

LIGJ
Nr. 10/2023

PËR INFORMACIONIN E KLASIFIKUAR¹

Në mbështetje të neneve 78 dhe 81, pika 1, të Kushtetutës, me propozimin e Këshillit të Ministrave,

KUVENDI
I REPUBLIKËS SË SHQIPËRISË

VENDOSI:

KREU I
DISPOZITA TË PËRGJITHSHME

Neni 1
Objekti

Objekti i këtij ligji është përcaktimi i parimeve bazë dhe i rregullave për krijimin, administrimin, deklasifikimin, zhvlerësimin 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, komprometimi ose ekspozimi i paautorizuar.

Neni 3
Fusha e veprimit

Ky ligj zbatohet nga institucionet e administratës publike dhe operatorët ekonomikë për të cilët për ushtrimin e detyrave të tyre dhe bazuar në parimin “nevojë për njohje” kërkohet të kenë qasje në informacionin e klasifikuar.

SKI-të sipas këtij ligji nuk përjashtohen nga detyrimet që rrjedhin nga fusha e veprimit të legjislacionit në fuqi që rregullon sigurinë kibernetike në Republikën e Shqipërisë, si pjesë e infrastrukturave kritike dhe të rëndësishme të informacionit.

Neni 4
Përkufizime

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

1. “Administrim i informacionit të klasifikuar” është regjistrimi, qarkullimi, shfrytëzimi, shumëfishimi, transportimi, transmetimi, ruajtja, arkivimi, asgjësimi dhe shkatërrimi i tij.
2. “Administratë publike” në kuptim të këtij ligji përfshin aparatën e Këshillit të Ministrave, ministritë, institucionet qendrore në varësi të Kryeministrit apo ministrave, përfshirë degët e tyre

¹ Ky projektligj është përafshuar pjesërisht me:

Vendimin e Këshillit të datës 23 shtator 2013 “Mbi rregullat e sigurisë për mbrojtjen e informacionit të klasifikuar të BE-së” (2013/488 / BE). Nr. CELEX 32013D0488, Fletore Zyrtare e Bashkimit Evropian seria L, nr. 274, datë 15.12.2013, faqe 1-50.

territoriale, administratën e prefektit, institucionet e pavarura, gjykatat, prokuroritë e çdo juridiksioni, Byronë Kombëtare të Hetimit, si dhe organet e qeverisjes së sistemit të drejtësisë.

3. “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.

4. “Autoritet klasifikues” janë titullarët e institucioneve, që në përmbushje të detyrave zyrtare, në mënyrë të drejtpërdrejtë apo me autorizim të Kryeministrit, fitojnë të drejtën për klasifikimin e informacionit.

5. “Autoriteti Kombëtar për Sigurinë e Informacionit të Klasifikuar” (AKSIK) është autoriteti përgjegjës për hartimin dhe kontrollin e zbatimit të politikave dhe standardeve të sigurisë për mbrojtjen e informacionit të klasifikuar “sekret shtetëror” të NATO-s, të BE-së, shteteve dhe organizatave të tjera ndërkombëtare.

6. “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 këtij ligji.

7. “Certifikata e sigurisë së personelit (CSP)” është dokumenti zyrtar i autoritetit shqiptar 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 njohjen, ruajtjen, administrimin dhe transferimin e informacionit të klasifikuar.

8. “Certifikata e sigurisë industriale (CSI)” është dokumenti zyrtar i autoritetit shqiptar 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 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 në një projekt/program apo kontratë/nënkontratë, që përmban informacion të klasifikuar.

9. “Deklarata e akreditimit të sigurisë (DAS)” është dokumenti zyrtar lëshuar nga AKSIK-u, që autorizon një SKI të ruajë, të përpunojë, të transmetojë informacion të klasifikuar në një mjedis të caktuar operacional.

10. “Deklasifikimi” është heqja e çdo klasifikimi të sigurisë.

11. “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 përputhje me këtë ligj, në interes të sigurisë kombëtare dhe mbrohet nga shkatërrimi, humbja, vjedhja, rrjedhja, përhapja e paautorizuar ose qasja nga çdolloj tjetër komprometimi sigurie.

12. “Klasifikimi” është procesi përmes të cilit një informacion përcaktohet si i klasifikuar “sekret shtetëror”, duke i caktuar nivelin e klasifikimit dhe afatin e ruajtjes së këtij klasifikimi në përputhje me këtë ligj.

13. “Kriptologji” është shkenca e studimit të kriptografisë dhe kript analizës.

14. “Material i klasifikuar ‘Sekret shtetëror’” përfshin dokumentet, makineritë, pajisjet, armatimet dhe komponentët e tyre të prodhuara ose në proces prodhimi, klasifikuar sipas këtij ligji.

15. “Menaxhimi i riskut” është një qëndrim sistematik për të përcaktuar se cilat masa të sigurisë janë të nevojshme për mbrojtjen e informacionit dhe mbështetjen e shërbimeve, burimeve, bazuar në vlerësimin e kërcënimit dhe dobësitë.

16. “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.

17. “Operator ekonomik” ka të njëjtin kuptim sipas përkufizimit të bërë në ligjin për prokurimet në fushën e mbrojtjes dhe të sigurisë.

18. “Siguria kombëtare” është mbrojtja e pavarësisë, integritetit territorial, rendit kushtetues, jetës dhe mirëqenies së qytetarëve, pasurisë kombëtare dhe marrëdhënieve me jashtë të Republikës së Shqipërisë.

19. “Sistemet e Komunikimit dhe Informacionit” (SKI) janë sistemet që trajtojnë ose do të trajtojnë informacion të klasifikuar “sekret shtetëror”, të NATO-s, BE-së, shteteve dhe/ose organizatave të tjera ndërkombëtare me të cilat Republika e Shqipërisë ka marrëveshje sigurie.

20. “Shkelje e sigurisë së informacionit të klasifikuar” është veprimi ose mosveprimi nga cildo që vepron në kundërshtim me rregullat e sigurisë së informacionit të klasifikuar.

21. “Vlerësimi i rrezikut dhe kërcënimit të sigurisë” është i gjithë procesi periodik i 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.

22. “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 më i ulët klasifikimi dhe afat i ri i ruajtjes së klasifikimit.

Neni 5

Parimet e sigurisë së informacionit të klasifikuar

Parimet e sigurisë së informacionit të klasifikuar janë:

- a) konfidencialiteti që nënkupton mbrojtjen e informacionit të klasifikuar nga qasja e paautorizuar;
- b) integriteti që nënkupton mbrojtjen e informacionit të klasifikuar nga modifikimi i paautorizuar;
- c) disponibiliteti që nënkupton garantimin e qasjes së nevojshme 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;
- d) pamohueshmëria që nënkupton sigurinë, që dërguesi dhe marrësi nuk mohojnë procesin e shkëmbimit të informacionit.

Neni 6

Rregulla të përgjithshme

1. Institucionet e administratës publike dhe operatorët ekonomikë, që kanë qasje në informacionin e klasifikuar “sekret shtetëror”, zbatojnë të gjitha masat për mbrojtjen e informacionit të klasifikuar në përputhje me kërkesat e këtij ligji.

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, referuar pikës 5 të nenit 17 të ligjit nr. 119/2014 “Për të drejtën e informimit”.

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, apo dhe për shkak të tyre në kuadrin e një institucioni të administratës publike apo operatori ekonomik.

Neni 7

Disiplinat për mbrojtjen e informacionit të klasifikuar

Disiplinat për mbrojtjen e informacionit të klasifikuar janë:

- a) siguria e informacionit;
- b) siguria e personelit;
- c) siguria fizike;
- ç) siguria e sistemeve të komunikimit dhe informacionit;
- d) 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

Informacioni i klasifikuar “sekret shtetëror”, në bazë të përmbajtjes, të vlerave dhe interesit shtetëror, klasifikohet në njërin nga katër nivelet e mëposhtme:

- a) “Tepër sekret”, kur ekspozimi i paautorizuar mund t’i shkaktojë dëme jashtëzakonisht të rënda sigurisë kombëtare;
- b) “Sekret”, kur ekspozimi i paautorizuar mund t’i shkaktojë dëme serioze sigurisë kombëtare;
- c) “Konfidencial”, kur ekspozimi i paautorizuar mund t’i shkaktojë dëme sigurisë kombëtare;
- ç) “I kufizuar”, kur ekspozimi i paautorizuar mund të dëmtojë veprimtarinë ose efektivitetin e institucioneve të administratës publike në fushën e sigurisë kombëtare.

Neni 10

Kategoritë e klasifikimit

Informacioni i nënshtrohet procesit të klasifikimit sipas niveleve të përcaktuara në këtë ligj për kategoritë e mëposhtme, kur lidhet me sigurinë kombëtare:

- a) raporte, analiza, informacione të paraqitura në mbledhjet e Këshillit të Sigurimit Kombëtar dhe të komisioneve të Kuvendit të Shqipërisë;
- b) raporte, analiza, informacione, që shkëmbehen apo ndahen në takime dypalëshe ose shumëpalëshe me delegacionet e shteteve/organizatave të huaja dhe me strukturat shtetërore;
- c) 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;
- d) 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;
- e) informacione për planet e mbrojtjes me rëndësi strategjike 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;
- f) vlerësimet strategjike të Forcave të Armatosura për kërcënimet, rreziqet dhe masat për përballimin e tyre;
- g) informacione për gatishmërinë luftarake, pajisjen, modernizimin, kompletimin me forca, mjete të Forcave të Armatosura;
- gj) çështjet kriptologjike, shkencore, teknologjike dhe ekonomike;
- h) informacionet lidhur me substancat e ndryshme kimike, biologjike, nukleare të rrezikshme për jetën dhe mjedisin;
- i) planimetritë, skemat dhe projektet për objektet e rëndësisë së veçantë;
- j) planet për sigurinë e personaliteteve të larta shtetërore të vendit dhe të huaja;
- k) programi për mbrojtjen e dëshmitarëve dhe të bashkëpunëtorëve të drejtësisë;
- l) veprimtaria e përgjimit parandalues të komunikimeve elektronike;
- ll) informacioni që lidhet me gjendjen, kapacitetin, operimin, vlerësimin e sigurisë, kërcënimet, dobësitë, riskun, incidente sigurie të sistemeve/pajisjeve që trajtojnë informacion të klasifikuar;
- m) planet dhe skemat e sigurisë fizike të zonave të sigurisë për informacionin e klasifikuar;
- n) planet e evakuimit të informacionit të klasifikuar “sekret shtetëror”, të NATO-s, BE-së, të shteteve dhe organizatave të tjera ndërkombëtare;
- nj) dokumentet që përmbajnë informacion të klasifikuar në prokurimet në fushën e mbrojtjes dhe sigurisë;
- o) regjistrat dhe librat për informacionin e klasifikuar “sekret shtetëror” pas plotësimit të tyre.

Neni 11

Ndalimi i klasifikimit

Ndalohet klasifikimi i një informacioni kur ai bëhet me qëllim që:

- a) të fshehë moszbatimin e ligjeve, paefekshmërinë apo gabimet e administratës publike;
- b) t'i privojë të drejtën e njohjes një individi, personi fizik a juridik, publik a privat;
- c) të pengojë apo të vonojë dhënien e informacionit që nuk kërkon mbrojtje në interes të sigurisë kombëtare.

Neni 12

Autoritetet klasifikuese

1. Autoritete klasifikuese të drejtpërdrejta në Republikën e Shqipërisë janë:

- a) Presidenti i Republikës;
 - b) Kryeministri.
2. Titullarët e institucioneve të tjera e marrin këtë të drejtë me autorizim 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 përkatës të administratës publike klasifikimin e tij.

2. Ky institucion vendos brenda 10 (dhjetë) 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. Autoriteti klasifikues cakton afatin e ruajtjes së klasifikimit të informacionit sipas vlerave të tij.
3. Një autoritet klasifikues mund ta zgjasë kohëzgjatjen e klasifikimit ose të riklasifikojë një informacion për periudha të vazhdueshme, që nuk i kalojnë 10 (dhjetë) vjet, në përputhje me dispozitat e këtij ligji.
4. Rregullat për klasifikimin “sekret shtetëror” të informacionit përcaktohen në rregulloren, që miratohet me vendim të Këshillit të Ministrave.

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:
 - a) kur informacioni është problemor, nga data e klasifikimit;
 - b) 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

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

Kur AKSIK-ja 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 të ndryshojë nivelin e klasifikimit.

Neni 18

Njësia organizative përgjegjëse për informacionin e klasifikuar

1. Njësia organizative përgjegjëse për informacionin e klasifikuar përgjigjet për marrjen, dërgimin, regjistrimin, shpërndarjen, shumëfishimin, ruajtjen dhe arkivimin e informacionit të klasifikuar.
2. Funkcionet e njësisë organizative përgjegjëse për informacionin e klasifikuar, me qëllim administrimin e tij, kryhen nga struktura/strukturat përgjegjëse për protokoll-arkivin, kartotekën në institucionet e administratës publike që administrojnë informacion të klasifikuar.
3. Njësia organizative përgjegjëse për informacionin e klasifikuar organizohet dhe vendoset në mjedise të përshtatshme në përputhje me masat që sigurojnë mbrojtjen e informacionit të klasifikuar, duke zbatuar standardet e sigurisë.
4. Rregullat e detajuara për funksionimin e njësisë organizative përgjegjëse për informacionin e klasifikuar dhe punën me informacionin e klasifikuar përcaktohen në rregulloren që miratohet me vendim të Këshillit të Ministrave.

Neni 19

Regjistrimi, shfrytëzimi, shumëfishimi, riprodhimi dhe përkthimi

1. Shfrytëzimi i informacionit të klasifikuar kryhet me qëllim ushtrimin e një detyre, në bazë të parimit “nevojë për njohje”, me miratim të titullarit të institucionit përkatës dhe vetëm nga persona të certifikuar përshtatshëm.

2. Shumëfishimi i informacionit të klasifikuar kryhet vetëm në njësitë organizative përgjegjëse për informacionin e klasifikuar, pas miratimit të titullarit të institucionit.

3. Përkthimi, riprodhimi, fragmentarizimi i një dokumenti ose i një materiali të klasifikuar, ruan klasifikimin e dokumentit origjinal dhe përmban të gjitha shenjëzimet e informacionit të klasifikuar.

4. Në rastet e sekuestrimit të informacionit të klasifikuar nga organi procedues, në përputhje me dispozitat e Kodit të Procedurës Penale, organi procedues zbaton dispozitat e këtij ligji për regjistrimin, shfrytëzimin, administrimin dhe ruajtjen e informacionit të klasifikuar.

5. Rregullat për regjistrimin, shfrytëzimin, shumëfishimin, riprodhimin dhe përkthimin e informacionit të klasifikuar “sekret shtetëror” përcaktohen në rregulloren që miratohet me vendim të Këshillit të Ministrave.

Neni 20

Transportimi fizik i informacionit të klasifikuar

1. Institucionet e administratës publike, të cilat administrojnë informacion të klasifikuar, mund ta kryejnë vetë transportimin, por duke zbatuar rregullat e transportimit të informacionit të klasifikuar.

2. Institucionet e administratës publike mund të hyjnë në marrëdhënie kontraktore me shërbimet postare për transportimin e objekteve dhe pakove postare të klasifikuara.

3. Rregullat e detajuara për transportimin fizik të informacionit të klasifikuar përcaktohen në rregulloren që miratohet me vendim të Këshillit të Ministrave.

Neni 21

Arkivimi i informacionit të klasifikuar

Informacioni i klasifikuar qëndron për shfrytëzim në njësitë organizative përgjegjëse për informacionin e klasifikuar maksimumi deri në 10 (dhjetë) 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 (dhjetë) vjeçar. Pas këtij afati dorëzohet në sistemin arkivor.

Neni 22

Deklasifikimi

1. Deklasifikimi i informacionit të klasifikuar është në dy lloje:

a) “Deklasifikim i plotë”, procesi i ndryshimit të autorizuar të statusit të një informacioni të klasifikuar “sekret shtetëror” në një informacion të paklasifikuar;

b) “Deklasifikim i pjesshëm”, procesi i ndryshimit të autorizuar të statusit të një pjese të informacionit të klasifikuar “sekret shtetëror” në informacion të paklasifikuar.

2. Informacioni mund të deklasifikohet:

a) me ndodhinë e një ngjarjeje apo të një date të veçantë, siç përcaktohet nga autoriteti i klasifikimit të informacionit;

b) me përfundimin e afatit kohor për klasifikim;

c) kur publikimi i tij diktohet nga interesa më të rëndësishme shtetërore, sesa nevoja për ta mbajtur atë të klasifikuar;

ç) me kërkesë të gjykatës, kur informacioni i klasifikuar është sekuestruar nga organi procedues në përputhje me Kodin e Procedurës Penale.

3. Informacioni i klasifikuar nuk deklasifikohet si rezultat i ekspozimit të paautorizuar të një informacioni identik apo të ngjashëm.

4. Përjashtimisht, konsiderohen të deklasifikuara dokumentet e ish-Sigurimit të Shtetit të Ministrisë së Punëve të Brendshme të Republikës Popullore Socialiste të Shqipërisë për periudhën 29 nëntor 1944 deri në ditën e krijimit të Shërbimit Informativ Kombëtar, 2 korrik 1991, të cilat disponohen nga të gjitha arkivat e rrjetit arkivor të Republikës së Shqipërisë. Nga zbatimi i kësaj dispozite, përjashtohen dokumentet e ish-Sigurimit të Shtetit që lidhen me marrëdhëniet ndërmjet shteteve dhe sigurinë kombëtare.

5. Çdo institucion i administratës publike 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 të përshtatshme.

6. Autoriteti i klasifikimit është njëkohësisht edhe autoritet deklasifikues.

7. Rregullat për deklasifikimin e informacionit të klasifikuar “sekret shtetëror” përcaktohen në rregulloren që miratohet me vendim të Këshillit të Ministrave.

Neni 23

Përjashtimet nga deklasifikimi

Përveç kur parashikohet ndryshe në këtë ligj, një informacion mund të përjashtohet nga deklasifikimi kur ekspozimi i tij:

a) zbulon identitetin e burimit konfidencial, zbatimin e një metode apo të një burimi informativ;

b) nxjerr informacion që dobëson veprimtarinë e kriptologjisë;

c) nxjerr informacion që mund të dobësojë planet e ngutshme të sigurisë kombëtare;

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

Neni 24

Zhvlerësimi

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

2. Rregullat për zhvlerësimin e informacionit të klasifikuar “sekret shtetëror” përcaktohen në rregulloren që miratohet me vendim të Këshillit të Ministrave.

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 këtë ligj, 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. Shkatërrimi është procesi, në përputhje me këtë ligj, i shkatërrimit fizik të një informacioni të klasifikuar “sekret shtetëror”, i cili bëhet me mënyra dhe mjete që nuk lejojnë rindërtimin e plotë ose të pjesshëm të tij.

3. Rregullat për asgjësimin dhe shkatërrimin e informacionit të klasifikuar përcaktohen në rregulloren që miratohet me vendim të Këshillit të Ministrave.

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 individ, duke iu referuar besnikërisë, besueshmërisë dhe sigurisë së tij, mund të autorizohet për të pasur qasje tek informacioni i klasifikuar, pa e rrezikuar sigurinë e këtij informacioni.

2. Lëshimi, refuzimi, pezullimi i përkohshëm ose heqja e “Certifikatës së sigurisë së personelit” bëhet nga AKSIK-ja.

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 heqjes së CSP-së 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.

5. Rregullat e detajuara për sigurinë e personelit përcaktohen në rregulloren që miratohet me vendim të Këshillit të Ministrave.

Neni 28

Kriteret për njohjen e informacionit të klasifikuar

1. Kanë të drejtë të njihen, të ruajnë, të administrojnë e të transferojnë informacion të klasifikuar vetëm personat, që:

a) sigurojnë të drejtën e njohjes për shkak të detyrës që kryejnë nga titullari i ministrisë/institucionit ose oficeri i sigurimit industrial i kontraktorit;

b) janë të brifuar më parë për njohjen e procedurave të sigurisë së informacionit të klasifikuar dhe të përgjegjësive individuale për shkeljet e sigurisë; dhe

c) janë të pajisur me CSP, me përjashtim të rasteve për njohjen me informacionin e klasifikuar në nivelin “I kufizuar”.

2. Presidenti i Republikës së Shqipërisë, Kryeministri dhe Kryetari i Kuvendit janë të autorizuar që të kenë qasje tek informacioni i klasifikuar për shkak të kryerjes së detyrave të tyre zyrtare e pajisur me CSP pa iu nënshtruar procedurave të verifikimit të sigurisë.

Neni 29

Listat e funksioneve për njohje me informacionin e klasifikuar

1. Institucionet e administratës publike miratojnë dhe dërgojnë në AKSIK 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

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:

a) ka qenë, është ose tenton të angazhohet fshehurazi, vetëm ose në bashkëpunim, apo në përbërje të një organizate të paligjshme, në veprimtari spiunazhi, sabotazhi, terrorizmi, tradhtie, rebelimi apo dhune të armatosur ndaj rendit kushtetues apo ka nxitur aktivisht dikë të kryejë veprimtari sabotazhi, spiunazhi, terrorizmi, tradhtie, rebelimi apo dhune të armatosur ndaj rendit kushtetues, përfshirë hapësirën kibernetike; ose

b) është apo ka qenë bashkëpunëtor në spiunazh, sabotazh, terrorizëm, tradhti, rebelim apo dhunë të armatosur ndaj rendit kushtetues, përfshirë hapësirën kibernetike, ka dyshime të ketë qenë i tillë apo bashkëpunëtor i përfaqësuesve të organizatave, shteteve të huaja, duke përfshirë këtu shërbimet e huaja të inteligjencës, të cilat mund të cenojnë sigurinë e vendit tonë ose të shteteve anëtare të NATO-s, BE-së, përveç rasteve kur këto bashkëpunime janë të autorizuara për shkak të detyrës; ose

c) 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; ose

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

d) qëllimisht ka fshehur, ka keqpërzantuar 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; ose

e) ka një historik varësie nga alkooli, përdorimi i drogave të jashtëligjshme apo keqpërdorimi i drogave të ligjshme; ose

ë) manifeston në vijimësi sjellje/tendenca me prirje kriminale, të cilat në kompleksitetin e tyre tregojnë se personi do të paraqesë një dobësi përballë shantazhit apo do të influencohet seriozisht nga presione të ndryshme;

f) me anë të veprimeve konkrete ka shprehur mungesë besnikërie, besueshmërie dhe sigurie; ose

g) 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; ose

gj) vuan nga çrregullime mendore kronike.

Neni 31

Bashkëpunimi ndërinstytucional

Gjatë procesit të verifikimit të sigurisë, AKSIK bashkëpunon me institucionet e tjera në Republikën e Shqipërisë, të cilat detyrohen të japin informacionet e kërkuara për verifikimin e sigurisë brenda afateve ligjore.

Neni 32

Shkëmbimi i informacionit dhe bashkëpunimi ndërkombëtar për sigurinë e personelit

AKSIK-ja 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

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 parashikimet e legjislacionit në fuqi për mbrojtjen e të dhënave personale.

KREU IV SIGURIA FIZIKE

Neni 34

Kuptimi i sigurisë fizike

1. Siguria fizike është tërësia e masave fizike, teknike, elektronike dhe procedurale 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”.

Neni 35

Zonat e sigurisë

1. Zonat e sigurisë janë hapësirat ku prodhohet, regjistrohet, shfrytëzohet, transmetohet, ruhet, arkivohet dhe shkatërrohet informacioni 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 klasifikuar.

3. Zonat e sigurisë ndahen në tri kategori:

- a) zona e sigurisë e klasit të parë;
- b) zona e sigurisë e klasit të dytë;
- c) zona administrative.

4. Informacioni i klasifikuar “sekret shtetëror” i nivelit “tepër sekret” prodhohet dhe administrohet në zonat e sigurisë së klasit të parë.

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

6. Informacioni i klasifikuar “sekret shtetëror” i nivelit “i kufizuar” prodhohet dhe administrohet në zonën administrative.

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 u nënshtrohet kontrolleve të rregullta fizike, teknike dhe hyrja në to duhet të ketë kontroll të rreptë.

2. Këto zona krijohen vetëm në institucione të veçanta, si dhe gjatë zhvillimit të takimeve në funksion të aktiviteteve të NATO-s/BE-së, në të cilat trajtohet informacion i klasifikuar.

3. Zonat teknikisht të sigurta përcaktohen me urdhër të titullarit të institucionit, në bazë të kritereve të përcaktuara me vendim të Këshillit të Ministrave.

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 e administratës publike marrin masa, sipas akteve nënligjore në fuqi, për zbatimin e mënyrave të sigurisë fizike të informacionit të klasifikuar.

5. Rregullat për sigurimin fizik të informacionit të klasifikuar përcaktohen në rregulloren që miratohet me vendim të Këshillit të Ministrave.

Neni 38

Evakuimi i informacionit të klasifikuar

1. Institucioni i administratës publike 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, të dëmtohet, të komprometohet, të shkatërrohet.

2. Për informacionin e klasifikuar të NATO-s, BE-së, titullari i institucionit miraton planin e evakuimit të informacionit të klasifikuar në bashkëpunim me AKSIK-un.

3. Rregullat për evakuimin e informacionit të klasifikuar përcaktohen në rregulloren që miratohet me vendim të Këshillit të Ministrave.

KREU V

SIGURIA NË SISTEMET E KOMUNIKIMIT DHE INFORMACIONIT

Neni 39

Kuptimi i sigurisë në sistemet e komunikimit dhe informacionit

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 përshtatshëm.

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, heqja dhe pezullimi i përkohshëm i Deklaratës së Akreditimit të Sigurisë

1. Lëshimi, refuzimi, pezullimi i përkohshëm ose heqja e Deklaratës së Akreditimit të Sigurisë (DAS) bëhet nga AKSIK-u.

2. Njoftimi për vendimin e marrë nga AKSIK-u për refuzimin, heqjen ose pezullimin e përkohshëm të DAS-it 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 përshtatshëm 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-në e akredituar nga AKSIK-u, asgjësohet në përputhje me procedurat e miratuara nga AKSIK-u.

Neni 43

Kërkesat e sigurisë së SKI-së

Institucionet e administratës publike 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 organizatave të huaja, me të cilat Republika e Shqipërisë ka marrëveshje sigurie nëpërmjet sistemeve të komunikimit dhe informacionit, duhet t’u përmbahen kërkesave përkatëse të sigurisë.

Neni 44

Siguria e komunikimeve

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 përshtatshëm nga AKSIK-ja.

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

Masat e sigurisë janë mekanizmat dhe procedurat e aplikuara nga subjektet, objekt i këtij ligji, me qëllim për të siguruar mbrojtjen e informacionit të klasifikuar.

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

Menaxhimi dhe garantimi i aspekteve të sigurisë së SKI-së kryhet nga autoritetet e mëposhtme të sigurisë:

1. Autoriteti Kombëtar i Sigurisë së Informacionit të Klasifikuar, i cili funksionon edhe si:

a) Autoritet Kombëtar i Akreditimit të Sigurisë (AKAS), përgjegjës për akreditimin e sigurisë të SKI-së, të cilat nuk janë pjesë e infrastrukturave kritike dhe të rëndësishme të informacionit, si dhe sistemeve të NATO-s, BE-së dhe shteteve/organizatave të huaja që operojnë në institucionet e administratës publike;

b) Autoriteti Kombëtar i Testimit dhe Vlerësimit të Sigurisë (AKTVS), përgjegjës për testimin dhe vlerësimin e elementeve hardware, firmware dhe software të SKI-së, që përpunojnë informacion të klasifikuar, për të cilët kërkohet testim dhe vlerësim i sigurisë.

Në rast të cenimit të integritetit të informacionit të klasifikuar, në SKI subjektet, objekt i këtij ligji, informojnë në mënyrë të menjëhershme AKSIK-un.

2. Drejtoria e Shifrës, e cila funksionon edhe si:

a) Autoritet Kombëtar i Sigurisë së Komunikimeve (AKSK), përgjegjës për:

i. kontrollin e informacionit teknik kriptografik, që lidhet me mbrojtjen e informacionit të klasifikuar;

ii. garantimin e përzgjedhjes, operimit dhe mirëmbajtjes së përshtatshme të sistemeve, produkteve dhe mekanizmave kriptografikë;

iii. garantimin e përzgjedhjes, operimit dhe mirëmbajtjes së përshtatshme të pajisjeve të sigurisë së SKI-së;

iv. trajtimin e çështjeve teknike dhe të sigurisë kriptografike për aspektet e sigurisë së komunikimeve.

b) Autoritet Kombëtar i Shpërndarjes Kriptografike (AKSHK), përgjegjës 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 ose organizatave të huaja;

c) Autoritet Kombëtar TEMPEST (AKT), përgjegjës për kontrollin dhe vlerësimin e sigurisë së emetimeve elektromagnetike të sistemeve.

3. Rregullat dhe procedurat e detajuara për sigurinë e informacionit të klasifikuar në sistemet e komunikimit dhe informacionit, përcaktohen në rregulloren e miratuar me vendim të Këshillit të Ministrave.

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.

2. Rregullat për mbrojtjen e informacionit të klasifikuar në fushën industriale përcaktohen në rregulloren që miratohet me vendim të Këshillit të Ministrave.

Neni 51

Inicimi i procedurave të sigurisë

1. Institucionet e administratës publike, 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, sipas parashikimeve të legjislacionit të posaçëm të prokurimit në këtë fushë.

2. Çdo institucion i administratës publike, 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, u 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 operatorëve 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 kriterëve 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:

- a) struktura e pronësisë dhe origjina e saj, duke përfshirë filialet/degët;
- b) partnerët e ngushtë vendas dhe të huaj;
- c) qëndrueshmëria ekonomike e financiare;

- c) përmbushja e detyrimeve financiare ndaj institucioneve të administratës publike 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 qasje 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 ose palëve të treta.

Neni 53

Vlefshmëria e CSI-së dhe tipat e saj

1. CSI-ja e lëshuar nga autoriteti përgjegjës për sigurinë e informacionit të klasifikuar është e vlefshme:
 - a) vetëm për qasje tek informacioni i klasifikuar;
 - b) për qasjen, të drejtën e ruajtjes dhe të administrimit të informacionit të klasifikuar në mjediset e operatorit ekonomik;
 - c) për qasjen, 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-ja 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 qasje tek informacioni i klasifikuar.

Neni 54

Masat e sigurisë së informacionit të klasifikuar gjatë procedurës së prokurimit dhe zbatimit të kontratës/nënkontratës

1. Autoriteti kontraktor dhe kontraktori marrin masa për sigurinë e informacionit të klasifikuar në procedurën e prokurimit 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 procedurës së prokurimit 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

Vlerësimi i influencës së huaj

1. Pronësia e huaj, si formë kontrolli apo influence, i referohet një situatë, 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 influencës së huaj synon të identifikojë shkallën aktuale ose potencialin e influencës së mundshme, të ushtruar për llogari të interesave të huaja, përmes së cilës synohet akses i paautorizuar në informacionin e klasifikuar.

3. Autoriteti përgjegjës për sigurinë e informacionit të klasifikuar kryen vlerësimin e influencës së huaj, referuar:

- a) pronësisë apo shumicës së aksioneve në zotërim;
- b) pozitive të administratorit, të stafit menaxherial apo të personelit në pozicione kyçe në veprimtarinë e operatorit ekonomik të interesuar.

4. Autoriteti përgjegjës për sigurinë e informacionit të klasifikuar, në bashkëpunim me operatorin ekonomik të interesuar, përdor masa sigurie kufizuese dhe mbrojtëse për “zbutjen” deri në kufij të pranueshëm të rrezikut të sigurisë nga potenciali i influencës së ushtruar për llogari të interesave të huaja, të cilat në tërësinë e tyre synojnë për të parandaluar aksesin e paautorizuar tek informacioni i klasifikuar.

KREU VII SHKËMBIMI I INFORMACIONIT TË KLASIFIKUAR

Neni 56

Informacioni i huaj

1. Institucionet e administratës publike e ruajnë informacionin e klasifikuar të shteteve të huaja apo organizatave ndërkombëtare sipas standardeve që sigurojnë një shkallë mbrojtjeje të njëjtë me atë që kërkohet nga shteti apo organizata ndërkombëtare.

2. Institucioni i administratës publike, para nënshkrimit të një marrëveshjeje ose protokollit teknik, që përfshin shkëmbimin e informacionit të klasifikuar, duhet të marrë më parë mendimin e AKSIK-ut.

3. Para nënshkrimit të një marrëveshjeje apo protokollit 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. Përfshihen nga ky detyrim marrëveshjet ose protokollat teknike urgjente të kërkuara nga palët, kur shkëmbimi i informacionit të klasifikuar ndikon drejtpërdrejt në masat për sigurinë e stabilitetin e vendit dhe ka rëndësi të madhe për sigurinë kombëtare. Në këto raste njoftohet AKSIK-u.

Neni 57

Informacioni i klasifikuar i NATO-s

Republika e Shqipërisë mbron dhe siguron:

- a) informacionin e klasifikuar, i shënuar si i tillë, i cili vjen nga NATO-ja;
- b) informacionet e klasifikuara, të shënuara si të tilla, të shteteve anëtare, të dorëzuara 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 zbaton standardet e sigurisë në përputhje me nivelin e klasifikimit të informacionit të klasifikuar të ardhur nga NATO-ja 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, të vendimeve dhe rezolutave që kanë të bëjnë me këtë traktat.

Neni 59

Informacioni i klasifikuar i BE-së

1. Informacioni i klasifikuar i BE-së regjistrohet, shpërndahet dhe administrohet sipas standardeve që sigurojnë shkallë mbrojtjeje të njëjtë me atë që kërkohet nga BE-ja, në zbatim të marrëveshjeve të përgjithshme të sigurisë.

2. Republika e Shqipërisë mbron dhe siguron:

- a) informacionin e klasifikuar, i shënuar si i tillë, i cili vjen nga BE-ja;
- b) 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-ja 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 regjistrimit

1. Sistemi i zyrave të regjistrimit të informacionit të klasifikuar të NATO-s dhe BE-së përbëhet nga Zyra e Regjistrimit Qendror pranë AKSIK-ut, zyrat e nënregjistrimit të informacionit të klasifikuar të NATO-s, BE-së dhe pikat e kontrollit, që krijohen në ministri dhe në institucionet e tjera të administratës publike. 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 e administratës publike mbrojnë informacionin e klasifikuar të NATO-s dhe BE-së sipas standardeve që sigurojnë shkallë mbrojtjeje të njëjtë me atë që kërkohet nga NATO-ja dhe BE-ja.

KREU VIII

AUTORITETI KOMBËTAR I SIGURISË SË INFORMACIONIT TË KLASIFIKUAR

Neni 62

Misioni

Misioni i Autoritetit Kombëtar të Sigurisë së Informacionit të Klasifikuar është organizimi, drejtimi e kontrolli i masave për ruajtjen, klasifikimin dhe administrimin e informacionit të klasifikuar.

Neni 63

Organizimi i AKSIK-ut

1. AKSIK-u është person juridik, publik e buxhetor në varësi të Kryeministrit, me seli në Tiranë.

2. AKSIK-u financohet nga buxheti i shtetit dhe të ardhura të tjera të ligjshme. Buxheti i AKSIK-ut është zë më vete në buxhetin e shtetit.

3. AKSIK-u ka stemën, logon dhe vulën e tij zyrtare. Stema e AKSIK-ut përbëhet nga stema e Republikës së Shqipërisë, me shënimet “Republika e Shqipërisë, Kryeministria, Autoriteti Kombëtar i Sigurisë së Informacionit të Klasifikuar”.

4. Vula e AKSIK-ut ka formën dhe elementet e përcaktuara në vendimin e Këshillit të Ministrave për rregullat e prodhimit, administrimit, kontrollit dhe ruajtjes së vulave zyrtare. Vula prodhohet, administrohet dhe ruhet në përputhje me legjislacionin në fuqi.

5. Struktura dhe organika e AKSIK-ut miratohen me urdhër të Kryeministrit sipas përcaktimeve të legjislacionit në fuqi për organizimin dhe funksionimin e administratës shtetërore.

6. AKSIK-u drejtohet nga drejtori i Përgjithshëm, i cili organizon e drejton të gjithë veprimtarinë e saj dhe përgjigjet para Kryeministrit.

7. Rregullorja për organizimin dhe funksionimin e brendshëm të AKSIK-ut miratohet me urdhër të Kryeministrit.

Neni 64

Detyrat e AKSIK-ut

AKSIK-u, në zbatim të misionit të tij, kryen dhe realizon këto detyra:

a) përgatit projektaktet nënligjore për çështjet që lidhen me sigurinë e informacionit të klasifikuar;

b) përcakton rregullat për elementet e sistemeve që administrojnë informacion të klasifikuar dhe bën rekomandime për përshtatshmërinë e tyre;

c) mbikëqyr dhe inspekton rregullat e sigurisë për informacionin e klasifikuar;

ç) monitoron proceset e sigurisë së informacionit të klasifikuar dhe lëshon rekomandime për vendosjen e praktikave të standardizuara;

d) 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;

e) kryen certifikimin e operatorëve ekonomikë me CSI-në;

ë) inspekton operatorët ekonomikë në lidhje me zbatimin e masave të sigurisë të informacionit të klasifikuar;

f) rekomandon marrjen e masave për përmirësimin e punës në rastet e mangësive apo parregullsive në fushën e informacionit të klasifikuar;

g) rekomandon marrjen e masave dhe vendos masa administrative individuale në rastet kur konstaton shkelje të rregullave të sigurisë së informacionit të klasifikuar kur këto rekomandime nuk plotësohen;

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

h) bashkëpunon me NATO-n, BE-në dhe me autoritetet kompetente të vendeve anëtare të këtyre organizatave për fushën të cilën mbulon;

i) merr pjesë dhe përgatit projekt marrëveshtjet mbi sigurinë e informacionit të klasifikuar me shtete apo organizata të tjera ndërkombëtare;

j) trajnon personelin që punon me informacion të klasifikuar.

Neni 65

Kompetencat e drejtorit të Përgjithshëm

Drejtori i Përgjithshëm i AKSIK-ut ka këto kompetenca:

a) drejton institucionin për realizimin e misionit dhe detyrave të ngarkuara;

b) përfaqëson institucionin në marrëdhëniet me:

i. institucionet e tjera brenda vendit;

- ii. shtetet dhe organizatat e tjera ndërkombëtare;
- c) nxjerr udhëzime për zbatimin e akteve nënligjore për mbrojtjen e informacionit të klasifikuar;
- ç) inicicion, negociacion dhe nënshkruan marrëveshjet për sigurimin e informacionit të klasifikuar me shtetet dhe organizatat ndërkombëtare;
- d) kërkon nga drejtuesit e institucioneve informacione në fushën e informacionit të klasifikuar dhe bashkëpunon për përmbushjen e përgjegjësisë;
- dh) miraton inspektimet periodike për zbatimin e legjislacionit në fushën e informacionit të klasifikuar nga institucionet e administratës publike;
- e) miraton planin e dezinfektimit elektronik, i cili do të kryhet në institucionet e administratës publike dhe operatorët ekonomikë;
- ë) miraton raportet e inspektimit për zbatimin e legjislacionit në fushën e informacionit të klasifikuar nga institucionet e administratës publike;
- f) lëshon, pezullon, revokon CSP-në, CSI-në, DAS-in;
- g) miraton programin e trajnimit të institucioneve dhe operatorëve ekonomikë;
- gj) menaxhon veprimtarinë e institucionit, duke përfshirë organizimin, personelin, veprimtarinë ekonomike/financiare të tij;
- h) informon periodikisht, por jo më pak se një herë në gjashtë muaj, Kryeministrin për çështjet në lidhje me informacionin e klasifikuar;
- i) kryen detyra të tjera të përcaktuara nga ligji apo aktet nënligjore në zbatim të tij.

Neni 66

Kriteret e emërimit të drejtorit të përgjithshëm

Drejtori i Përgjithshëm i AKSIK-ut emërohet me vendim të Këshillit të Ministrave, me propozim të Kryeministrit dhe duhet të plotësojë kriteret e mëposhtme:

- a) të jetë shtetas shqiptar;
- b) të ketë zotësi të plotë për të vepruar;
- c) të zotërojë një diplomë të nivelit të dytë “Master i shkencave” apo “Master profesional” të përfunduar në fund të studimeve të ciklit të dytë me 120 kredite dhe me kohëzgjatje normale 2 vjet akademike ose të barasvlershme me to, sipas legjislacionit për arsimin e lartë;
- ç) të ketë përvojë pune jo më pak se 10 (dhjetë) vjet në çështje që lidhen me mbrojtjen dhe sigurinë kombëtare;
- d) të ketë marrë një vlerësim të lartë për aftësitë profesionale, etike dhe integritetin moral të tij, nëse u është nënshtruar vlerësimeve të mëparshme;
- dh) të mos ketë qenë i dënuar me vendim gjyqësor të formës së prerë;
- e) 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;
- ë) të plotësojë kriteret për t’u pajisur me certifikatë sigurie sipas legjislacionit në fuqi;
- f) të mos ketë qenë anëtar, bashkëpunëtor apo i favorizuar nga ish-Sigurimi i Shtetit para vitit 1990, sipas ligjit për të drejtën e informimit me dokumentet e ish-Shërbimit të Sigurimit të Republikës Popullore Socialiste të Shqipërisë;
- g) të mos ketë konflikt interesi me detyrën në përputhje me legjislacionin e konfliktit të interesit.

Neni 67

Rastet e lirimit dhe shkarkimit nga detyra

1. Drejtori i Përgjithshëm i AKSIK-ut lirohet nga detyra kur:

- a) humbet shtetësinë shqiptare;
- b) është dënuar me vendim të formës së prerë për kryerjen e një vepre penale;

- c) plotësohet mosha për pension të plotë pleqërie;
 - ç) jep dorëheqjen nga detyra;
 - d) deklarohet i paaftë për punë nga komisioni përgjegjës mjekësor, sipas ligjit.
2. Drejtori i Përgjithshëm i AKSIK-ut shkarkohet nga detyra:
- a) për shkelje të dispozitave të këtij ligji apo akteve të tjera ligjore;
 - b) kur i hiqet ose i refuzohet certifikata e sigurisë sipas legjislacionit në fuqi;
 - c) kur kryen veprimtari që krijon konflikt interesash;
 - ç) kur mungon në detyrë pa arsye për më shumë se 30 (tridhjetë) ditë rresht.

Neni 68

Punonjësit e AKSIK-ut

1. Marrëdhëniet e punës së nëpunësve të AKSIK-ut rregullohen në bazë të legjislacionit për nëpunësin civil. Marrëdhëniet e punës së drejtorit të Përgjithshëm dhe punonjësve administrativë të AKSIK-ut rregullohen në bazë të dispozitave të Kodit të Punës.
2. Për shkak të natyrës së veçantë të punës, punonjësi i AKSIK-ut trajtohet me shtesë mbi pagë.
3. Masa e shtesës mbi pagë përcaktohet në vendimin përkatës të Këshillit të Ministrave.
4. Nëpunësit/punonjësit e AKSIK-ut duhet të plotësojnë kushtet për pajisje me certifikatë sigurie personeli.

KREU IX

MBIKËQYRJA SHTETËRORE

Neni 69

Mbikëqyrja shtetërore

Mbikëqyrja shtetërore në fushën e mbrojtjes së informacionit të klasifikuar nënkupton mbikëqyrjen e institucioneve të administratës publike, 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 në fuqi për inspektimet.
3. Në përfundim të inspektimit, AKSIK-u 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 për inspektimet.

Neni 71

Mbikëqyrja dhe inspektimet e sigurisë

AKSIK-u 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

Institucionet e administratës publike apo operatorët ekonomikë, 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 të një personi i paautorizuar.

2. Kur shkelja e mësipërme nuk përbën veprë penale, përbën kundërvajtje administrative dhe dënohet sipas legjislacionit në fuqi.

3. Në çdo rast tjetër të shkeljes së dispozitave të këtij ligji, kur personat përgjegjës nuk dënohen me gjobë sipas përcaktimeve të nenit 75 të këtij ligji, kërkohet dhënia e masave disiplinore ndaj tyre sipas legjislacionit në fuqi.

Neni 74

Procedurat e konstatimit të shkeljeve të sigurisë

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 të struktura ose oficeri i sigurisë i institucionit të administratës publike dhe nëpërmjet tij tek titullari i këtij institucioni dhe në AKSIK. 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 veprë penale konsiderohen kundërvajtje administrative.

3. Konsiderohen shkelje sigurie:

a) dëmtimi i informacionit të klasifikuar;
b) aksesit i paautorizuar në informacionin e klasifikuar i një individi/operatori ekonomik;
c) mosregjistrimi i informacionit të klasifikuar në regjistrin e duhur;
ç) mosrespektimi i rregullave për mirëmbajtjen dhe ruajtjen e regjistrave për informacionin e klasifikuar;

d) shumëfishimi, përkthimi, fragmentarizimi i informacionit të klasifikuar në kundërshtim me këtë ligj;

dh) mosrespektimi i afateve për shfrytëzimin e informacionit të klasifikuar;

e) transportimi fizik i informacionit të klasifikuar në kundërshtim me këtë ligj;

- ë) mbajtja e informacionit të klasifikuar jashtë zonave të sigurisë në kundërshtim me këtë ligj;
 - f) moszbatimi i rregullave të përcaktuara në këtë ligj lidhur me shkatërrimin e informacionit të klasifikuar;
 - g) lejimi i hyrjes së personave të paautorizuar në ambientet e njësisë organizative, përgjegjëse për informacionin e klasifikuar;
 - gj) mosraportimi i shkeljeve të sigurisë;
 - h) mbajtja e pajisjeve dhe mjeteve të paautorizuara ose të paakredituara përshtatshëmrisht në zonat e sigurisë;
 - i) prodhimi dhe ruajtja e informacionit të klasifikuar në sisteme të paakredituara përshtatshëmrisht më parë nga AKSIK-u;
 - j) transmetimi i informacionit të klasifikuar në sisteme komunikimi të paakredituara përshtatshëmrisht më parë nga AKSIK-u;
 - k) klasifikimi i informacionit në kundërshtim me listën e informacioneve të klasifikuara;
 - l) mosvendosja e shenjëzimeve të përcaktuara në informacionin e prodhuar për llogari të “sekret shtetëror”;
 - ll) moskryerja e inventarit periodik fizik të informacionit të klasifikuar;
 - m) mosdërgimi i kërkesës për akreditimin e pajisjeve apo sistemeve të komunikimit në të cilat trajtohet informacioni i klasifikuar;
 - n) pengimi i kryerjes së mbikëqyrjes së masave të sigurisë dhe inspektimeve;
 - nj) mosnxjerrja e akteve në fushën e informacionit të klasifikuar;
 - o) moszbatimi i rekomandimeve të lëna nga inspektimi i kryer nga AKSIK-u;
 - p) 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;
 - q) mosrespektimi i standardeve të sigurisë sipas planit të miratuar në kuadrin e transportimit fizik të informacionit të klasifikuar;
 - r) moskryerja e verifikimit paraprak nga struktura e sigurisë;
 - rr) moskryerja e brifimeve dhe debrifimeve të sigurisë.
4. Shkelje të rënda sigurie konsiderohen shkeljet e parashikuara në shkronjat “a”, “b”, “d”, “e”, “ë”, “f”, “gj”, “i”, “j”, “k”, “l”, “m”, “n”, “nj”, “o”, “p”, “r” të pikës 3 të këtij neni.
5. 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.
6. Shkelje të lehta sigurie konsiderohen shkeljet e parashikuara në shkronjat “c”, “ç”, “dh”, “g”, “h”, “ll”, “q”, “rr” të pikës 3 të këtij neni.
7. 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.
8. Gjobat e vendosura kundër subjekteve, që shkelin dispozitat e këtij ligji, sipas përcaktimeve të pikave 5 dhe 7 të këtij neni arkëtohen në buxhetin e shtetit.

Neni 76

Përgjegjësia administrative

1. Titullari i institucionit të administratës publike mban përgjegjësi ligjore dhe administrative për shkeljet ligjore të parashikuara në shkronjat “e”, “i”, “j”, “m”, “n”, “nj”, “o”, “p” të pikës 3, të nenit 75, të këtij ligji.
2. Personi përgjegjës, i cili kryen shkeljen, mban përgjegjësi ligjore dhe administrative për shkeljet ligjore të parashikuara në shkronjat “a”, “b”, “d”, “dh”, “ë”, “f”, “gj”, “h”, “i”, “j”, “k”, “l”, “p”, “q”, “r”, “rr” të pikës 3 të nenit 75 të këtij ligji.
3. Struktura e sigurisë mban përgjegjësi ligjore dhe administrative për shkeljet ligjore të parashikuara në shkronjat “gj”, “h”, “i”, “j”, “r”, “rr” të pikës 3 të nenit 75 të këtij ligji.

4. Punonjësi i njësisë organizative, përgjegjëse për informacionin e klasifikuar, mban përgjegjësi ligjore dhe administrative për shkeljet ligjore të parashikuara në shkronjat “b”, “c”, “ç”, “d”, “dh”, “g”, “ll” të pikës 3 të nenit 75 të këtij ligji.

Neni 77

Shlyerja e masës së dënimit me gjobë

Shlyerja e masës së dënimit me gjobë bëhet në përputhje me parashikimet e ligjit për kundërvajtjet administrative.

Neni 78

Ankimi i sanksioneve administrative

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

KREU XI DISPOZITA TË FUNDIT

Neni 79

Nxjerrja e akteve nënligjore

1. Ngarkohet Këshilli i Ministrave që brenda 1 viti nga hyrja në fuqi e këtij ligji të nxjerrë aktet nënligjore në zbatim të neneve 14, pika 4; 18, pika 4; 19, pika 5; 20, pika 3; 22, pika 7; 24, pika 2; 26, pika 3; 27, pika 5; 36, pika 3; 37, pika 5; 38, pika 3; 45, pikat 3 dhe 4; 46, pika 2; 49, pika 3, dhe 50, pika 2, të këtij ligji.

2. Ngarkohet AKSIK-u të nxjerrë udhëzimin mbi procedurat në zbatim të rregulloreve të miratuara me vendim të Këshillit të Ministrave.

3. Aktet nënligjore, të miratuara në zbatim të ligjit nr. 8457, datë 11.2.1999, “Për informacionin e klasifikuar “Sekret shtetëror””, të ndryshuar, mbeten në fuqi deri në miratimin e akteve të reja nënligjore për sa kohë nuk bien ndesh me parashikimet e këtij ligji.

Neni 80

Shfuqizime

Ligji nr. 8457, datë 11.2.1999, “Për informacionin e klasifikuar “Sekret shtetëror””, të ndryshuar”, shfuqizohet.

Neni 81

Hyrja në fuqi

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

Miratuar më datë 2.2.2023.

**Shpallur me dekretin nr. 28, datë 15.2.2023, të Presidentit të Republikës së Shqipërisë,
Bajram Begaj**