenti i Republikës;
3. Kryeministri.
4. Titullarët e institucioneve të tjera e marrin këtë të drejtë me delegim nga Kryeministri.

**Neni 13**

**Propozimi i shtetasve**

1. Çdo shtetas shqiptar, kur çmon se një informacion i caktuar nën kontrollin e shtetit ose jashtë tij ka vlerat e nevojshme për t’u klasifikuar i propozon institucionit shtetëror përkatës klasifikimin e tij.
2. Ky institucion vendos brenda 10 ditëve nëse informacioni do të klasifikohet ose jo dhe njofton shtetasin për vendimin e marrë.

**Neni 14**

**Kohëzgjatja e klasifikimit**

1. Informacioni klasifikohet për aq kohë sa e kërkon interesi i sigurisë kombëtare.
2. Në klasifikimin origjinal, autoriteti klasifikues cakton afatin e ruajtjes sipas vlerave të informacionit.
3. Nëse autoriteti klasifikues nuk përcakton një afat më të shkurtër për deklasifikim, ky afat do të jetë 10 vjet nga data e klasifikimit origjinal.
4. Një autoritet klasifikues mund ta zgjasë kohëzgjatjen e klasifikimit ose të riklasifikojë një informacion për periudha të vazhdueshme që nuk i kalojnë 10 vjet, në përputhje me dispozitat e këtij ligji.

**Neni 15**

**Llogaritja e afatit**

1. Afati është periudha kohore gjatë të cilës një informacion i caktuar qëndron i klasifikuar.
2. Afati llogaritet si më poshtë:
   1. Kur informacioni është problemor, nga data e klasifikimit origjinal (fillestar);
   2. Kur ka si objekt ngjarje apo ndodhi, nga data e ngjarjes apo ndodhisë.

3. Informacioni i deklasifikuar konsiderohet i zakonshëm.

**Neni 16**

**Identifikimi i sekretit shtetëror**

1. Çdo sekret shtetëror në procesin e klasifikimit duhet të përmbajë:

a. njërin nga katër nivelet e klasifikimit;

b. identitetin dhe pozitën e autoritetit klasifikues;

c. institucionin apo zyrën e origjinës;

ç.udhëzimet e deklasifikimit nëse përcaktohen të tilla nga autoriteti klasifikues.

**Neni 17**

**Klasifikimi i parregullt**

1. Kur DSIK konstaton se një informacion është klasifikuar në kundërshtim me dispozitat e këtij ligji, kërkon nga institucioni që ka bërë klasifikimin të heqë dokumentin nga lista e informacioneve të klasifikuara, ose ndryshimin e nivelit të klasifikimit.

**Neni 18**

**Qarkullimi fizik i informacionit të klasifikuar**

1. Zyra e Informacionit të Klasifikuar krijohet me qëllim administrimin e informacionit të klasifikuar.
2. Zyra e Informacionit të Klasifikuar organizohet dhe vendoset në mjedise të përshtatshme në përputhje me masat që sigurojnë mbrojtje të informacionit të klasifikuar.
3. Të gjitha dokumentet dhe/ose materialet e klasifikuara hyrëse fizikisht ose elektronikisht merren në dorëzim dhe regjistrohen nga punonjësi i Zyrës së Informacionit të Klasifikuar.

**Neni 19**

**Shfrytëzimi, shumëfishimi, riprodhimi dhe përkthimi**

1. Shrytëzimi i informacionit të klasifikuar kryhet me qëllim ushtrimin e një detyre në bazë të parimit "nevojë për njohje", me miratim të titullarit dhe vetëm nga persona të certifikuar përshtatshmërisht.
2. Shumëfishimi i informacionit të klasifikuar kryhet vetëm në Zyrat e Informacionit të Klasifikuar, pas miratimit të titullarit të institucionit.
3. Përkthimi, riprodhimi, fragmentarizimi i një dokumenti dhe/ose i një materiali të klasifikuar, ruan klasifikimin e dokumentit origjinal dhe përmban të gjitha shenjëzimet e informacionit të klasifikuar.

**Neni 20**

**Transportimi i informacionit të klasifikuar**

1. Institucionet shtetërore të cilat administrojnë informacion të klasifikuar mund ta kryejnë vetë transportimin, por duke zbatuar rregullat e transportimit të informacionit të klasifikuar.
2. Institucionet shtetërore mund të hyjnë në marrëdhënie kontraktore me shërbimet postare për transportimin e objekteve dhe pakove postare të klasifikuara.

**Neni 21**

**Arkivimi i dokumentit të klasifikuar**

1. Informacioni i klasifikuar, qëndron për shfrytëzim në zyrat e informacionit të klasifikuar maksimumi deri në 10 vjet nga koha e krijimit, pavarësisht nga niveli i klasifikimit dhe afati i ruajtjes së këtij klasifikimi. Me miratim të titullarit të institucionit mund të qëndrojë edhe mbi afatin 10 vjeçar. Pas këtij afati dorëzohet në sistemin arkivor.

**Neni 22**

**Deklasifikimi**

1. Deklasifikimi i informacionit të klasifikuar është në dy lloje:
2. **“Deklasifikim i plotë”** është procesi i ndryshimit të autorizuar të statusit të një informacioni të klasifikuar “sekret shtetëror” në një informacion të paklasifikuar;
3. **“Deklasifikim i pjesshëm”** është procesi i ndryshimit të autorizuar të statusit të një pjese të informacionit të klasifikuar “sekret shtetëror” në informacion të paklasifikuar.
4. Informacioni mund të deklasifikohet me:
   1. ndodhinë e një ngjarjeje apo të një date të veçantë, siç përcaktohet nga autoriteti i klasifikimit origjinal;
   2. përfundimin e afatit kohor për klasifikim;
   3. kur publikimi i tij diktohet nga interesa më të rëndësishme shtetërore sesa nevoja për ta mbajtur atë të klasifikuar.
5. Informacioni i klasifikuar nuk deklasifikohet si rezultat i ekspozimit të paautorizuar të një informacioni identik apo të ngjashëm.
6. Çdo institucion shtetëror ka detyrimin të publikojë bibliografinë e informacionit të klasifikuar “sekret shtetëror”, të deklasifikuar plotësisht apo pjesërisht. Publikimi bëhet në “Fletoren zyrtare”, në faqen zyrtare të internetit të ministrisë apo të institucionit dhe me mënyra të tjera.
7. Autoriteti i klasifikimit origjinal është njëkohësisht edhe autoritet deklasifikues.

**Neni 23**

**Përjashtimet nga deklasifikimi**

* + 1. Një informacion mund të përjashtohet nga deklasifikimi kur ekspozimi i tij:

1. zbulon identitetin e burimit konfidencial, zbatimin e një metode apo të një burimi informativ;
2. nxjerr informacion që dobëson veprimtarinë e kriptologjisë;
3. nxjerr informacion që mund të dobësojë planet e ngutshme të sigurisë kombëtare;

ç. dëmton një traktat apo marrëveshje ndërkombëtare, marrëdheniet midis Republikës së Shqipërisë dhe shteteve të huaja apo veprimtarinë e mëtejshme diplomatike.

**Neni 24**

**Zhvlerësimi**

Kur informacioni i klasifikuar humbet disa vlera fillestare, ai mund të zhvlerësohet duke u klasifikuar e ruajtur në një nivel më të ulët.

**Neni 25**

**Rishikimi sistematik për deklasifikim**

1. Informacioni i përjashtuar nga deklasifikimi i nënshtrohet rishikimit sistematik të deklasifikimit.
2. Çdo institucion që zotëron informacion origjinal të klasifikuar, harton dhe zbaton një program për rishikimin sistematik të deklasifikimit për dokumente me vlera historike, të përjashtuara nga deklasifikimi.

**Neni 26**

**Asgjësimi dhe shkatërrimi**

1. Asgjësimi është procesi në përputhje me legjislacionin në fuqi, në të cilin për një informacion të klasifikuar “sekret shtetëror” vendoset asgjësimi i tij për shkak të humbjes së vlerave për ruajtje të mëtejshme dhe nuk është e nevojshme të deklasifikohet.
2. Shkatërrimiështë procesi në përputhje me legjislacionin në fuqi, i shkatërrimit fizik të një informacioni të klasifikur “sekret shtetëror”, i cili bëhet me mënyra dhe mjete që nuk lejojnë rindërtimin e plotë ose të pjesshëm të tij.

**KREU III**

**SIGURIA E PERSONELIT**

**Neni 27**

**Siguria e Personelit**

1. Siguria e personelit është tërësia e masave dhe procedurave, mbi bazën e të cilave vlerësohet nëse një person duke iu referuar besnikërisë, besueshmërisë dhe sigurisë së tij, mund të autorizohet për të patur akses tek informacioni i klasifikuar, pa e rrezikuar sigurinë e këtij informacioni.
2. Lëshimi, refuzimi, pezullimi i përkohshëm ose revokimi i “Certifikatës së Sigurisë së Personelit”, bëhet nga DSIK.
3. Kur ekspozohet informacioni i klasifikuar apo për shkak të një kushti të përcaktuar nga qeveria e një shteti tjetër, arsyet e refuzimit, pezullimit të përkohshëm apo revokimit të CSP nuk i bëhen me dije individit, institucionit kërkues apo operatorit ekonomik.
4. Procesi i verifikimit të sigurisë vijon edhe pas pajisjes së aplikantit me CSP. Kjo përfshin vlerësim të vazhdueshëm sigurie për çdo ndryshim në sjelljen e individit që e bën atë të cenueshëm nga pikëpamja e besnikërisë, besueshmërisë dhe e sigurisë së tij.

**Neni 28**

**Kriteret për njohjen e informacionit të klasifikuar**

1. Kanë të drejtë të njihen, të ruajnë, administrojnë e transferojnë informacion të klasifikuar vetëm personat, që:
2. sigurojnë të drejtën e njohjes për shkak të detyrës që kryejnë nga titullari i ministrisë/institucionit ose oficeri i sigurimit industrial i kontraktorit;
3. janë të brifuar më parë për njohjen e procedurave të sigurisë së informacionit të klasifikuar dhe të përgjegjësive individuale për shkeljet e sigurisë;
4. janë të pajisur me CSP, me përjashtim të rasteve për njohjen me informacionin e klasifikuar në nivelin “I kufizuar”.
5. Presidenti i Republikës së Shqipërisë dhe Kryeministri, janë të autorizuar që të kenë qasje tek informacioni i klasifikuar, për shkak të kryerjes së detyrave të tyre zyrtare e pajisen me CSP, pa iu nënshtruar procedurave të verifikimit të sigurisë.

**Neni 29**

**Listat e funksioneve për njohje me informacionin e klasifikuar**

1. Institucionet shtetërore miratojnë dhe dërgojnë në DSIK listën e funksioneve që për shkak të detyrave zyrtare njihen me informacionin e klasifikuar.
2. Rishikimi i këtyre listave bëhet periodikisht dhe në përputhje me ndryshimet e strukturës organizative të institucionit përkatës.

**Neni 30**

**Kriteret themelore të vlerësimit të sigurisë**

1. Kriteret themelore, mbi bazën e të cilave vlerësohet ekzistenca ose jo e rrezikut të sigurisë për informacionet e klasifikuara, që shërbejnë si bazë për të lëshuar, pezulluar, refuzuar pajisjen ose revokuar mbajtjen e mëtejshme të një CSP-je, janë rastet kur një individ rezulton se:
2. ka qenë, është ose tenton të angazhohet fshehurazi, vetëm në bashkëpunim apo në përbërje të një organizate të paligjshme, 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;
3. 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-s, BE-së, përveç rasteve kur këto bashkëpunime janë të autorizuara për shkak të detyrës;
4. 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;

ç. është apo ka qenë mbështetës i një organizate të përshkruar si në shkronjën “c”, të pikës 1, të këtij neni, është apo ka qenë i/e lidhur ngushtë me ndonjë anëtar të një organizate të tillë;

1. qëllimisht ka fshehur, ka keqprezantuar 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;

dh. rezulton i dënuar për një ose më shumë vepra penale;

1. ka një historik varësie nga alkooli, përdorimi i drogave të jashtëligjshme, apo keqpërdorimi i drogave të ligjshme;

ë. 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. me anë të veprimeve konkrete ka shprehur mungesë besnikërie, besueshmërie dhe sigurie;
2. ka kryer shkelje sigurie, ose 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;

gj. vuan nga çrregullime mendore kronike.

**Neni 31**

**Bashkëpunimi ndërinstitucional**

1. Gjatë procesit të verifikimit të sigurisë, DSIK bashkëpunon me institucionet e tjera në Republikën e Shqipërisë të cilat duhet të japin informacionet e kërkuara për verifikimin e sigurisë, duke iu përmbajtur afateve ligjore.

**Neni 32**

**Shkëmbimi i informacionit dhe bashkëpunimi ndërkombëtar për sigurinë e personelít**

1. DSIK ka të drejtë të bashkëpunojë dhe të shkëmbejë informacion sipas nevojës me autoritetet homologe të vendeve të tjera lidhur me kryerjen e procedurave për sigurinë e personelit.

**Neni 33**

**Trajtimi i të dhënave personale dhe i informacionit të klasifikuar**

1. Trajtimi i të dhënave personale dhe i informacionit të klasifikuar, të grumbulluara gjatë procesit të aplikimit dhe të verifikimit të sigurisë, për t’u pajisur me CSP, kryhet në përputhje me parashikimit e legjislacionit në fuqi.

**KREU IV**

**SIGURIA FIZIKE**

**Neni 34**

**Kuptimi i sigurisë fizike**

1. Siguria fizike është tërësia e masave fizike, teknike, elektronike dhe proceduriale për ruajtjen e zonave, ndërtesave, zyrave, dhomave dhe pajisjeve ku prodhohet, administrohet dhe shkatërrohet informacioni i klasifikuar.
2. Masat e sigurisë fizike shërbejnë për të siguruar një nivel proporcional të mbrojtjes fizike të informacionit të klasifikuar ndaj rrezikut të vlerësuar, në bazë të procesit të "Vlerësimit të rrezikut dhe kërcënimit të sigurisë".
3. Procesi i "Vlerësimit të rrezikut dhe kërcënimit të sigurisë" nënkupton të gjithë procesin periodik të identifikimit, kontrollit dhe minimizimit të rrezikut të sigurisë dhe ngjarjeve të pasigurta për informacionin e klasifikuar, i cili identifikon zonat që kanë nevojë për mjete dhe masa mbrojtëse.

**Neni 35**

**Zonat e sigurisë**

1. Zonat e sigurisë janë hapësirat ku prodhohet, regjistrohet, shfrytëzohet, transmetohet, ruhet, arkivohet dhe shkatërrohet informacion i klasifikuar.
2. Titullari i institucionit miraton me urdhër ndarjen e zonave të sigurisë, planin dhe skemën e sigurisë fizike të objektit ku mbahet dhe administrohet informacioni i klasfikuar.
3. Zonat e sigurisë ndahen në tre kategori:

a. zona e sigurisë e klasit të parë;

b. zona e sigurisë e klasit të dytë;

c. zona administrative.

1. Informacioni i klasifikuar “sekret shtetëror”, “konfidencial” e lart, prodhohet dhe administrohet në zonat e sigurisë së klasit të parë dhe të dytë.

**Neni 36**

**Zonë teknikisht e sigurt**

1. Zonë teknikisht e sigurt është zona në të cilën organizohen takime të klasifikuara dhe kërkon mbrojtje kundër sulmeve teknike dhe përgjimeve. Zona teknikisht e sigurt i nënshtrohet kontrolleve të rregullta fizike, teknike dhe hyrja në to duhet të ketë kontroll të rreptë.

**Neni 37**

**Mënyrat e sigurisë fizike**

1. Siguria teknike është tërësia e masave teknike që merren për të shmangur hyrjen me forcë ose të fshehtë të personave dhe të mjeteve të paautorizuara.
2. Sigurimi me roje përfshin ruajtjen e zonave të sigurisë gjatë dhe pas orarit zyrtar të punës.
3. Siguria elektronike është marrja e masave për vendosjen e pajisjeve, mjeteve dhe sistemeve të vëzhgimit, sinjalizimit e kontrollit, me qëllim parandalimin e ndërhyrjes nga persona të paautorizuar në zonat e sigurisë.
4. Institucionet shtetërore marrin masa për zbatimin e mënyrave të sigurisë fizike të informacionit të klasifikuar sipas akteve nënligjore në fuqi.

**Neni 38**

**Evakuimi i informacionit të klasifikuar**

1. Institucioni shtetëror merr masa për evakuimin e informacionit të klasifikuar në rastet e gjendjes së luftës, gjendjes së jashtëzakonshme, të fatkeqësive natyrore dhe të emergjencave të tjera civile, gjatë të cilave ky informacion mund të përvetësohet, dëmtohet, kompromentohet, shkatërrohet, etj.
2. Për informacionin e klasifikuar të NATO-s, BE-së, titullari i institucionit miraton planin e evakuimit të informacionit të klasifikuar në bashkëpunim me DSIK-në.

**KREU V**

**SISTEMET E KOMUNIKIMIT DHE INFORMACIONIT**

**Neni 39**

**Kuptimi i sigurisë në sistemet e komunikimit dhe informacionit**

1. Siguria e sistemeve të komunikimit dhe informacionit është aplikimi i masave të sigurisë për mbrojtjen e sistemeve të komunikimit dhe të informacionit, në vijim referuar si SKI, ku prodhohet, ruhet, përpunohet ose transmetohet informacioni i klasifikuar në përmbushje të objektivave të sigurisë, konfidencialitetit, integritetit, disponueshmërisë, autenticitetit dhe pamohueshmërisë.

**Neni 40**

**Akreditimi i sigurisë së SKI-së**

1. Informacioni i klasifikuar prodhohet, ruhet, transmetohet vetëm në sisteme të akredituara përshtatshmërisht.
2. Akreditimi i sigurisë përcakton nivelin e përshtatshëm të mbrojtjes, identifikon dhe pranon riskun e mbetur i cili duhet të monitorohet përgjatë jetëgjatësisë së sistemit.

**Neni 41**

**Lëshimi, refuzimi, revokimi dhe pezullimi i përkohshëm i Deklaratës së Akreditimit të Sigurisë**

1. Lëshimi, refuzimi, pezullimi i përkohshëm ose revokimi i Deklaratës së Akreditimit të Sigurisë (DAS) bëhet nga DSIK.
2. Njoftimi për vendimin e marrë nga DSIK për refuzimin, revokimin ose pezullimin e përkohshëm të DAS, i komunikohet me shkrim titullarit të institucionit përkatës, që ka iniciuar kërkesën për akreditimin e sigurisë së sistemit.

**Neni 42**

**Siguria e informacionit në SKI**

1. Pajisjet kompjuterike dhe SKI të akredituara identifikohen, ruhen dhe mbrohen përshtatshmërisht në përputhje me nivelin më të lartë të klasifikimit të informacionit që trajtohet në to.
2. Informacioni i klasifikuar që trajtohet në pajisje kompjuterike dhe SKI asgjësohet në përputhje me procedurat e miratuara nga DSIK.

**Neni 43**

**Kërkesat e sigurisë së SKI-së**

1. Institucionet shtetërore dhe operatorët ekonomikë/kontraktorët që për nevoja pune prodhojnë, ruajnë, përpunojnë, shpërndajnë ose transmetojnë informacion të klasifikuar “sekret shtetëror”, të NATO-s, BE-së, shteteve dhe/ose organizatave të huaja, me të cilat Republika e Shqipërisë ka marrëveshje sigurie nëpërmjet sistemeve të komunikimit dhe informacionit duhet t’i përmbahen kërkesave të sigurisë së SKI-së.

**Neni 44**

**Siguria e komunikimeve**

1. Gjatë transmetimit elektromagnetik të informacionit të klasifikuar implementohen masa të veçanta për përmbushjen e objektivave të sigurisë dhe mbrojtjen e transmetimeve nga detektimi, interceptimi dhe shfrytëzimi i paautorizuar, në përputhje me legjislacionin në fuqi.

**Neni 45**

**Siguria kriptografike**

1. Produktet dhe mekanizmat kriptografikë që përdoren për mbrojtjen e informacionit të klasifikuar gjatë transmetimit, përpunimit ose ruajtjes së këtij informacioni, akreditohen përshtatshmërisht nga DSIK.
2. Personeli që menaxhon materialet kriptografike autorizohet në mënyrë specifike për menaxhimin e tyre.
3. Procedurat për përzgjedhjen, operimin dhe mirëmbajtjen e materialeve kriptografike përcaktohen me vendim të Këshillit të Ministrave.
4. Procedurat për shpërndarjen dhe menaxhimin e materialeve kriptografike përcaktohen me vendim të Këshillit të Ministrave.

**Neni 46**

**Siguria e emetimeve**

1. Për mbrojtjen e informacionit të klasifikuar në nivel konfidencial e lart aplikohen masa sigurie nga emetimet elektromagnetike kompromentuese.
2. Procedurat për menaxhimin e sigurisë së emetimeve përcaktohen me vendim të Këshillit të Ministrave.

**Neni 47**

**Masat e sigurisë së SKI-së**

1. Masat e sigurisë janë mekanizmat dhe procedurat e menaxhimit të sigurisë me qëllim pengimin, parandalimin, detektimin, rezistimin dhe rikuperimin nga impaktet e incidenteve që prekin objektivat e sigurisë së informacionit të klasifikuar, përfshirë raportimin e incidenteve të sigurisë.

**Neni 48**

**Menaxhimi i riskut të sigurisë**

1. SKI-të që trajtojnë informacion të klasifikuar janë subjekt i procesit të menaxhimit të riskut të sigurisë, përfshirë vlerësimin e riskut të sigurisë, në përputhje me legjislacionin në fuqi.
2. Procesi i menaxhimit të riskut të sigurisë së sistemeve siguron vlerësimin e vazhdueshëm të kërcënimeve dhe dobësive të sistemeve.

**Neni 49**

**Autoritetet e sigurisë së SKI-së**

1. Për menaxhimin dhe garantimin e aspekteve të sigurisë së SKI-së, ngrihen dhe operojnë autoritetet e mëposhtme të sigurisë:
2. Autoriteti Kombëtar i Akreditimit të Sigurisë (AKAS) është DSIK, përgjegjëse për akreditimin e sigurisë së sistemeve kombëtare, si dhe sistemeve të NATO-s, BE-së dhe shteteve/organizatave të huaja që operojnë në institucionet shtetërore.
3. Autoriteti Kombëtar i Testimit dhe Vlerësimit të Sigurisë (AKTVS) është DSIK, përgjegjëse për testimin dhe vlerësimin e elementëve *hardëare,* *firmëare* dhe *softëare* të SKI-së për të cilët kërkohet testim dhe vlerësim i sigurisë.
4. Autoriteti Kombëtar i Sigurisë së Komunikimeve (AKSK) është DSIK, i cili është përgjegjës për:
5. Kontrollin e informacionit teknik kriptografik që lidhet me mbrojtjen e informacionit të klasifikuar;
6. Garantimin e përzgjedhjes, operimit dhe mirëmbajtjes së përshtatshme të sistemeve, produkteve dhe mekanizmave kriptografikë;
7. Garantimin e përzgjedhjes, operimit dhe mirëmbajtjes së përshtatshme të pajisjeve të sigurisë së SKI-së;
8. Trajtimin e çështjeve teknike dhe të sigurisë për aspektet e sigurisë së komunikimeve.

ç. Autoriteti Kombëtar i Shpërndarjes (AKSH) është Drejtoria e Shifrës, e cila   
 është përgjegjëse për menaxhimin e materialit kriptografik dhe garantimin e   
 ndjekjes së procedurave për mbajtjen në llogari, ruajtjen, shpërndarjen dhe   
 shkatërrimin e materialit kriptografik kombëtar, të NATO-s, BE-së dhe   
 shteteve dhe/ose organizatave të huaja.

d. Autoriteti Kombëtar TEMPEST (AKT) është Drejtoria e Shifrës, e cila është   
 përgjegjëse për sigurinë e emetimeve elektromagnetike të sistemeve.

dh.Autoriteti Kombëtar i Mbrojtjes Kibernetike (AKMK) është DSIK, e cila   
 harton dhe zhvillon konceptet, strategjinë, politikat dhe mbikëqyr zbatimin e   
 legjislacionit në fuqi për mbrojtjen kibernetike të sistemeve të klasifikuara.   
 AKMK në rast krize në SKI, përgjigjet në mënyrë të menjëhershme duke marrë   
 masa reaguese ndaj sulmeve kibernetike për minimizimin apo eliminimin e   
 riskut dhe tejkalimin e krizës.

**KREU VI**

**PROJEKTE TË KLASIFIKUARA DHE SIGURIA INDUSTRIALE**

**Neni 50**

**Kuptimi i sigurisë industriale**

1. Siguria industriale është aplikimi i sistemit të masave të sigurisë, procedurave dhe rregullave bazë, përmes të cilave realizohet parandalimi i përhapjes së paautorizuar, humbjes apo shkeljes së sigurisë së informacionit të klasifikuar, i cili trajtohet në kushtet e zbatimit të një projekti, programi, kontrate dhe nënkontrate në fushën e mbrojtjes dhe të sigurisë që përmban informacion të klasifikuar.

**Neni 51**

**Inicimi i procedurave të sigurisë**

1. Ministritë dhe institucionet shtetërore, të cilat gjatë veprimtarisë së tyre prodhojnë, administrojnë dhe qarkullojnë informacion të klasifikuar, kanë të drejtë të iniciojnë procedurat për kryerjen e një prokurimi në fushën e mbrojtjes dhe të sigurisë që përmban informacion të klasifikuar.
2. Çdo ministri apo institucion shtetëror, në cilësinë e autoritetit kontraktor ka përgjegjësi, që gjatë hartimit të dokumentacionit të tenderit apo zbatimit të kontratës në fushën e mbrojtjes dhe të sigurisë që përmban informacion të klasifikuar, të aplikojë sistemin e masave të sigurisë që garanton mbrojtjen e këtij informacioni, sipas kërkesave të përcaktuara në të gjitha disiplinat e sigurisë së informacionit të klasifikuar.
3. Operatorët ekonomikë të interesuar për të marrë pjesë në një prokurim në fushën e mbrojtjes dhe të sigurisë, i cili përmban informacion të klasifikuar, i nënshtrohen rregullave specifike të sigurisë.
4. Angazhimi i operatorëve ekonomikë, në një prokurim në fushën e mbrojtjes dhe të sigurisë që përmban informacion të klasifikuar në nivelin “Konfidencial” e lart, bëhet vetëm pasi më parë operatori ekonomik është i pajisur me nivelin e kërkuar të Certifikatës së Sigurisë Industriale (CSI).

**Neni 52**

**Certifikata e Sigurisë Industriale dhe verifikimi i sigurisë**

1. Pajisja e operatoreve ekonomikë me CSI kryhet nga autoriteti përgjegjës për sigurinë e informacionit të klasifikuar pas kryerjes së vlerësimit të rrezikut të papranueshëm të sigurisë.
2. Vlerësimi i rrezikut të papranueshëm të sigurisë kryhet duke iu referuar kritereve të qëndrueshmërisë ekonomike të operatorit ekonomik dhe të besueshmërisë së tij për qëllime të sigurisë së informacionit të klasifikuar.
3. Objekt i verifikimit të sigurisë për një operator ekonomik që kërkon të pajiset me CSI, është:
4. struktura e pronësisë dhe origjina e saj duke përfshirë filialet/degët;
5. partnerët e ngushtë vendas dhe të huaj;
6. qëndrueshmëria ekonomike e financiare;

ç. përmbushja e detyrimeve financiare ndaj institucioneve shtetërore dhe   
 të tretëve;

d. aftësia, kapacitetet teknike, fizike dhe ato për sigurinë e informacionit   
 të klasifikuar, referuar kërkesave të legjislacionit në fuqi;

dh. individi ose individët që zotërojnë pronësinë e operatorit ekonomik;

e. administratori dhe individët e tjerë që janë pjesë e stafit menaxherial   
 në momentin e aplikimit për pajisje me CSI;

ë. punonjësit që do të kenë akses tek informacioni i klasifikuar;

f. individët e propozuar nga administratori për detyrën e oficerit të   
 sigurisë industriale dhe të zëvendësit të tij;

g. shkalla e ndikimit të potencialit të mundshëm të influencës së   
 ushtruar për llogari të interesave të huaja.

**Neni 53**

**Vlefshmëria e CS-së dhe tipet e saj**

1. CSI-ja e lëshuar nga autoriteti përgjegjës për sigurinë e informacionit të klasifikuar është e vlefshme:
2. vetëm për akses tek informacioni i klasifikuar;
3. për akses, të drejtën e ruajtjes dhe të administrimit të informacionit të klasifikuar në mjediset e operatorit ekonomik;
4. për akses, të drejtën e ruajtjes dhe të administrimit të informacionit të klasifikuar, si dhe përdorimit të sistemeve të akredituara të komunikimit dhe të informacionit në mjediset e operatorit ekonomik.

2. CSI lëshohet në nivelin “konfidencial”, “sekret” dhe “tepër sekret” për informacionin e klasifikuar “sekret shtetëror”, të NATO-s dhe të BE-së.

3. Autoriteti kontraktor, verifikon vlefshmërinë dhe tipin e CSI-së tek autoriteti përgjegjës për sigurinë e informacionit të klasifikuar, përpara se operatori ekonomik i interesuar dhe personeli i tij të kenë akses tek informacioni i klasifikuar.

**Neni 54**

**Masat e sigurisë së informacionit**

**të klasifikuar gjatë tenderimit dhe zbatimit të kontratës/nënkontratës**

1. Autoriteti kontraktor dhe kontraktori marrin masa për sigurinë e informacionit të klasifikuar në procesin e tenderimit dhe të zbatimit të kontratës/nënkontratës në fushën e mbrojtjes dhe të sigurisë që përmban informacion të klasifikuar.
2. Autoriteti kontraktor dhe kontraktori zbatojnë standardet e sigurisë gjatë transportit të materialit të klasifikuar dhe kryerjes së vizitave ndërkombëtare.
3. Autoriteti përgjegjës për sigurinë e informacionit të klasifikuar, mbikëqyr zbatimin e masave të sigurisë gjatë procesit të tenderimit dhe zbatimit të kontratës/nënkontratës në fushën e mbrojtjes dhe të sigurisë që përmban informacion të klasifikuar, si dhe bashkëpunon me autoritetet homologe për projektet dhe sigurinë industriale.

**Neni 55**

**Ndikimi i influencës së huaj**

1. Pronësia e huaj si formë kontrolli apo influence, i referohet një situate kur individualisht një palë e tretë e huaj, individ, operator ekonomik apo qeveri, vlerësohet që posedon ndikim apo autoritet mbi një operator vendas, në një shkallë të tillë, ku pala e tretë mund të përfitojë akses tek informacioni i klasifikuar.
2. Vlerësimi i ndikimit dhe influencës së huaj, synon të identifikojë shkallën aktuale ose potencialin e influencës së mundshme të ushtruar për llogari të interesave të huaja, duke shfrytëzuar nivelet e pronësisë apo të shumicës së aksioneve që ato kanë në zotërim.

**KREU VII**

**SHKËMBIMI I INFORMACIONIT TË KLASIFIKUAR**

**Neni 56**

**Informacioni i huaj**

1. Institucionet shtetërore e ruajnë informacionin e klasifikuar të shteteve të huaja, apo organizatave ndërkombëtare, sipas standardeve që sigurojnë një shkallë mbrojtjeje të njejtë me atë që kërkohet nga shteti apo organizata ndërkombëtare.
2. Institucioni shtetëror para nënshkrimit të një marrëveshjeje, ose protokolli teknik që përfshin shkëmbimin e informacionit të klasifikuar, duhet të marrë më parë mendimin e DSIK-së.
3. Para nënshkrimit të një marrëveshjeje, apo protokolli teknik që përmban shkëmbimin e informacionit të klasifikuar, duhet të jetë lidhur më parë marrëveshja për sigurinë e informacionit të klasifikuar midis autoriteteve të sigurisë kombëtare të shteteve palë.
4. Përjashtohen nga ky detyrim, marreveshjet ose protokollet teknike urgjente të kërkuara nga palët, kur shkëmbimi i informacionit të klasifikuar ndikon drejtpërdrejtë në masat për sigurinë e stabilitetin e vendit dhe ka rëndësi të madhe për sigurinë kombëtare. Në këto raste, njoftohet DSIK.

**Neni 57**

**Informacioni i klasifikuar i NATO-s**

1. Republika e Shqiperisë mbron dhe siguron:
2. Informacionin e klasifikuar, i shënuar si i tillë, i cili vjen nga NATO;
3. Informacionet e klasifikuara, të shënuara si të tilla, të shteteve anëtare të dorëzuar Republikës së Shqipërisë, në mbështetje të një operacioni, programi, projekti ose kontrate të NATO-s.

**Neni 58**

**Siguria e informacionit të klasifikuar të NATO-s**

1. Republika e Shqipërisë bën çdo përpjekje për vendosjen e standardeve të sigurisë, në përputhje me nivelin e klasifikimit të informacionit të klasifikuar të ardhur nga NATO apo vendet anëtare të saj.
2. Republika e Shqipërisë siguron mospërdorimin e informacionit të klasifikuar të NATO-s për qëllime të ndryshme nga ato të përcaktuara në Traktatin e Atlantikut të Veriut, vendimet dhe rezolutat që kanë të bëjnë me këtë traktat.

**Neni 59**

**Informacioni i klasifikuar i BE-së**

1. Informacioni i klasifikuar i BE-së regjistrohet, shpërndahet, administrohet sipas standardeve që sigurojnë shkallë mbrojtjeje të njëjtë me atë që kërkohet nga BE, në zbatim të marrëveshjeve të përgjithshme të sigurisë.
2. Republika e Shqipërisë mbron dhe siguron:
3. Informacionin e klasifikuar, i shënuar si i tillë, i cili vjen nga BE;
4. Informacione të klasifikuara, të shënuara si të tilla, të shteteve anëtare dorëzuar Republikës së Shqipërisë, në mbështetje të një operacioni, programi, projekti ose kontrate të BE-së.

**Neni 60**

**Siguria e informacionit të klasifikuar të BE-së**

1. Republika e Shqipërisë bën çdo përpjekje për vendosjen e standardeve të sigurisë, në përputhje me nivelin e klasifikimit të informacionit të klasifikuar të ardhur nga BE apo vendet anëtare të saj
2. Republika e Shqipërisë siguron mospërdorimin e informacionit të klasifikuar të BE-së për qëllime të ndryshme nga ato të përcaktuara nga palët.

**Neni 61**

**Sistemi i regjistrit**

1. Sistemi i zyrave të regjistrit të informacionit të klasifikuar të NATO-s dhe BE-së përbëhet nga Zyra e Regjistrit Qendror pranë DSIK-së, zyrat e nënregjistrit të informacionit të klasifikuar të NATO-s, BE-së dhe pikat e kontrollit që krijohen në ministri dhe institucione shtetërore. Ky sistem është përgjegjës për regjistrimin, shpërndarjen dhe administrimin e informacionit të klasifikuar të shkëmbyer në kuadrin e bashkëpunimit me NATO-n dhe BE-në.
2. Institucionet shtetërore mbrojnë informacionin e klasifikuar të NATO-s dhe BE-së, sipas standardeve që sigurojnë shkallë mbrojtjeje të njëjtë me atë që kërkohet nga NATO dhe BE.

**KREU VIII**

**DREJTORIA E SIGURISË SË INFORMACIONIT TË KLASIFIKUAR**

**Neni 62**

**Misioni**

1. Misioni i Drejtorisë së Sigurimit të Informacionit të Klasifikuar është organizimi, drejtimi e kontrolli i masave për ruajtjen, klasifikimin dhe administrimin e informacionit të klasifikuar.

**Neni 63**

**Organizimi i DSIK-së**

1. DSIK është person juridik publik buxhetor në varësi të Kryeministrit.
2. DSIK ka buxhetin e saj, si zë më vete në buxhetin e shtetit.
3. DSIK ka emblemën dhe stemën e saj.
4. Struktura dhe organika e DSIK-së miratohet nga Kryeministri.
5. DSIK drejtohet nga drejtori i përgjithshëm, i cili emërohet me vendim të Këshillit të Ministrave, me propozim të Kryeministrit.
6. Rregullorja për organizimin dhe funksionimin e brendshëm të DSIK-së miratohet me urdhër të Kryeministrit.

**Neni 64**

**Detyrat e DSIK-së**

1. DSIK, në zbatim të misionit të saj, kryen dhe realizon këto detyra:
2. Përgatit projektaktet nënligjore për çështjet që lidhen me sigurinë e informacionit të klasifikuar;
3. Përcakton rregullat për elementët e sistemeve që administrojnë informacion të klasifikuar dhe bën rekomandime për përshtatshmërinë e tyre;
4. Mbikëqyr dhe inspekton rregullat e sigurisë për informacionin e klasifikuar;

ç. Monitoron proceset e sigurisë së informacionit të klasifikuar dhe lëshon rekomadime për vendosjen e praktikave të standardizuara;

1. Kryen certifikimin e personelit, i cili do të administrojë informacionin e klasifikuar;

dh.Kryen akreditimin e sigurisë së sistemit në të cilin prodhohet, administrohet, përpunohet dhe ruhet informacioni i klasifikuar;

1. Kryen certifikimin e operatorëve ekonomikë me CSI;

ë. Inspekton operatorët ekonomikë në lidhje me zbatimin e masave të sigurisë të informacionit të klasifikuar;

1. Rekomandon marrjen e masave për përmirësimin e punës në rastet e mangësive apo parregullsive në fushën e informacionit të klasifikuar;
2. Rekomandon marrjen e masave dhe vendos masa administrative individuale në rastet kur konstaton shkelje të rregullave të sigurisë së informacionit të klasifikuar;

gj. Shqyrton kërkesat për autoritet klasifikues nga institucione që nuk e kanë atë dhe nëse është e përshtatshme, ia propozon për miratim Kryeministrit;

1. Bashkëpunon me NATO-n, BE-në dhe me autoritetet kompetente të vendeve anëtare të këtyre organizatave për fushën të cilën mbulon;
2. Merr pjesë dhe përgatit projektmarrëveshtjet mbi sigurinë e informacionit të klasifikuar me shtete apo organizata të tjera ndërkombëtare;
3. Trajnon personelin që punon me informacion të klasifikuar.

**Neni 65**

**Kompetencat e Drejtorit të Përgjithshëm**

1. Drejtori i Përgjithshëm i DSIK-së, ka këto kompetenca:
   1. Drejton institucionin për realizimin e misionit dhe detyrave të ngarkuara;
   2. Përfaqëson institucionin në marrëdheniet me:
2. institucionet e tjera brenda vendit;
3. shtetet dhe organizatat e tjera ndërkombëtare;
   1. Nxjerr urdhëzime për zbatimin e akteve nënligjore për mbrojtjen e informacionit të klasifikuar;

ç. Inicion, negocion dhe nënshkruan marrëveshjet për sigurimin e   
 informacionit të klasifikuar me shtetet dhe organizatat ndërkombëtare;

* 1. Kërkon nga drejtuesit e institucioneve informacione në fushën e informacionit të klasifikuar dhe bashkëpunon për përmbushjen e përgjegjësive;

dh. Miraton inspektimet periodike për zbatimin e legjislacionit në fushën e   
 informacionit të klasifikuar nga institucionet shtetërore;

* 1. Miraton planin e dezinfektimit elektronik, i cili do të kryhet në institucionet shtetërore dhe operatorët ekonomikë;

ë. Miraton raportet e inspektimit për zbatimin e legjislacionit në fushën e   
 informacionit të klasifikuar nga institucionet shtetërore;

* 1. Lëshon, pezullon, revokon CSP, CSI, DAS;
  2. Miraton programin e trajnimit të institucioneve dhe operatorëve ekonomikë;

gj.Menaxhon veprimtarinë e institucionit, duke përfshirë organizimin,   
 personelin, veprimtarinë ekonomike/financiare të tij;

* 1. Informon periodikisht, por jo më pak se një herë në gjashtë muaj, Kryeministrin për çështjet në lidhje me informacionin e klasifikuar;
  2. Kryen detyra të tjera të përcaktuara nga ligji apo aktet nënligjore në zbatim të tij.

**Neni 66**

**Kriteret e emërimit të Drejtorit të Përgjithshëm**

1. Drejtor i Përgjithshëm i DSIK-së emërohet shtetasi shqiptar, i cili plotëson kriteret e mëposhtme:
2. ka përfunduar ciklin e dytë të studimeve universitare, dhe është i pajisjur me diplomë “Master i shkencave”;
3. të ketë përvojë pune jo më pak se 10 (dhjetë) vjet në çështje që lidhen me mbrojtjen dhe sigurinë kombëtare;
4. të ketë marrë një vlerësim të lartë për aftësitë e tij profesionale, etike dhe integritetin moral të tij, nëse u është nënshtruar vlerësimeve të mëparshme;

ç. të mos ketë punuar për një agjenci sigurie ose inteligjente të një shteti tjetër;

d. ndaj tij të mos ketë nisur një hetim penal ose të mos ketë qenë i dënuar me vendim gjyqësor të formës së prerë;

dh. ndaj tij të mos jetë marrë masa disiplinore e largimit nga puna, ose ndonjë masë tjetër disiplinore, e cila është ende në fuqi, sipas legjislacionit në fuqi, në momentin e aplikimit;

1. të plotësojë kriteret për t’u pajisur me certifikatë sigurie sipas legjislacionit në fuqi;

ë. nuk ka qenë anëtar, bashkëpunëtor ose i favorizuar nga ish-Sigurimi i Shtetit   
 para vitit 1990, sipas ligjit mbi të drejtën e informimit me dokumentet e Ish-  
 Shërbimit të Sigurimit të Republikës Popullore Socialiste të Shqipërisë.

**Neni 67**

**Rastet e lirimit dhe shkarkimit nga detyra**

1. Drejtor i Përgjithshëm i DSIK-së lirohet nga detyra, kur:
2. humbet shtetësinë shqiptare;
3. është dënuar me vendim të formës së prerë për kryerjen e një vepre penale;
4. kur plotësohet mosha për pension të plotë pleqërie;

ç. kur jep dorëheqjen nga detyra;

1. kur deklarohet i paaftë për punë nga komisioni përgjegjës mjekësor, sipas ligjit.
2. Drejtor i Përgjithshëm i DSIK-së shkarkohet nga detyra:
3. për shkelje të dispozitave të këtij ligji apo akteve të tjera ligjore;
4. nuk plotëson kushtet për pajisjen me CSP sipas legjislacionit në fuqi;
5. kur kryen veprimtari, që krijon konflikt interesash;

ç. kur zbulohen raste të papajtueshmërisë së funksionit të tij;

d. kur mungon në detyrë pa arsye për më shumë se 30 (tridhjetë) ditë rresht.

**Neni 68**

**Punonjësit e DSIK-së**

* + - 1. Punonjësit e DSIK-së janë nëpunës civilë dhe punonjës me kontratë.
      2. Për shkak të natyrës së veçantë të punës, punonjësi i DSIK-së trajtohet me shtesa mbi pagë. Masa e shtesës mbi pagë përcaktohet me vendim të Këshillit të Ministrave.
      3. Puonjësit e DSIK-së duhet të plotësojnë kushtet për pajisje me certifikatë sigurie personeli.

**KREU IX**

**MBIKËQYRJA SHTETËRORE**

**Neni 69**

**Mbikëqyrja shtetërore**

1. Mbikëqyrja shtetërore në fushën e mbrojtjes së informacionit të klasifikuar nënkupton mbikëqyrjen e institucioneve shtetërore, personelit, pajisjeve të përdorura prej tyre në lidhje me zbatueshmërinë e masave të sigurisë që burojnë nga dispozitat për sigurinë e informacionit të klasifikuar.

**Neni 70**

**Mbikëqyrja e masave të sigurisë**

1. Mbikëqyrja e masave të sigurisë bëhet nëpërmjet kryerjes së inspektimeve periodike apo rastësore në institucionet të cilat prodhojnë, administrojnë, ruajnë apo përpunojnë informacion të klasifikuar.
2. Inspektimet kryhen duke respektuar parimet e pavarësisë së inspektimit, proporcionalitetit në veprimtarinë e inspektimit, programimit të inspektimeve, si dhe parashikimeve të tjera në legjislacionin përkatës.
3. Në përfundim të inspektimit, DSIK i dërgon subjektit të inspektuar raportin përfundimtar të inspektimit me rekomandimet dhe masat administrative përkatëse, afatet, përmirësimin e mangësive dhe masat e marra ndaj personave që kanë shkelur rregullat e sigurisë.
4. Procedurat e inspektimeve kryhen në bazë të legjislacionit në fuqi.

**Neni 71**

**Mbikëqyrja dhe inspektimet e sigurisë**

1. DSIK është struktura përgjegjëse për kryerjen e mbikëqyrjes dhe inspektimeve periodike të sigurisë tek autoriteti kontraktor, institucioni përfitues, kontraktori dhe sipas rastit edhe tek nënkontraktori, gjatë realizimit të kontratave në fushën e mbrojtjes dhe të sigurisë, të cilat përmbajnë informacion të klasifikuar.

**Neni 72**

**Struktura dhe oficeri i sigurisë**

1. Institucionet shtetërore apo personat juridikë që prodhojnë, apo administrojnë informacion të klasifikuar, caktojnë strukturën e sigurisë ose oficerin e sigurisë, me qëllim mbikëqyrjen e zbatimit të masave në fushën e informacionit të klasifikuar.

**KREU X**

**SHKELJET E SIGURISË DHE MASAT ADMINISTRATIVE**

**Neni 73**

**Shkelje e sigurisë së informacionit** **të klasifikuar**

1. Shkelje e sigurisë së informacionit të klasifikuar është veprimi, ose mosveprimi nga cilido që vepron në kundërshtim me rregullat e sigurisë së informacionit të klasifikuar dhe që rezulton, ose jo në ekspozimin e pjesshëm apo tërësor tek një person i paautorizuar.
2. Kur shkelja e mësipërme nuk përbën vepër penale, përbën kundërvajtje administrative dhe dënohet sipas legjislacionit në fuqi.

**Neni 74**

**Procedurat e konstatimit të shkeljeve të sigurisë**

1. Të gjitha shkeljet e sigurisë për rastet e vjedhjes, marrjes, dhënies, humbjes, rrjedhjes, shkatërrimit të paautorizuar të informacionit të klasifikuar “sekret shtetëror”, duhet të raportohen menjëherë tek struktura ose oficeri i sigurisë i institucionit shtetëror dhe nëpërmjet tij tek titullari i këtij insitucioni dhe DSIK. Në këto raste titullari i institucionit me urdhër të veçantë krijon një komision për të shqyrtuar çështjen.

**Neni 75**

**Kundërvajtjet administrative dhe sanksionet**

1. Mosrespektimi i dispozitave të këtij ligji sjell përgjegjësi administrative sipas rasteve të parashikuara në pikën 3, të këtij neni.
2. Veprimet dhe mosveprimet, në përputhje me këtë ligj dhe për aq sa nuk përbëjnë vepër penale, konsiderohen kundërvajtje administrative.
3. Konsiderohen shkelje sigurie:
4. Humbja, dëmtimi, bërja publike, zbulimi apo dhënia e informacionit të klasifikuar “sekret shtetëror” personave të paautorizuar apo mediave vizive dhe audio;
5. Shkelja e detyrimit për të ruajtur konfidencialitetin e informacionit të klasifikuar;
6. Lejimi i aksesit në informacionin e klasifikuar për një person/operator ekonomik të paautorizuar dhe certifikuar përshtatshmërisht;

ç. Mosregjistrimi i informacionit të klasifikuar në regjistrin e duhur;

1. Mosplotësimi i saktë dhe mosrespektimi i rregullave për mirëmbajtjen dhe ruajtjen e regjistrave për informacionin e klasifikuar “sekret shtetëror”;

dh.Mospërdorimi i regjistrave që nuk janë prodhuar sipas modelit të miratuar nga DSIK;

1. Kopjimi, përkthimi, fragmentarizimi i informacionit të klasifikuar në kundërshtim me këtë ligj;

ë. Mosrespektimi i afateve për shfrytëzimin e informacionit të klasifikuar “sekret shtetëror”;

1. Transportimi ose mbajtja me vete e informacionit të klasifikuar në kundërshtim me këtë ligj;
2. Mosdërgimi pranë DSIK-së i bibliografisë së deklasifikimit të informacionit të klasifikuar;

gj. Moszbatimi i rregullave të përcaktuara në këtë ligj, lidhur me shkatërrimin e informacionit të klasifikuar “sekret shtetëror”;

1. Lejimi i hyrjes së personave të paautorizuar në ambientet e Zyrës së Informacionit të Klasifikuar (ZIK);
2. Mosmarrja e masave për mbylljen e informacionit të klasifikuar “sekret shtetëror” në dollapë metalikë apo kasaforta, mosmbyllja e dyerve dhe dritareve në përfundim të orarit zyrtar;
3. Mosraportimi i shkeljeve të sigurisë tek DSIK;
4. Mbajtja e pajisjeve dhe mjeteve të paautorizuara ose të pacertifikuara përshtatshmërisht në zonat e sigurisë;
5. Prodhimi dhe ruajtja e informacionit të klasifikuar “sekret shtetëror” në sisteme të pacertifikuara përshtatshmërisht më parë nga DSIK-ja;
6. Transmetimi i informacionit të klasifikuar në sisteme komunikimi të pacertifikuara përshtatshmërisht më parë nga DSIK-ja;
7. Mosvendosja e shenjëzimeve të përcaktuara në informacionin e prodhuar për llogari të “Sekret shtetëror”;
8. Moskryerja e inventarit periodik fizik të informacionit të klasifikuar “Sekret shtetëror” dhe mosnjoftimi në DSIK për rezultatin e inventarit;

nj. Mosdërgimi i kërkesës për akreditimin e pajisjeve apo sistemeve të komunikimit në të cilat trajtohet informacion i klasifikuar;

1. Pengimi i kryerjes së mbikëqyrjes;
2. Mosnxjerrja e akteve në fushën e informacionit të klasifikuar;
3. Moszbatimi i rekomandimeve të lëna nga inspektimi i kryer nga DSIK;
4. Mosraportimi i shkeljeve të sigurisë kur individi vihet në dijeni;
5. Moszbatimi i masave të parashikuara në Instruksionin e Sigurisë së Projektit, në kuadrin e zbatimit të kontratës në fushën e mbrojtjes dhe të sigurisë që përmban informacion të klasifikuar;
6. Mosrespektimi i standardeve të sigurisë sipas planit të miratuar në kuadrin e transportit të materialit të klasifikuar;
7. Moskryerja e verifikimit paraprak;
8. Moskryerja e brifimeve dhe debrifimeve të sigurisë.
9. Shkelje të rënda sigurie konsiderohen shkeljet e parashikuara në shkronjat“a”, “b”, “c”, “ç”, “e”, “f”, “gj”, “j”, “l”, “ll”, “m”, “o”, “p”, “q”, “r”, “s”, “t”, “u” të pikës 3, të këtij neni.
10. Shkeljet e rënda dënohen me gjobë nga 100 000 (njëqind mijë) - 200 000 (dyqind mijë) lekë, në përputhje me parashikimet e legjislacionit në fuqi për kundërvajtjet administrative.
11. Shkelje të lehta sigurie konsiderohen shkeljet e parashikuara në shkronjat “d”, “dh”, “ë”, “g”, “h”, “i”, “k”, “n”, “v”, të pikës 3, të këtij neni.
12. Shkeljet e lehta dënohen me gjobë nga 15 000 (pesëmbëdhjetë mijë) - 30 000 (tridhjetë mijë) lekë, në përputhje me parashikimet e legjislacionit në fuqi për kundërvajtjet administrative.
13. Gjobat e vendosura kundër subjekteve që shkelin dispozitat e këtij ligji, sipas përcaktimeve të pikave sipas pikës 5 dhe 7, tëtë këtij neni, arkëtohen në buxhetin e shtetit.

**Neni 76**

**Përgjegjësia administrative**

* + - 1. Titullari i autoritetit publik mban përgjegjësi ligjore dhe administrative për shkeljet ligjore të parashikuara në shkronjat “g”, “gj”, “j”, “nj”, “o”, “p”, “q”, “s”, “t”, “u”, të pikës 3, të nenit 73, të këtij ligji.
      2. Personi përgjegjës i cili kryen shkeljen, mban përgjegjësi ligjore dhe administrative për shkeljet ligjore të parashikuara në shkronjat “a”, “b”, “c”, “e”, “ë”, “gj”, “i”, “k”, “l”, “ll”, “m”, “t”, të pikës 3, të nenit 73, të këtij ligji.
      3. Struktura e sigurisë mban përgjegjësi ligjore dhe administrative për shkeljet ligjore të parashikuara në shkronjat “c”, “gj”, “k”, “l”, “ll”, të pikës 3, të nenit 73, të këtij ligji.
      4. Punonjësi i Zyrës së Informacionit të Klasifikuar mban përgjegjësi ligjore dhe administrative për shkeljet ligjore të parashikuara në shkronjat “ç”, “d”, “dh”, “h”, “n”, “u”, “v” të pikës 3, të nenit 73, të këtij ligji.

**Neni 77**

**Mënyra e shlyerjes së masës së dënimit me gjobë**

1. Masa e dënimit e përcaktuar me gjobë, shlyhet me këste mujore.
2. Këstet mujore caktohen në një masë të tillë që nëpunësit dhe familjes së tij t’i garantohet jetesa, të paktën në nivelin e pagës minimale, të miratuar me vendim të Këshillit të Ministrave.

**Neni 78**

**Ankimi i sanksioneve administrative**

1. Personi ndaj të cilit është vendosur sanksioni administrativ, sipas dispozitave të këtij ligji, ka të drejtë të bëjë ankim në gjykatën kompetente, sipas legjislacionit në fuqi.

**KREU XI**

**DISPOZITAT E FUNDIT**

**Neni 79**

**Aktet nënligjore**

1. Ngarkohet Këshilli i Ministrave të nxjerrë aktet nënligjore për zbatimin e këtij ligji, brenda 1 viti nga data e hyrjes në fuqi të tij.
2. Krijimi, klasifikimi, regjistrimi, qarkullimi, shfrytëzimi, shumëfishimi, arkivimi, sigurimi fizik, transportimi fizik, deklasifikimi, zhvlerësimi, asgjësimi dhe shkatërrimi i informacionit të klasifikuar përcaktohen me vendim të Këshillit të Ministrave.
3. Procedurat dhe përgjegjësitë e institucioneve për verifikimin e sigurisë dhe lëshimin, refuzimin, pezullimin e përkohshëm ose revokimin e “Certifikatës së Sigurisë së Personelit” përcaktohen me vendim të Këshillit të Ministrave.
4. Rregullat, procedurat dhe kërkesat për mbrojtjen e informacionit të klasifikuar gjatë prokurimit në fushën e mbrojtjes dhe të sigurisë përcaktohen me vendim të Këshillit të Ministrave.
5. Aktet nënligjore të miratuara para datës së hyrjes në fuqi të këtij ligji, që nuk bien në kundërshtim me këtë ligj, do të zbatohen deri në miratimin e akteve nënligjore në zbatim të këtij ligji.

**Neni 80**

**Shfuqizime**

Ligji nr.8457, datë 11.02.1999, “Për informacionin e klasifikuar “Sekret shtetëror”, i ndryshuar, shfuqizohet.

**Neni 81**

**Hyrja në fuqi**

Ky ligj hyn në fuqi 15 ditë pas botimit në “Fletoren zyrtare”.

**K R Y E T A R I**

**LINDITA NIKOLLA**

1. *Ky projektligj është përafruar pjesërisht me:*

   *Vendimin e Këshillit të datës 23 shtator 2013 “Mbi rregullat e sigurisë për mbrojtjen e informacionit të klasifikuar të BE” (2013/488 / BE). NR. CELEX 32013D0488, “Fletore zyrtare” e Bashkimit Evropian seria L, nr.274, datë15.12.2013, faqe 1-50.* [↑](#footnote-ref-1)